

Research Online Study material for CISA/ISA

Module : 1

Reference No : M1001

Question: The auditor should ensure that the policy has been formulated and communicated by

- [a] Asks employees for related documents that they have in hand
- [b] Identifies areas where relevant information has not been communicated
- [c] Assesses the commitment of the management
- [d] Identifies its misuse

Module 1- Control and Audit Objectives

Control objective

According to standard guidelines issued by the Institute of Information Systems Audit and Control Association (PO6), it is the responsibility of the management to communicate the control objectives, policies and practices of the company. They should also provide direction while formulating, developing and documenting policies. The policy should be in line with the overall objectives of the company, and must include all significant activities. It is not enough if security policies are developed, they should also be communicated to employees. The procedure to be followed must also be detailed by the management. The management should also ensure that procedures are being implemented. The policy should be reviewed and updated periodically.

Audit objective

The auditor (IS audit) should ensure that the management has taken the required steps to formulate, communicate and implement policies and procedures. He should:

Understand roles and responsibilities: The auditor should understand the policy by interviewing the top management and senior members of the company. He should also obtain copies of similar policies and procedures developed by the management, understand the roles and responsibilities of the employees concerned, including that of the implementation team.

Evaluate controls: The auditor should evaluate controls by assessing(commitment of the management):

Whether the top management has created a conducive environment through its policy statements

Whether the management has discharged the responsibility of formulating the policy

Whether the policy has been communicated to employees

Whether there is awareness among employees on procedures to implement the policy

Whether procedures are being followed by employees

Whether resources are made available for implementing the policy

Whether periodical reviews are being undertaken

Assess compliance: After assessing and understanding the level of control, the auditor should perform a compliance test:

Have employees have received policy documents?

Are they aware of details?

Have resources been committed for formulating, communicating and implementing the policy?

Have employees at all levels understood their roles and responsibilities?

Is the policy being reviewed periodically?

How does the management enforce compliance?

Is the creation of exceptional reports, comparisons and the like undertaken?

Is follow up on exceptional reports undertaken?

Is feedback is provided to the management?

Check substantive procedures: Having assessed the level of compliance, the auditor should perform a substantive test. He can compare the policy with those adopted in similar companies or with best practices in the industry. He should identify areas for improvement. Based on the test, the auditor should be able to evaluate whether

The controls are weak

The management's commitment is in accordance with the policy

The policy has been effectively communicated

Resources have been equitably allocated

The policy has been updated to reflect changes in corporate activities

All areas have controls that are in accordance with risks

The policy is being misused in any area

Note: Please refer to our earlier articles for detailed information on

- General guidelines for framing a security policy
- General guidelines for framing a network policy

Answer: [c] Assesses the commitment of the management.

Explanation: During the evaluation stage, the auditor evaluates only the management's commitment to the policy.

Module : 1

Reference No : M1002

Question: While conducting the audit, the auditor shall allocate the audit resources to:

- [a] Sequentially selected areas
- [b] Prioritised areas
- [c] Randomly selected areas
- [d] All areas subject to audit

Module 1 - Use of CAATTs in Audit Management - Part 1

This is the first of the two part series on Use of CAATTs in Audit Management.

Audit is a function that deals with various clients and platforms. In this process an audit firm should deploy the right manpower with specialisation in several domains. Audit management needs planning, organising, directing and the like. Concept of materiality is applicable in audit also. Audit involves reviewing processes, activities, and information in risk areas. Manpower and resources should be directed to important and risky areas so that the cost comes down. An audit management involves planning and managing individual audit engagements, maintaining records of prior and current audit, directing and scheduling personnel, and communicating effectively with audit clients, senior management and board of directors. The tools that are generally used by the auditors in audit management and administration may be classified as follows:

- Inventory of the audit universe
- Personnel database and skills inventory
- Risk analysis and risk management
- Planning and scheduling
- Project management and audit tracking
- Communications
- Presentations
- Studying the results and findings

Pre-audit

Inventory: Before beginning the actual task, it will save a lot of time and effort, if the auditor equips himself with the inventory knowledge of his client or the industry. An inventory in the following areas would be useful to prepare the scope of audit and deploy the correct manpower

Inventory of the audit universe: The auditor on the basis of availability must allocate the audit resources to the prioritised areas, which are determined after discussion with the senior management. The auditor in this is guided by the risk analysis performed by him or management. The inventory of the audit universe should show the areas to be covered and must include:

- The priority areas and the basis for determining priority
- Audit cycle
- Results of last and prior audits
- Summary of audit findings, recommendations and follow up

- Indicators of risk and the nature of risks (monetary, reputation, legal, environmental, privacy, confidentiality, availability etc.)
- New development and commercial implementation of technology
- Special notations, instructions etc.
- In case of regulated industry, the mandatory areas should be covered and specifically looked into.

The audit universe does not always remain the same. Sometimes they are subject to significant changes. The auditor should evaluate the universe to understand the changes that have taken place and acquire the expertise for evaluation purpose if he does not possess them.

Personal database and skills inventory: Provides information for planning and project development. It helps the auditor to map the training and experience required for audit. It also provides information on weak areas. Audit of such areas may be assigned to others or a specialist may be called for.

Risk analysis and Risk Management: The scope of audit and commitment of resources should be based on the risk areas determined by the management or the auditor. The management will perform risk analysis and risk management in which the auditor may or may not be involved. If the management does not conduct risk analysis and risk management then the auditor should assess them and communicate the same to management to ensure consistency. The risk assessment is an iterative process. The auditor should maintain the results of risk assessments as part of their working papers to serve as reference for subsequent audit projects. The auditor should not be just concerned with risk control. He should also focus on controls that minimise risks. The auditor should supplement the risks identified by him with those identified by the management. The probability of risks and the cost involved should be assessed. The result of his assessment should be communicated to the management and he should satisfy himself that the management has understood the threats and the liabilities thereof.

Pre-audit planning and scheduling, the audit and post audit of Use of CAATTs in Audit Management is dealt in the second part of the series.

Answer: [b] Prioritised areas.

Module : 1

Reference No : M1003

Question: Which of the computer assisted audit techniques and tools help the auditor to identify the impact of delays and rescheduling audit plans

- [a] Planning and scheduling
- [b] Project management and audit tracking
- [c] Inventory of the audit universe
- [d] Risk analysis

Module 1 - Use of CAATTs in Audit Management - Part 2

This is the second part of two part series on Use of CAATTs in Audit Management. In this part we cover the pre-audit planning and scheduling, the audit and post audit of Use of CAATTs in Audit Management.

Planning and scheduling: Audit planning is both strategic and tactical. The inventory of audit universe, priority of audit and availability of audit resources provide input to the strategic audit schedule. Tactical planning is performed for each audit project.

Strategic audit planning – The auditor before commencing audit should address the known problem is key control areas, as it will impact the scope and time required to assess and test controls.

Tactical audit planning – The auditor should employ software tools to assist him in assessing the available skills and allocating the appropriate people to specific audits. The allocation of people should be possible even when the audit is not completed so that the required persons can proceed to other audits where they are required. The software should also assess the impact of schedule and priority changes, compensate for special assignments, and extend the impact of schedule overruns to other projects remaining in the schedule.

Audit

Project management and audit tracking: Each audit undertaken is to be approached by an auditor as a project in itself. He needs to plan and schedule properly. When an audit firm undertakes several audit programs simultaneously tracking the status of audit and deploying resources appropriately is one important aspect of audit management. Project management and audit tracking whether simple or sophisticated help in audit planning and scheduling, and to make the best use of available resources. The software should also report on any variances from plans and provide reports and graphics to assist in decision making. The software used for project management and tracking helps the auditor to schedule all audit projects and subtasks individually and collectively. It also provides a detail summary of the impact of delays or rescheduling on related or subsequent audit plans. Auditor before using the software should determine if the same software is being used in the organisation to decide whether to use the same software for audit purpose or not.

Communications: It is important that the audit progress and findings be communicated within the audit team and with the business being subject to audit. This helps the auditor to check the work in progress and provide immediate feedback. For this purpose auditors can use electronic communications.

Presentation: Presentation of information in form of charts, graphs, pictures, sound and video clips help in better understanding of information. Presentation of information in this format is now possible with the availability of sophisticated software. Presentations can be delivered either in person or via mail or other file transfer. Presentations can also be linked to audit working files or databases to provide consistency and continuous update as needed.

Tracking of results/ findings: Organisations may gain enhanced internal controls, economies, efficiencies or other measurable improvements from implementing the audit recommendations. The benefits derived to the organisation can be reported as benefits of employing audit service. If the recommendations of audit are not carried out the auditor should investigate and should follow up until the findings are resolved.

Post audit

Customer satisfaction assessment: The auditors may maintain customer satisfaction software to maintain a database of customer responses. This helps the auditor to measure the performance against target levels. Auditor should be cautious and should not allow anticipation of feedback to impair performance, independence or objectivity.

Training and education: The auditor should assess the needs for training the staff involved in audit in computer-based training.

Reference library: An audit reference library can be assembled in electronic form and made available for local, portable and remote access. The information that can be provided may include

- Reference works from professional associations
- Regulatory requirements and guidelines
- Reference manuals

- Policies and procedures
- Contracts and legal documents
- Forms, formats, templates and any other item.

Answer: [b] **Project management and audit tracking**

Module : 1

Reference No : M1004

Question: While conducting an audit, the auditor should

- [a] Insist that a security policy exists
- [b] Not insist for a security policy
- [c] Insist that a security policy exists, and accept the existing policy
- [d] Insist that a security policy exists. However he may not accept the existing policy

Module 1 - Security Audit - Part 1

Information is a valuable asset that must be protected from a wide range of threats in order to preserve business continuity. This helps in maximising return on investments thereby reducing damage to business. Information exists in -printed, written, or electronic form.

Information security involves the preservation of confidentiality, integrity and availability of the information. This is achieved by implementing an appropriate set of controls. The controls can be policies, practices, procedures, organisational structures and software functions. Information security also includes the human interface to the information.

The final aim for which the management requires an audit is to get an assurance that information is backed-up and the risk of losing this information is kept to a minimum. Before commencing the audit, the auditor should understand the purpose for which it is to be carried out. This requires an understanding of what needs to be protected.

A security audit involves the assessment of the policy based procedures and level of risk created by these actions. The auditor, while performing the security audit should carry out number of tasks which include

- Preparation
- Reviewing of the policy
- Gathering information
- Technical investigation
- Reviewing data
- Reporting
- Post audit actions

Preparation: The organisation's IT system comprises a number of components including hosts, servers, firewalls, the network, communication lines, application programs, and databases. The auditor must decide on how thoroughly he will audit each of these components. This depends on the security level of each component. A plan in which the audit must be carried out should be drafted so that access to some systems can be restricted. Testing of these components must be done after business hours so that the routine activities of the business are not disturbed. A time should be fixed to meet up with selected staff members to assess how they work and whether their operations are as per the security policy. A series of questions should be

prepared in advance so that the same can be used during the discussion with staff members. Interviewing personnel involved in security administration and user groups will give the auditor a better understanding. Depending on the security level and the components, different auditing tools have to be used to conduct the security audit.

Auditors should verify audit tools and the environment before commencing the audit. This should ensure that tools are not tampered with and are reliable. These tools can either be developed by the auditor or may be acquired.

Reviewing policies and documents: The auditor must obtain a copy of the overall security policy. For an effective security management audit, a security policy should exist. Each component of the information system viz. servers, network, firewall etc. have different roles to play and security policies should include each of these components. If the security policy does not exist, the management should be advised to create one. If a policy exists, the auditor must first review it to determine if the policy covers all the basic components of the security policy. (Refer to our article on security policy) The mere existence of a policy is not sufficient, it must be read and understood by the people. The auditor should assess how well the staff has understood the security policy. He should also assess the procedure for dissemination of information and documents.

Gathering information: The most important task in audit is gathering information. By interviewing staff members the auditor can gather important information that may not be available even after assessing the policy and other related documents. Interviews should not be limited to technical staff but must extend to all users in the system, managers, and even others who are not directly involved. The interviews will help the auditor to determine the usage pattern and whether users have seen and read the policy. The auditor should try to obtain information about what users can and can't do, and whether they can obtain root or system administration privileges and their opinion is about the security audit. He should also find out what are the critical systems. The auditor must review all other documents especially those related to emergency procedures and reporting incidents.

The other aspects of audit are covered in a different article.

Answer: [d] Insist that a security policy exists. However he may not accept the existing policy

Module : 1

Reference No : M1005

Question: At what stage the risk assessment should be included in the security program while adding the new system or modifying the old system?

- [a] When the new system is added or old system is modified
- [b] At the end of the year along with all other additions or modifications during the year
- [c] Need not be done
- [d] After a defined period say every 3 months

Module 1 - Management Guideline on Security Program - Part 1

Security program reflects the commitment of the senior management for security management, planning and security controls. The security program is a framework of continuous cycle of activities for assessing risks, developing and implementing security procedures to address the risks and monitor the effectiveness of the procedures in addressing the risks.

This is first of three part series on management guideline on security program.

Assessment of risk and development of security plans: For an effective security it is necessary that risk assessment should be done to determine the level of security needed. Security plan should be developed based on the results of the risk assessment. The plan acts as a foundation for implementation of security in the company. The management should ensure that

- Risk assessment is being done on a regular basis and same is documented
- It covers all the important systems, processes and data
- Risk assessment is performed whenever systems, facilities and other important functions change
- Data sensitivity and integrity is considered while performing risk assessment
- Security plan is documented and it covers areas that are subject to high risks
- Security budget is prepared based on security plan
- The management approvals are documented

Incorporation of security measure into new or modified systems and processes: The security plans are not static. When new systems are added or modification to the existing systems are made the risk assessment should be done and accordingly modifications are to be made to security plan.

- Process should be defined for including the security measures in new or modified systems and processes
- Security safeguards for reducing or eliminating security threats and vulnerabilities are defined, implemented and documented
- Cost benefit analysis on both monetary and non-monetary aspects are done before implementing security measures
- The user department decision is taken on the measures to be implemented for minimizing the risks and residual risk is taken into account before making a decision
- A responsible person from IT management takes care of the security measures while installing a new hardware or software or making changes to the configuration of the existing hardware or software
- An independent certification is obtained before installing a critical new technology service
- Security aspect is taken into consideration before outsourcing an activity either operation/ process or implementing/ maintaining security itself
- External services have adequate security control
- The implemented security controls are tested
- User department are satisfied with the test results
- Security manager is satisfied with all the implemented security controls or the areas where it should be implemented
- Re-certification for security controls is obtained periodically from external service providers

Documentation, approval and maintenance of security program: The top management and the security officer should approve the security program. It should be documented so that it can be referred in future and all the people related to security can read it and understand their responsibilities. The document should be clear and should be easily understandable. When there is any security breach or violation the document can be easily referred and the prescribed procedure can be followed. This includes that

- Security program is documented and maintained
- The scope is wide enough to cover all major facilities and operations
- It embraces
 - Rules of the system
 - System interconnection
 - Personal controls

- Technical security
- Continuity of support
- Training
- Approved by the user department and other affected parties
- Standards and procedures exist to document management decision with regard to activities, applications, systems or technologies
- Users identification and access right are centrally established
- Security program is reviewed periodically
- Program is flexible to incorporate current conditions and risk
- Owner of computer related resources are identified.

Answer: [a] When the new system is added or old system is modified

Module : 1

Reference No : M1006

Question: _____ is an estimate of the degree of certainty that the population average will be within the precision level selected

- [a] Standard deviation
- [b] Confidence level
- [c] Precision
- [d] Range

Module 1 - Statistical Sampling

Sampling involves the selection and analyses of a finite number of items in order to obtain information about the population from which they are selected. It is an application of a procedure to only a part of the population in an attempt to form a judgment about the entire population.

Sampling can be done either statistically or on the basis of judgment. Statistical sampling requires selection of items to represent the population mathematically. In the case of judgment sampling, selection of items is based on the judgment of the selector or on what suits the audit objective. Judgment sampling differs from statistical sampling in one respectB the degree with which the judgment sample represents the population cannot be demonstrated mathematically. Judgment sampling is used when it is not essential to have a precise representation of the condition of the population or in cases where it is not possible, practical or necessary to use statistical sampling.

Statistical sampling has become an integral part of the auditor=s toolkit. It is used in conducting performance or operational audits. Using statistical sampling it is possible to state with a stipulated degree of confidence that the number of error in the sample applies proportionately to the unsampled portion of the universe as well. The advantages of using statistical sampling are-

1. The sample result is objective and defensible. The question of bias that may occur in judgment sampling does not arise.
2. It is possible to know in advance the maximum size of the sample needed. It can be used in cases where the confidence level desired is high for the risk being evaluated.
3. It helps the auditor determine the degree of risk up to which the sample selected by him may not be a representative of the entire population.

4. Auditing the entire data is a voluminous and tedious task, which may lead to errors of omission of facts. With statistical sampling it is possible to arrive at a more accurate judgment.
5. With statistical sampling it is possible to test several characteristics of the population using one sample. This saves time and money.
6. Test results are projected within known limits of reliability.
7. Data can be combined and evaluated even if it is obtained by different users.

Basic Statistical terms

1. **Average:** The average or mean is the measurement of the central tendency of a variable. It is the sum of the sample values divided by the number of items in the sample. For example if the sample consists of four invoices with the value of 40,30,12,10; the average will be the total i.e 92 divided by 4 (the number of values). The average is 23.
2. **Range:** The difference between the highest and the lowest number in a group of observations. For example if the number of items for a particular stock number in each of six storerooms were 4, 8, 9, 2, 7 and 6, the range would be from 2 to 9.
3. **Standard deviation:** It is the measure of frequency distributions= variability. The greater the variability, the larger the value of the standard deviation. To obtain the standard deviation it is required to calculate the difference between the value of each individual item in the population and the population mean; square these differences, add them, divide the sum by the total number of items and finally extract the square root.
4. **Reliability (also known as Confidence Level):** An estimate of the degree of certainty that the population average will be within the precision level selected. Standard deviation is the key to determining reliability.
5. **Precision:** The range within which the universal average will lie, with the degree of certainty specified in the confidence level. It is also known as confidence interval. Precision is the range of values about a statistical value measured by a sample (generally the mean) that will have a given probability of containing the true value of the population=s statistics. It is described in terms of a plus and minus value about a sample mean. For example, if the confidence interval is 1, precision would be +/- 0.50
6. **Frequency distribution:** It is the classification of items in set of data values by a quantitative characteristic. The more number of classes in a frequency distribution the more the detail shown. However, too many details can make summarisation difficult.

Answer: [b] Confidence level

Module : 1

Reference No : M1007

Question: Which sampling plan will be used to find evidence of at least one improper transaction in the population?

- [a] Discovery sampling
- [b] Acceptance sampling
- [c] Dollar unit sampling
- [d] Attribute sampling

Module 1 - Sampling Plans And Selection Techniques

It is not possible to check all transactions while conducting an audit. Sampling is used to audit selected transactions that will represent the entire population.

The sampling plans most often used are as follows:

1. **Estimation sampling:** It is the determination within the specified limits and with a specified risk the frequency of occurrence of some such events or errors. It helps the auditor to arrive at a conclusion regarding the entire population. It includes sampling for attributes and sampling of variables.
 - Attribute sampling: It is a means of establishing the frequency of occurrence of some kind of event or type of item. It is used to determine the characteristics or attributes of a population. The results of such a sampling operation are commonly expressed as a percentage of the type of event specified. Each observation is mutually exclusive i.e. it can only fall in one category. Attribute sampling answers the question "How many?"
 - Stop or Go Sampling is an extension of attribute sampling. It is used to reach a conclusion about the upper precision limit of an attribute sample. It allows the objective to be attained with a smaller sample size than possible using attribute sampling.
 - Variables sampling: It provides an estimate of an average or total value of a population. It is used for estimating means or other values. It answers the question "How much?"
2. **Acceptance sampling:** It consists of selection of a sample of a given size from a given population by random methods. The population is rejected if the sample contains more than a certain number of disparities are found and vice versa. Acceptance sampling deals only with a rate of occurrence of events such as errors, disparities etc. The auditors generally use this to test transactions.
3. **Discovery sampling:** Sometimes referred to as exploratory sampling, it is used where evidence of a single error or instance of irregularity would call for intensive investigation. The auditor generally uses it when there is fraud, avoidance of internal controls, evasion of regulation or other critical performance or quality control measures are in question.
4. **Dollar unit sampling:** It is used for both attribute and variable sampling. The sample units are defined in individual dollars rather than as physical units such as inventory items. The technique is applied on individual accounts or inventory items containing the dollar selected.
5. **Judgment sampling:** In this method the user uses his judgment to determine the sample size.

Sampling selection techniques:

1. Unrestricted random numbers: In this technique each item in the population has an equal chance of being included in the sample.
2. Interval sampling: In this method the items are selected from the population in such a way that there is a uniform interval between sample items. The first item is chosen at random.
3. Stratified sampling: In this method the items in the population are first segregated into two or more classes called strata. Items within each stratum are generally comparable and each stratum is sampled independently. This method is suitable when there is a wide variance among the sampled items in the characteristics to be measured.
4. Cluster sampling: In this method the population is formed into groups or clusters of items. All the cluster will contain the same number of items. Then the items within the selected clusters will be sampled or examined in their entirety.
5. Multistage samples: Sampling is performed in stages. The sampling units at each stage are sub-sampled from the larger units chosen at the previous stage.

Evaluation of results:

The auditor after performing the sampling technique using the sampling plan or selection technique must evaluate his results. If the auditor uses statistical sampling then the statistical methods aid in evaluating the results. The following rules aid in meaningful evaluation of test results:

1. The findings of each sample must be evaluated separately.
2. The acceptable error rate depends on the auditor's judgment of the significance of the errors.
3. When the sample reveals a critical exception the auditor should consider whether to stop the testing and apply other procedures to arrive at a conclusion about the characteristic of the sample.

Answer: [a] Discovery sampling

Module : 1

Reference No : M1008

Question: Possible errors related to a security issue during application development can be identified by reviewing-

- [a] System logs
- [b] Security policies
- [c] Code reviews
- [d] System configuration files

Module 1 - Security Audit - Part 2

Part 2 of this series on security auditing deals with:

1. Technical investigation
2. Reviewing of data
3. Reporting

Technical investigation: This involves running a scan using various static tools that gather vast amounts of information. These tools require little user intervention.

The security audit should examine system logs, start up processes, documents related to configuration of various IT components, and source code of application programs.

The auditor should therefore examine

- System logs to understand usage patterns, sites which disallow or restrict user access, and improper use
- Systems for known vulnerabilities
- Start up process to check for applications that have been disallowed. The list should be compared with applications that are installed on the machine
- Static items to check for alteration and or inclusion of unwanted or dangerous commands
- System, execution and configuration files of applications and programs that run on a privileged mode (run as root)
- Network resources to check for services that are overloading system resources.

Applications developed by the organisation must be subjected to a complete code review. The auditor will require the assistance of a developer in case he does not possess required skills /language in which the

application has been developed. For instance, when changing over from a normal user to a system account user, the auditor should report if the program does not have documentation or comments within the source code as this can hamper the review.

The auditor should also conduct active testing to determine how effective existing security measures are. If there is no system failure during the test, it implies that security measures are functioning as planned. However, before conducting such tests the auditor should decide if it is actually necessary as it can adversely affect the network. If the decision is made to carry out the test, then the auditor should ensure that the systems are fully backed up and the back ups are usable. The test should also be carried out after working hours.

Reviewing data: All the data collected during the audit must be preserved. This should form a part of the working papers of the auditor. The data collected can be in written or electronic form. Data which is in electronic form should not be stored online even in encrypted form. The data should be kept in a secure place so that unauthorised access can be checked. Any kind of access to the data should be only on a "need to know" basis.

Reporting: All findings from the audit must be presented to the concerned persons in the form of a report. This may include board-level directors, IT managers and IT staff. The report must clearly state the findings and the recommendations if any. The level of technical detail should increase as the report continues. When reporting to high-level staff, the information should be in clear/non-technical language. The report should have a logical structure. It should include-

- An executive summary with prioritised recommendations
- Scope of the audit
- Detailed information
- Final conclusions and detailed recommendations.

Post audit actions : After the report has been submitted, the auditor should ensure that the recommendations are implemented. If not, he should obtain an explanation regarding the same.

Answer: [c] Code reviews

Module : 1

Reference No : M1009

Question: The auditor during the course of his audit of IT steering committee interviews the members of the committee. This process helps the auditor to ascertain

- [a] Members of the committee are the persons who have more number of years of experience in the company
- [b] Members are appointed by the IS project sponsor
- [c] Committee is in charge of allocation of resources and prioritising the projects
- [d] The organisation culture is in no way influencing the committee and its management practices

Module 1 - Audit of IT Steering Committee IT auditors have always advocated the need for an IT steering committee. Many IT companies are following this recommendation. But the setting up of IT steering committee by itself does not guarantee efficient working. The auditor during the course of his audit must evaluate the functioning of the committee.

Objectives:

The auditor during the course of the IT steering committee must ensure Whether duties and responsibilities of the committee are well defined, documented and communicated throughout the company.

Whether members possess the qualification to undertake their respective roles as member of committee.

Effectiveness of the committee in monitoring and supervising the IT related activities.

Audit

Review of charter:

The auditor must obtain the copy of the IT steering committee and review it to determine whether Charter is in agreement with the overall objectives of the organisation.

Charter is current.

Roles and responsibilities have been clearly defined and specified.

Charter specifies the members' authority for management of IT projects, for setting priorities, allocation of resources and monitoring the progress.

Committee is made responsible for directing the activities of the sub-committees including the project steering committee.

The members have the authority to review the investments in projects over a specified amount.

Documents:

The auditor should review on sample basis, the documents generated by the committee, eg. minutes. The sample selected should depend on the time at which the audit is undertaken, frequency of the meetings, and availability of the documents. All the variances between the functions defined in the charter and the functions undertaken must be reviewed to ensure that the roles and responsibilities are clearly understood by the members and the internal controls that exist are functioning effectively.

Information System (IS) department:

The auditor must interview the personnel of IS department. The IS department has to report to the IT steering committee. The committee in turn is responsible for monitoring and measuring the performance of the IS department. The IS department must be free to raise their issues with the committee. The auditor must ensure that there exists a cordial relationship between the two so that projects and other IT plans are successful.

IS project sponsor:

IS project sponsors should also be interviewed. The interview process and the examination of other documents help the auditor to determine if they have been any deviations in the implementation stage. This also includes the documents of IT steering committee. This helps the auditor to correctly assess the deviations as the committee might have made some changes in the plan like resource allocation, setting of priorities and the like.

IT steering committee:

The members of the committee must be interviewed. This process along with the understanding of the management practices helps the auditor to ascertain whether the

Committee has the support of top management.

Members have the relevant experience and skills.

Committee is not biased in making decisions.

Company has allocated resources to the committee.

Members are updating their knowledge and understanding of IT skills.

Proper procedures are defined for the operations.

Committee has formulated procedures and reports as to how the other departments are to report to them with regard to their IT functions.

Key performance indicators have been determined to measure the effectiveness of the committee.

Stakeholders are communicated about the decisions taken by the committee.

The auditor should keep in mind that the managing practices of the committee are influenced by the corporate culture. The auditor should compare the IT steering committee with the committee of other companies and make recommendations with respect to the changes that should be made in the charter or in the required skills of the members of the committee and its functioning.

Audit report:

The audit report should contain the findings and recommendations of the auditor. All the findings must be supported by documentary evidence. The auditor should ensure that the report especially the findings and recommendations are discussed with the stakeholders.

Answer: [c] Committee is in charge of allocation of resources and prioritising the projects

Module : 1

Reference No : M1010

Question: The IT auditor considers the controls that are present for the evaluation of the internal controls. Which of the following controls cuts across the hierarchical line and follow the data as it flows in the organisation?

- [a] Corrective controls
- [b] Management controls
- [c] Application controls
- [d] Detective controls

Module 1 - Types of Controls

Internal controls are the controls, which help the organisation to manage such risks that effect the attainment of the goals and objectives. The primary objective of internal controls is to ensure

- Reliability and integrity of information
- Compliance with policies, plans, procedures, laws and regulations
- Safeguard of assets
- Efficient use of resources
- Accomplishment of established objectives and goals

The IT auditor considers the controls that are present for the evaluation of his internal controls. The controls that are present in the organisation can be broadly classified on the following basis

- Application and management controls
- Preventive, corrective and detective controls

Application and management controls:

These controls ensure that the development, implementation and the operation of IT proceed in a planned and controlled manner. Management controls are the fundamental controls that cover all application systems. The absence of the management controls is a serious concern for the auditors. They are protective layers around applications and can be compared to the layers in an onion. When the management controls are weak, it is not worthwhile for the auditor to review and evaluate the application controls. It is therefore necessary for the auditor to first evaluate the management controls. The management controls in an organisation depend upon the hierarchy and the different functions that are performed in the organisation. The functions and the responsibilities of each person should be well defined.

The application controls ensure that each application system protects the company's assets, maintains the data integrity and processes the data efficiently. The application controls can be categorised as under:

Data preparation controls: These controls ensure that all data is converted to machine readable form, is authorised, complete and accurate, is fed into the computer and then returned for proper filing.

System access controls: This is to ensure that only authorised personnel gain access to the system and other resources.

Input controls: This is to ensure that data entered into the computer is authorised, accurate and complete, the errors in the data are identified, rectified and re-entered for processing.

Transmission controls: This is to ensure that data sent through transmission media is authorised, accurate and complete.

Processing controls: This is to ensure that the data entered into the system is processed and that the processing is authorised, accurate and complete.

Output controls: This is to ensure that output is distributed to the right personnel and that it is authorised, accurate and complete. With the help of audit trails, data can be traced from the source to final output and vice versa.

Backup and recovery controls: Through such a control the data that is lost or the integrity of which is corrupted, can be restored.

Application controls are horizontal in nature. They cut across the hierarchical lines and follow the data as it flows in the organisation. The management controls are vertical in nature and they follow the hierarchical structure as it exists in the organisation.

Preventive, detective and corrective controls:

Preventive controls:

- Designed to discourage errors and regularities
- Used during the early stage of flow of data
- To detect problems before they arise
- Is used during input and operation stage

Examples: segregation of duties, establishing well defined policies and procedures.

Detective controls:

- Identifies an error or regularity after it has occurred

- Includes input validation controls
- Reports the error or irregularity

Examples: Internal audits, designing controls such as limit check in the program

Corrective controls:

- Corrects identified errors
- Should be subject to detective controls after making the corrections
- Modifying the processing system to minimise the re-occurrence of the problem

Example: Backup procedures, contingency planning.

Answer: [c] Application controls

Module:1

Reference No:M1011

Question: The success of Control Self Assessment (CSA) depends on culture of the organisation, project leader and the skills of the people involved in CSA. While implementing, the pitfall to be avoided is

- [a] Generalisation of the planning process
- [b] Implementation on small projects
- [c] Management support
- [d] Broadening the focus of CSA's effectiveness

Module 1 - Control Self Assessment

Control self-assessment (CSA) is the involvement of management and staff in the assessment of internal controls. It evaluates informal or subjective controls in areas such as ethical practices, management philosophy and human resource policies. It involves appraisals with the staff to determine whether the processes are in place, are effective and whether the objectives are being met. There are different CSA practices and each has its own advantages and disadvantages.

Viewpoint

From the employee's perspective, CSA solicits open communication, teamwork and encourages improvement. Vis-à-vis the management, it assists in determining whether the organisation is meeting its objectives.

Implementation

1. Scope: The management should decide
 - The areas that should be subjected to CSA.
 - The level at which it will be used - workgroup, division et al.
 - Objectives that must be met.
2. Organisation culture: CSA impacts the organisational culture. Based on the organisational culture, the management should decide on the approach of CSA.
3. Use: The result of CSA can be used for internal audit purpose.
4. Process: The management should decide on
 - Framework

- The tools and techniques to be used
- Documentation
- Report format

Internal audit: CSA process can be implemented either by internal auditors or operational managers. There is a difference of opinion among CSA practitioners as to who should implement it. Some believe that the presence of internal auditors in the meetings is by itself an oversight control while others feel that only the operational managers can effectively perform it.

Advantages

1. Early detection of risks.
2. Facilitates development of action plans that help in guarding against business risks.
3. Costly and ineffective controls are eliminated or reduced.
4. Identifies risky areas where controls have to be developed.
5. Evaluation of existing controls.
6. Emphasises on the managerial responsibility for development and monitoring of internal control.

Pitfalls

The success of CSA depends on culture of the organisation, project leader and the skills of the people involved in CSA. But there are inherent pitfalls viz.

1. Recruiting wrong personnel.
2. Generalisation of the planning process.
3. Its application on big projects and setting higher goals.
4. Lack of management support.
5. Narrowing the focus of CSA's effectiveness.

Overcoming the pitfalls

1. Recruitment: The right person should be recruited. The person should possess good conversational skills, should be a good listener and a good coach. He must be in a position to structure loosely jointed information, concepts and ideas.
2. Generalisation of the process: The process should be well defined. It should include planning, structuring, documentation and follow up.
3. Application on big projects: Often the management starts applying CSA on big projects and by setting very high goals. The management lacks the knowledge and experience and hence the project fails. The CSA should first be implemented on a small scale and eventually the scope should be enhanced.
4. Management support: The implementation of CSA requires the support of all personnel involved.
5. Narrow focus on controls: The effective implementation of CSA requires focus on operating procedures, ethics and objectives. The focus should not be limited to financial and other controls that are concrete and measurable.

Conclusion

CSA is a vital tool for auditors and management. If used effectively it helps in identifying the strengths and weakness of the organisation.

Answer: [a] Generalisation of the planning process

Module:1

Reference No:M1012

Question: Which of the following are considered while determining the sensitivity of information -

- [a] Availability and integrity
- [b] Integrity and Confidentiality
- [c] Availability and Confidentiality
- [d] Availability, Integrity and Confidentiality

Module 1 - Sensitivity of Information

While planning for information security, it is very important to understand the various types of information handled by the system. In addition, the importance of information should also be determined to decide on the security procedures that are to be implemented for it. Information refers to all the data that is stored, processed or transmitted by the system. Analysing the importance and sensitivity of information forms the basis of effective risk management. Understanding the sensitivity of information is crucial for

- Analysts/programmers who design security controls
- Internal and external auditors who evaluate security measures
- Managers who decide on the level of security to be implemented

Organisations should decide on the level of laws, regulations and policies that form guidelines for the security plan of the organisation. An example of such a policy is the Information Privacy Policy where an organisation specifies the types of information that employees cannot disclose, and the action that the organisation can take if an employee violates the privacy policy.

The meaning of sensitivity

Information as well as Information systems have different life cycles. The process for assessing the sensitivity of information should be done at the beginning of the lifecycle and should be monitored at every stage. Sensitivity of information is assessed based on the following requirements -

- Availability
- Integrity
- Confidentiality

Performing an analysis of the above mentioned requirements helps in determining the value of the system, and is a very important factor for risk management. The system needs security due to following reasons -

Confidentiality - It refers to the non-disclosure of information, which is restricted to concerned parties. The system may also contain information that should be protected from unauthorised access. Personal information of employees, business information such as business plans etc are examples of confidential information that needs to be protected.

Integrity - It refers to certain types of information that should be protected from unauthorised and unintentional modifications. Financial transactions are an example of such information. For instance in a financial transaction, where A has transferred \$1000 to B and an unauthorised person changes the amount or the name of the party, then the information has lost its integrity. Therefore the need to safeguard such information arises.

Availability - This refers to information that should not be lost during a given time frame. For instance, a database of customers contains information that should be protected from being lost, otherwise problems in client servicing can arise.

Organisations should analyse the information and protect it based on at least one of the above three aspects. They should further analyse the kind of protection that information requires and find the most cost-effective option. The type of protection required usually depends upon the importance of information and the environment in which it is processed. All information that is evaluated on the three factors (confidentiality, integrity and availability) can be classified into -

- High protection requirement - Critical for the system
- Medium protection requirement - Important for the system but not top priority
- Low protection requirement - A certain amount of security required but not as much as the above two categories

Conclusion

Once the sensitivity of information is identified, adequate protection measures can be taken thereafter. n.

Answer: [d] Availability, Integrity and Confidentiality.

Module:1

Reference No:M1013

Question: Which of the following is not a component of audit risk?

- [a] Inherent risk
- [b] Control risk
- [c] Detection risk
- [d] Restrictive risk

Module 1 - Audit Risk

Risk that the auditor may assign to an incorrect audit opinion is called audit risk. It has two aspects -

- 1) The risk associated when an auditor makes an incorrect conclusion based on the findings
- 2) The risk associated when an auditor overlooks an error

Components

The three components of audit risk are -

- Inherent Risk (IR)
- Control Risk (CR)
- Detection Risk (DR)

Inherent risk - Inherent risk can occur either alone or in combination with other errors, in the absence of internal controls. For instance, inherent risks related to operating system security are -

- Incorrect documentation or leakage of information
- Change in /intrusion of data or programs
- Security lapses

Usually, the inherent risk in an IT audit is high because an error in one IT system may affect other systems as well.

Control risk - Control risk is an error that

- Comes under the purview of the audit
- Could be present either alone, or in combination with other errors
- Cannot be prevented/noticed and corrected in time by the internal control system

For instance, the internal control system may specify a procedure to manually review computer logs. However, it may not be carried out, as the numbers of logs is generally very high. In such a case, the control risk is very high. On the other hand, in cases where the review is automated, the control risk is very low.

An Information System Auditor checks whether internal control procedures are relevant, effective and functioning properly. If he finds that they are not appropriate, then the auditor assesses the control risk to be very high.

Detection risk - The risk associated with the audit procedures that have been adopted -

- An auditor may not detect an error
- It could be present either alone or in combination with other errors

For instance, detection risk in administrative software is high, as there is a large number of log entries, and logs for the entire audit period are often not available.

Levels of risk

There are two levels of audit risks -

Acceptable level- Risk associated with any error in the information system that is acceptable by the auditor.

Achievable level- Risk associated with the fact that the information system will contain errors. Since it is an ex-ante concept, it is referred to as achievable level of audit risk rather than achieved level of audit risk. In other words it is the estimated level of inherent, control and detection risk.

The aim of the auditor should be to achieve an acceptable level of audit risk.

Answer: [d] Restrictive risk.

Module:1

Reference No:M1014

Question: The HR policy of a company should state that

- [a] Employees should take leave
- [b] If the employee has not taken leave, he should be given an incentive
- [c] Employees should be forced to go on leave for a few days
- [d] Employees should take leave only when they have some important personal work

Module 1 - The Management's Guidelines on the Security Program - Part 3

The security program reflects the commitment of the senior management towards security management, planning and security controls. A security program is a framework of a continuous cycle of activities performed to assessing risks. It also helps in developing and implementing security procedures that address these risks, and monitoring the effectiveness of procedures that address them.

This is last in the series on the management's guidelines on security program.

Awareness of the security policy and program: Merely creating and documenting a security policy does not serve any purpose.. For effective implementation, the security policy should be communicated to all users, and they should be aware of the ways in which they can contribute to it.

- Employees should be aware that the policy and document exists
- That a program exists for training new employees and contractors
- That employees and contractors receive periodic training
- That employees are made aware of security practices related to availability, confidentiality and integrity
- That the security policy is circulated to all the employees

Responding to incidents: All incidents that adversely affect the functioning of a company must be immediately reported so that corrective measures can be taken in time.

- An environment should exist in which users can easily report such incidents
- A response team should exist to handle incidents reported by users
- The Roles and responsibilities of teams should be defined. Team members should have the required knowledge, skills and abilities
- The head office, security groups and law enforcement agencies should be identified and a response team contact them in case there is a need to do so
- The response team should be familiar with all potential security threats that can arise and update themselves with the latest information on them
- A procedure should exist for systematic investigation of security threats and incidents
- If an incident receives media attention, then the response teams are required to contact the organisation's Public Relations Office

The HR policy: It addresses all issues related to hiring, transfer and termination procedures . The HR policy also specifies the procedures to be followed for dealing with employees. If the procedure is followed as recommended by the policy, it can minimise the chances of fraudulent persons entering the organisation and damaging the assets of the company.

Before appointment

- The references provided by the employees must be contacted and the backgrounds should be checked
- The employee must sign the security agreement
- The HR policy should address all issues related to security

On the job

- There should be rotation of jobs
- All the employees must be forced to go on leave for a few days
- When the employee goes on leave, his job should be temporarily assigned to another employee

Termination and transfer

- The policy should state that an exit interview should be conducted when an employee is terminated
- When leaving the company, all the employees (whether terminated or transferred) should return articles that belong to the company like keys, identification cards, passes etc.
- The management should be informed about the termination and transfer of employees, and the IDs and passwords of such persons should be revoked
- Terminated employees should be made to sign a contract for non-disclosure of confidential information
- Timely action should be taken regarding the transfer or termination of employees

Answer: [c] Employees should be forced to take leave for a few days

Module:1

Reference No:M1015

Question: Which of the following is 'TRUE' with regards to the IT audit report?

- [a] The auditor should take into consideration the subsequent events
- [b] The auditor should issue the report to all interested parties
- [c] The report need not touch upon standards and the internal control of the organisation
- [d] The auditor should state in his report that all his recommendations should be implemented

Module 1 - Audit Report

The audit report is the final step in the audit process. The report of the auditor is formal written communication in which the auditor states his opinion and the suggestions.

Users: The auditor should first recognise the users of the report and their requirements. The users may be the auditee, their representatives, Board of Directors and the government.

Purpose: The main purpose of the report is to provide a clear picture of the functioning of the organisation including the weak areas and measures to overcome them. The report conveys whether the standards are being met and internal controls are functioning as desired.

Form: The report may be oral or written. The written report should have a title, and should be signed and dated. Oral reports are ideal for reporting minor findings that do not have any significant impact and does not require management's attention. Oral reports are normally used in cases where immediate action is required. Irrespective of the media, reports at all times should have a formal authentication.

Scope: The report should state the scope of audit work performed, the period after which it is to be reviewed, the areas that are subject to audit and the limitations if any. Each functional area that has been subject to audit is evaluated to determine the adequacy, efficiency, effectiveness and quality of ongoing operations. The auditor should make a mention of areas that are adequate and effective and express his satisfaction in the report. But if he finds the controls or the functioning ineffective or inadequate he should qualify them in the report.

Audit findings: When there is a considerable difference between the expectations and findings, the auditor must gauge the significance of the difference and give a written report. Marginal differences however can be discussed orally. The audit findings that need qualification should include a statement on the findings, the cause, its impact and the recommendation thereof. Recommendation: Inability to obtain sufficient information on each element can have a bearing on the report and the recommendations. For such areas the

auditor may state in his report, the general recommendations for approaching and tackling the problem.
Conclusion: The auditor may include a conclusion in his report when he considers it appropriate. The conclusion may be based on the overall opinion of the areas that were subject to audit or on a specific area.

Subsequent events: Subsequent events are those that arise after the completion of audit and before the issuance of audit report, and require the auditor to make changes in his findings, recommendations or conclusion. For example, insolvency of a major customer.

Distribution of report: The report should be distributed to those identified for distribution and must mention that it is for their information and use. Where any restrictions are placed on the distribution the same must be stated in the audit report.

Timeliness: The report should be issued on time for it to be effective. The purpose of the report will be lost if it is issued after a considerable period on completion of audit. Any significant findings that require an immediate action may be discussed with the management before issuing the report.

Follow up: The auditor to ensure that the management takes an action on the recommendations stated in the report, may request the management to respond in writing. The auditor may evaluate the response to satisfy that the actions taken are as desired.

Answer: [a] The auditor should take into consideration the subsequent events

Module:1

Reference No:M1017

Question: Which of the following requires the creation of a dummy entity for Concurrent Auditing Techniques?

- [a] Snapshot/ Extended Record
- [b] Continuous and Intermittent Simulation (CIS)
- [c] Integrated Test Facility (ITF)
- [d] System Control Audit Review File (SCARF)

Module 1 - Concurrent Auditing Techniques

Introduction

For an effective audit, the auditor needs to have an audit trail of all the transactions that have been conducted. In a traditional environment, an audit trail exists naturally. However, in a computerised environment where paper work is less, the auditor needs to adjust audit procedures to compensate for the lack of a paper audit trail.

“What is an audit trail?”

An Audit trail consists of a series of documents that have a record of the sequence of events and authorisation of a transaction right from the initial recording stage to final postings. In a computerised environment, audit trail records show which system has been accessed, and what operations have been performed during a given period of time.

In the traditional audit, the controls are not very effective. They really do not help in preventing or detecting a mistake, as the effectiveness of controls is verified ex-post. Therefore the auditor relies on substantive procedures. In a computerised environment, audit trails are followed to assure that controls are in place and operating as desired. To verify this, auditors use concurrent auditing techniques.

Concurrent Auditing Techniques

Whenever audit trails are missing or when the auditor does not want to rely on the audit trails, the technique of concurrent auditing comes into use. Concurrent auditing techniques collect evidence as transactions are processed. It is used when the audited information is required on a more timely basis. Concurrent audit techniques can be used for compliance and substantive testing. There are a variety of concurrent audit techniques. The following are few of them-

Integrated Test Facility (ITF):

In this method, a dummy entity is created and the data is processed for verifying the authenticity, accuracy and completeness of a transaction. Data that can be used may be actual data or artificial data created by the auditor. After the processing is completed, the auditor compares the output with the expected result. The dummy records are later removed. However, the issue that arises is whether real or artificial data should be used or not.

Snapshot/ Extended Record:

In this method, pre and post transaction images are captured by the software during processing. They are used by applications that perform important processes. Individual records may be stored for transactions or snapshots that are later reviewed by the auditor. This method can be used in conjunction with ITF.

System Control Audit Review File (SCARF):

In this method audit software modules are embedded in the production system to continuously monitor transactions. The information is collected and transferred to a special SCARF file for the auditors' review.

Continuous and intermittent simulation (CIS):

This method is a variation of the above method. The audit software modules are embedded in the database system. The transactions that are of interest are trapped. The results of trapped transactions after the processing are compared with the results of the database processing by the auditor.

Disadvantages of Concurrent Auditing Techniques:

- The result of concurrent audit techniques depends on the expertise of the auditor.
- Development and operational costs are high.
- It requires the support of systems personnel
- The technique is sensitive to system changes and can be implemented only if there is a stable environment.

Answer: [c] Integrated test Facility (ITF)

Module:1

Reference No:M1018

Question: Which of the following is not true with regard to the establishment of a security management structure?

- [a] Security management should have authority in accordance with the responsibility
- [b] Security management should have the overall responsibility of security
- [c] Security management structure should be approved by all the employees
- [d] Security management should have the required independence

Module 1 - Management Guideline on Security Program - Part 2

Security program reflects the commitment of the senior management for security management, planning and security controls. The security program is a framework of continuous cycle of activities for assessing risks, developing and implementing security procedures to address the risks and monitor the effectiveness of the procedures in addressing the risks.

This is second of three part series on security program.

Establishment of security management structure: Without a properly designed organisation structure for security implementation and management there will be chaos and no security personnel will know his position and the responsibilities attached to his position. Everyone will think that it is others duties to perform and eventually there would be a security lapse.

The personnel will not know whom to report when there are strong violations and the decisions that should be taken. The objectives are

- Security management structure has been identified
- It is documented
- Security manager is appointed
- Security manager reports to the top management
- Security management has the required independence
- Security management has authority in accordance with the responsibility
- Security management has the overall responsibility of security
- There exists an optimal coordination, communication and liaison between the IT and the security structure
- Adequate resources are allocated for the development and implementation of the policies, standards, procedures and security awareness program.

Security policy is documented and approved:

- Security policy has been created
- Policy includes the security for all the functions in the organisation
- Policy specifies the purpose and objective, and management structure
- Policy adheres to the overall business objectives
- Policy is approved by all the departments in the company
- Policy provides for the preventive measures, identification of irregularities, limitation of losses and timely restoration of activities
- Responsibility of the following are defined
 - Owners of data, equipment and software
 - Users
 - Management
 - Security personnel

Basic security features are implemented: The policy should specify the basic features that should be implemented. This features relate to the physical security, logical security and other general controls.

- Security related equipment - hardware, software and all other equipments are secured
- Security design is prepared and the same is kept confidential
- Access is on 'need to know basis'
- Access rights that are granted to the users are reviewed on periodical basis
- Procedure exists for granting the access rights
- The security violations are immediately reported to the administrator
- Log is maintained for recording all security violations and the log is reviewed by responsible official
- Anti-virus software is installed
- Adequate measures are taken to ensure that only authorised software is in use and no unauthorised software is installed on the system
- Personnel are well informed on whom to contact when the virus is infected or the systems are not working properly
- The data files, software and related documents are adequately backed up and stored at on-site as well as at off-site
- Security and other related logs are maintained for a reasonable period of time

Answer: [c] Security management structure should be approved by all the employees

Module:1

Reference No:M1019

Question: Which of the following is not a method of Control Self Assessment (CSA)?

- [a] Delphi technique
- [b] Interview technique
- [c] Interactive workshop
- [d] Control guide

Module 1 - Control Self Assessment Methods

Control Self Assessment (CSA) is being implemented in a number of countries for the assessment of internal control. The main purpose of the implementation is the legislative and government regulations framed by these countries.

CSA is the independent verification of the adequacy of controls, in which the management takes the full responsibility for the internal controls through planning and operating a control self-assessment process.

Methods:

There are six methods of CSA. Some methods are more mechanical which require less of human intervention while others are behavioral requiring more of human intervention. A number of software and hardware aids are now available that aid in CSA. We shall now discuss each of the six methods:

1. **ICQ Self Audit:** Internal Control Questionnaire (ICQ) is a list of questions that are used by the auditor to obtain an understanding of the internal control. Some auditor fill up the questionnaire based on his observation and interviews during the preliminary phase of audit while others require the management to fill it as a form of self audit. The questions have to replied in Yes, No or Not

Applicable. Where the answer is in 'No' an explanation is required to be given. For the success of the results of ICQ

- It must be prepared with the assistance of management
 - Risk assessment should be used to identify the areas to be included in the questionnaire
 - Goals and objectives of company should be identified
 - Obstacles that are faced by the company or may be faced by the company should be highlighted
 - Ways to overcome the above should be identified
 - Alteration or making changes to ICQ, if the customer has any problems in filling it up
2. Customised Questionnaires: Customized questionnaire is similar to ICQ. In customized questionnaire the questions are customised to comply with laws and regulations and the questions are to be answered either in Yes or No.
 3. Control guides: The auditors and/or controllers for the purpose of internal financial controls use control guides or the internal control workbooks. They contain the description of the expected set of internal controls that should be present in the particular operation. The workbooks deal with the operations, the risks that are present in the operations and controls that should be present to mitigate or eliminate those risks.
 4. Interview techniques: In this method the senior management are interviewed on various issues of the company. The advantage of this method is that brings about interaction between the auditor and the management, unlike other methods where the forms are required to be filled and mailed to the auditors.
 5. Control Model Workshops or Control Design Workshop: This method is developed by Tim Leech and MCS Consulting. The management and staff are trained to focus and deal with assessing, managing and reporting on the internal controls through control design models. A facilitator transfers the knowledge to work group to help it in assessing controls and risks.
 6. Interactive workshops: Paul Makosz of PDK Consulting developed this method. In this method the facilitator draws out the information during the workshop and the management owns the issue of internal controls and problems related to it throughout the workshop.

Answer: [a] Delphi technique

Module:1

Reference No:M1020

Question: Which of the following is not the objective of the establishment of security management structure?

- [a] Organisation management structure is identified
- [b] Security management has the required independence
- [c] There exists an optimal coordination, and communication between the IT and the security structure
- [d] Security management has the overall responsibility of security

Module 1 - Audit of Security Program

Security program reflects the commitment of the senior management for security management, planning and security controls. The security program is a framework of continuous cycle of activities of assessing risks, developing and implementing security procedures to address the risks and monitor the effectiveness of the procedures in addressing the risks.

Assessment of risk and development of security plans: The auditor should

- Review risk assessment policies
- Review recent high level risk assessment
- Ascertain whether the management has approved the results of risk assessment
- Review Security plan
- Determine that the security plan has been approved by a responsible official
- Interview security manager
- Identify the person who has performed the risk assessment and assess his objectivity
- Identify the person who has reviewed the results of risk assessment and assess his objectivity

Incorporation of security measures into new or modified systems and processes:

- Review the process of defining the security measures in new or modified systems and processes
- Interview managers of user department and the security officer
- Review the security requirements for certain departments
- Review the documents giving approval for the security measures that are to be implemented
- Review the test plans to ascertain that the security measures were tested

Documentation, approval and maintenance of security program:

- Review security program
- Ascertain whether all the major activities are covered in the program
- Verify if any additional activities are included and the rationale behind their inclusion
- Ascertain whether the program is reviewed periodically
- Determine the date when it was last updated

Establishment of security management structure:

- Review the organizational structure
- Review the security management job description
- Identify the security manager
- Interview the security management personnel
- Compare the personnel records of the security personnel with their job description

Security policy is documented and approved:

- Review the policy
- Review all documents relating to the policy
- Interview the persons responsible for implementation of the policy

Basic security features are implemented:

- Interview the security manager and obtain from him the documents authorizing access to the system
- Identify the staff who are allowed access to the security related equipments and confirm that they have the access rights
- The places where the security equipments are maintained should be located, a tour should be made of the place to identify the controls which exist and observe the equipments to make sure that there are no signs of tampering
- Confirm whether the security logs are maintained and that the same have been reviewed
- Review the security violation reports and the resolutions
- Ascertain whether a procedure exists for analyzing and correcting systems impacted by malicious software

- Determine whether the backups of data files, software and related documents is maintained at on-site and off-site by reviewing the backup log
- Identify the off-site location and tour both the on-site and off-site
- Ascertain that the procedures exist to restrict access to the above
- Verify whether access to the facilities is restricted and the security measures are implemented
- Confirm whether the visitor log and card pass log is maintained
- Review the above log and assess that the procedure prescribed is complied with

Awareness of the security policy and program:

- Review the material available for training the employees
- Review the process of distributing the policy
- Confirm whether the policy has been distributed to all the employees
- Interview the personnel to understand their awareness of the policy

Responding to incidents:

- The security manager, response team members and users should be interviewed
- Documents relating to incidents handling activities must be reviewed
- Qualifications of the response team members must be determined
- Interview the response team to know their level of awareness about the current security threats
- Process of responding to incidents must be reviewed

HR policy:

- The auditor should review the HR policy
- The policies on confidentiality and security arrangements, job rotations and the termination and transfer procedures should be reviewed
- It should be assured that the HR policy is being followed
- In case of new recruitments confirm whether the background was checked and the references contacted
- Where the position of the company is considered as sensitive, inspect the personal records and confirm that the background was investigated before appointing the person on such post
- Personnel records should be reviewed to confirm that all the employees have gone on a vacation or sick leave in the previous year
- Determine who performed the job of the person who has gone on vacation
- It should be confirmed that the same employee does not work for a long duration on one job and his task is rotated after a reasonable period of time on one job
- Review certain documents to confirm that the termination and transfer of employee is as per procedure specified in the policy

The system generated list of users should be obtained and the same should be compared with the list obtained from the personnel to confirm that the log in ID and password of terminated or transferred employees are deleted

Answer: [a] Organisation management structure is identified

Module:1

Reference No:M1021

Question: The feasibility study is conducted after _____ phase.

- [a] Business requirement
- [b] Need/ user request
- [c] Design specification
- [d] Program specification

Module 1 - Audit of System Development Life Cycle - Part 1

System development life cycle (SDLC) is used to develop or modify the application systems. The life cycle starts when there is a need for some application. The proposal should pass through feasibility study, design and development, testing, implementation, system acceptance and approval, post implementation review and maintenance. The roles and responsibilities for design, development and maintenance should be defined so as to ensure a smooth progress.

The auditor may either participate in the development process or may conduct an ex-post review. When an auditor participates in the development of application he should ensure that his independence is in no way affected. During the course of his audit, it must be ensured that the new or revised application system meets the company's needs, the internal controls are adequate and meet the objectives of the company and that the application is properly implemented.

In this article we discuss in detail the various phases of SDLC where the auditor must focus his attention.

Need/ User request phase: The user request is initiated by the user of the application system and not by the software development group. The auditor should review whether the need has been approved by steering committee or well constituted project committee. User request form should include details regarding the project objectives, details of users and the way they will use, the criticality of the project and the time frame within which the project should be completed. Auditor should check that an appropriate authority signs such a document.

Feasibility study: It is performed to take a decision on whether to accept the request or not. During this phase different alternatives are evaluated and one of the alternative is selected for developing the request. The auditor should determine whether the following have been considered in the feasibility study:

- Impact on the existing environment
- Project start up and delay factors
- Resources that will be required both for development and maintenance
- Costs that will be incurred and the benefit to be derived from developing the request
- Risks associated with the development

Business Requirement specification: Primarily, software is developed to satisfy a particular need/s of function. The phase identifies the business functions that are supported by the software request. The auditor should confirm whether the following have been considered in the business requirement specification

- The business functions, which the system will be required to support
- Whether it is batch processing or on-line processing
- Response time that is required for on-line processing and turnaround time for batch processing
- Functional relations i.e. the relations and dependencies among the various components of the application
- Security requirements
- Data retention requirements
- Output distribution requirements
- Expected transaction volumes

Answer: [b] Need/ user request

Module:1

Reference No:M1022

Question: In System Development Life Cycle (SDLC) the functional specification are translated into the logical and physical design during _____ stage.

- [a] Functional specification
- [b] Program specification
- [c] Detailed design specification
- [d] Business requirement specification

Module 1 - Audit of System Development Life Cycle - Part 2

System development life cycle (SDLC) is used to develop or modify the application systems. The life cycle starts when there is a need for some application.

This is the second of a four part series on audit of SDLC. In this article we discuss the functional specifications, detailed design specification and program specification related to audit of SDLC.

Functional specifications: The business specifications are transposed to functional requirements in this phase. It entails the analysis of business requirements to produce a preliminary design of the proposed system. The specifications are from the users perspective, as the technical deliverables required for the program is not developed at this stage. The audit in this phase should determine whether the following are included in the functional specification

- Data flow diagrams to trace the data through all its processing points
- Screen definitions defining the input fields and any checks that will be used
- Data definitions, the relationship, naming conventions and the like
- Inputs including the source, the types of data and description of data
- Report definitions describing the report, the data that should be contained in the report and the users of the report
- Service level agreements defining the schedule of processing time, deadlines for input and report distribution
- Capacity requirements - the volume of transactions and the expected growth
- Conversion requirements stating the method used to create data on the new system and method for reconciling data
- Control and security requirements, which includes the input edit requirements and audit trails for critical data from the point of its origin
- System interface requirements - interfaces to other systems
- Specifying backup and its frequency, restart and recovery process
- Contingency requirements containing the analysis of unavailability of the application before the business is affected
- Hardware requirements

Detailed Design Specification: The functional specifications are translated into the logical and physical design. The application development group develops the detailed design. If any changes are made in the functionality during the design phase, then the functional specification should be updated and reviewed by the user. The auditor should determine whether the following are included in the detailed design specification

- Database requirements including detailed relationship between data elements
- File requirements giving the description of each file, file access method, list of fields within a record, data attributes, anticipated number of records
- System flow diagram containing the sequential flow of diagrams that are executed and the relationship between input and output
- Program requirements including the programs used and their purpose, description of formulas and calculations and the interrelationship between other programs
- System operational requirements containing the job streams, backup and recovery procedures for the application, system start up and shut down procedures
- Screen design including the fields in each screen and the purpose of each field, description of how screen is triggered, logical flow of the screens by specifying screens that pull other screen in a flow
- Reports design with data contained in each fields of the report and each data field should be defined in terms of how the result was derived

Program specification: They are developed to address the content of each input and output as well as description of the program logic. It is developed before the commencement of programming. It provides the programmer with a thought process to determine the steps to code the required programs. The auditor should determine whether the following are included in the program specification

- Description of all input and output
- Description of all programs in terms of the logic

Answer: [c] Detailed design specification

Module:1

Reference No:M1023

Question: In the System Development life Cycle (SDLC) the user should be involved in (1) design (2) development (3) implementation of new system and changes to the existing system. Which of the following is true?

- [a] 1, 2
- [b] 2, 3
- [c] 1, 3
- [d] 1, 2, 3

Module 1 - Audit of System Development Life Cycle - Part 3

System development life cycle (SDLC) is used to develop or modify the application systems. The auditor during the course of his audit ensures that the new or revised application system meets the company's needs, the internal controls are adequate and meet the objectives of the company and that the application is properly implemented.

This is the concluding part of the series on audit of SDLC. In this article we discuss the acceptance testing, parallel test, installation plan and post implementation review of audit of SDLC.

Acceptance testing: The testing is performed in a controlled environment and simulates the production environment. The user conducts the test, as he is more fluent in determining whether the software meets the requirement of the business. The production data is used for testing. The purpose of this test is to

- Check for all error handling conditions

- Ensure processing accuracy
- Ensure that audit trails record accurately all required data

The auditor should ensure that:

- Acceptance test plan contains the criteria given below
 - Transaction processing i.e. output generation, file maintenance, inquiry capability
 - System processing constraints
 - Error handling routines
 - Stress tests
 - Input/ output verification
- Programmers do not have the access to update the data files, which are used for test. Programs that are executed during the acceptance test are contained in the acceptance test library and not on individual programmers library
- Only after the plans are tested, should they be moved in the production environment.

Parallel test: Parallel testing is usually done in the production environment when the system to be implemented is a standalone process. But in case the system is not autonomous with respect to the rest of the system the testing should be performed in a pre-production environment. The data is later converted to the production system during the implementation and conversion stage. Parallel testing is most appropriate when

- Manual system is to be converted to an automated system
- When an application is to be rewritten which does not alter the functionality of the system

The auditor should ensure that the test plan contains

- Methods to be used for input and verification of results
- Timeframe within which the test should be performed
- Process for documentation of the results

Installation plan: The plan ensures that the system is functioning within the production environment. The auditor should determine that the following are included in the installation plan

- Steps for monitoring the initial stages of production processing
- Notifying the appropriate individuals of the date when the conversion from one system to another is to take place
- Timeframe within which the processing can be switched back to the old system if the new system fails
- Steps for fallback to the old system
- Process for shutting down the old system

Post implementation review: The review is performed to determine whether the system is functioning as desired and meeting the requirements of the business. It also discloses problems within the SDLC. An emergency change, maintenance request or an enhancement request can disclose the problem in SDLC. The auditor should ensure that

- Process exists for soliciting user feedback on the overall effectiveness of the system
- User surveys are performed to determine if the system is operating at the acceptable level
- Emergency changes and maintenance request can be traced to the original software request to determine whether it has attributed to breakdown in the SDLC

Post implementation review may not be required for all the projects. Only installation of large systems will be subject to post implementation review.

To sum up

The auditor should ensure that

- An approved methodology is used for developing systems and for designing controls into the system
- The user is involved in the design, development and implementation of new system and changes to the existing system
- Systems development is subject to budgetary controls
- New systems are developed only after a need analysis
- Systems are not implemented until they are adequately tested and approved.
- New and amended applications are moved to the production environment only after they are tested
- New systems have been subject to post implementation review
- Testing and training is done on separate development systems because there is a risk of production data being corrupted by failed testing.

Answer: [d] 1, 2, 3

Module : 1

Reference No : M1024

Question: User controls are designed to ensure that data collected and entered into the system is

- [a] Authorised
- [b] Accurate
- [c] Complete
- [d] All of the above

Module 1 - Audit of Application Controls - An Overview Part 1

The auditor during the scope of his work is required to review the operation of the application system. The auditor can conduct this review when the system is being developed or after it is implemented. While carrying out the audit, he wants an assurance that there are adequate controls over the data. The level of controls depends on the sensitivity of data and the risk involved in incorrect or unauthorised processing of data.

There should be adequate controls to ensure that data entered is accurate, complete and authorised. Ensuring this is the responsibility of user department. Besides this, there should be controls over input, processing, output and the data that is stored in the application.

There can be no specific rule about the control mechanisms that should be present in the application, which the auditor should look for. He should obtain an understanding of data processing application by reviewing the related documents and by discussing the same with IT staff and users.

In this article we discuss some general principles about the controls that are usually present in the application system.

User controls: The controls ensure that the data collected and entered into the system is authorised, accurate, complete and correct. The user department implements the controls. The auditor should ensure that there exists a proper control over the source documents before and after they are entered in the

system. Once entered, the access should be restricted to authorised individuals and for this purpose logical access controls should be implemented. All the data that has been entered should have been checked with the source data prior to it being processed by the system.

Input controls: Input controls are programmed into the application system to ensure that the data is accurate and complete. They are performed as the data is entered in the application system. The auditor should ensure that the application system has the following features

Pre-defined format for data to be entered into the input fields. . For example, the input field for date should be checked for DD/MM/YYYY format

Relationships, if any, between the data items have been defined

All data that could be computed with other data input should be automated and computed and not entered again. For example, the total price should be calculated automatically by the system when the user enters the unit price and the number of items

Check digit or other similar check is used for verification of key data items to ensure that the data has been entered correctly. For example a check digit is added to an account number so it can be checked for accuracy when it is used

- Verification for accuracy of key data items of a transaction unless which, processing should not be allowed
- Specification of default value where a value in the data field does not change
- Notifying the user when duplicate entries are being made
- Unique reference number for every transaction that is entered
- Verification of sensitive data by a second user.

Answer: [d] All of the above

Module:1

Reference No:M1025

Question: _____ tests individual programs.

- [a] Unit testing
- [b] System testing
- [c] Acceptance testing
- [d] Parallel testing

Module 1 - Audit of SDLC - Part 3

System development life cycle (SDLC) is used to develop or modify the application systems. The auditor may either participate in the development process or they may conduct an ex-post review.

This is third of four part series on audit of SDLC. In this article we discuss data conversion plan, unit testing and system testing.

Data conversion plan: These plans meant for accurate conversion of data is used only when there is a danger that the software may change the presentation of data. It is a prelude to the parallel test plan. It must be ensured by the auditor that the following are included in the conversion plan

- Method to be used for converting the data

- Procedures that are required for converting the data
- Cutover requirements i.e. point at which data is to be converted
- Process to verify the proper conversion of data
- Process to be used for executing the conversion programs from a secured library

The data can be converted using the following methods

- Data which is re-input into the new system
- Data which is massaged via conversion programs to meet the current system's input requirements
- Data which does not require any alteration

The following audit criteria must be met by each method

1. For the data which is re-input into the new system, it should be ensured that

- There exists a verification function for such data
- Conversion programs have been tested
- Process exists to ensure that input file captured the data correctly

2. For the data which is massaged via conversion programs, it should be ensured that

- Conversion programs have been tested
- Transactions converted are verified using the checks - field verification, totals, cross-footing, record size

3. For data that is transferred without any alteration, it should be ensured that

- They are verified using the field verification, totals, cross-footing, record size, bit error checks.

Unit testing: It is the testing of individual programs before they are linked to the entire application. It involves identifying the problems in the program in a standalone environment. It is the testing of the programs. It is performed in a non-frozen environment so that it can be changed during the course of the test. The auditor has to ensure that the following test criteria are included

- File updating, merging, sorting
- Decision logic
- System interfaces
- Invalid transactions and their error handling routines
- Restart and recovery routines
- Stress testing i.e. volume testing
- Error conditions
- Page counters and overflow headers

System testing: System testing is performed only when all the required programs are completed. The test is performed to ensure its functionality. The auditor should ensure the following test criteria in the system development plan.

- Verification of all functions as per the functional and design specification
- Program interfaces
- System interfaces
- Restart and recovery procedures
- Transaction validation and rejection

- Transaction processing cycle
- System performance criteria
- System output generation
- Test data - The data to be used for testing should be specified. It should be ensured that the data covers all the types of test conditions in the program.

Answer: [a] Unit Testing

Module:1

Reference No:M1026

Question: Which of the following need not be emphasised while choosing technology insurance policy?

- [a] Evaluation of the company's exposure to technology risk
- [b] Reading the terms and conditions of the policy carefully
- [c] Not making any assumptions and obtaining clarifications where required
- [d] Focussing on purchasing a general insurance policy

Module 1- Technology Insurance

Most of us insure our homes and business against fire, burglary, floods and the like. But not many of us think of insuring it against computer disaster or what is known as Technology Twisters. Technology twisters that usually strike with little or no warning may cause physical damage. Technology twisters can arise in the form of viruses, hackers, disgruntled employees, poorly drafted technology agreements and any other possible risk pertaining to e-commerce. Hence it is important to adequately insure ourselves against Technology Twisters.

Here is an example to understand the impact of Technology Twister on the business.

Let us suppose that you deal in giving stock tips to the clients. One day your employee disgruntled that he is not earning enough decides to play some mischief. He buys the stock and then convinces the clients to buy it. The prices increase and the employee sells his stock. This will lead to the fall in the prices. This will surely lead to your client suing you. Not only this, even the Stock Exchange Commission will take stringent measures against you. What do you do then? If you do not have a policy or the policy is ambiguous, you will spend most of the time in court just determining the extent of your coverage.

Guidelines for choosing a policy:

Where business relies heavily on technology and use of Internet, it is important to have technology insurance. In developed countries like USA, many insurance companies are offering such policies each of them differing significantly. The following should be kept in mind while choosing a policy:

- Evaluate the company's exposure to technology risk. This may be done either by consulting a technology lawyer or through self-assessment. While carrying out a self-assessment, make sure that the company has a security policy and that it is being enforced in the company. Also assess how the confidential information is being maintained and the persons with access rights and the measures taken by the company from infringing another company's copyright, trademark and patent. The above-mentioned areas are not exhaustive.
- A specific policy on technology insurance should be sought. The general insurance policies do not include technology related incidents in their description of coverage.
- Policy should be read carefully. Do not make any assumptions. Doubts if any must be clarified with the insurance company before the agreement is entered into. Usually we see that the limitations or

exclusions of coverage are given an implicit mention in the terms and conditions of the policy and are very important to the business.

- Last but not the least set aside some money for insurance. Its true that insurance don't come cheap but neither do law suits. To keep the cost of premium down, consider purchasing a policy with the largest deductible you can afford to lose.

Conclusion: Don't cheat yourself by saying that you don't need insurance. If you are using anti-virus software, building powerful firewalls or hesitant to divulge your personal information on the Internet, then you must settle for an insurance policy. As your business progresses the dependence on technology increases. The Technology Twister will affect you without any warning causing greater damage than you can comprehend. Take this threat seriously and handle it as if it were a question of life and death.

Answer: [d] Focussing on purchasing a general insurance policy.

Module:1

Reference No:M1027

Question: User controls are designed to ensure that data collected and entered into the system is

- [a] Authorised
- [b] Accurate
- [c] Complete
- [d] All of the above

Module 1- Audit of Application Controls - An Overview Part 1

The auditor during the scope of his work is required to review the operation of the application system. The auditor can conduct this review when the system is being developed or after it is implemented. While carrying out the audit, he wants an assurance that there are adequate controls over the data. The level of controls depends on the sensitivity of data and the risk involved in incorrect or unauthorised processing of data. There should be adequate controls to ensure that data entered is accurate, complete and authorised. Ensuring this is the responsibility of user department. Besides this, there should be controls over input, processing, output and the data that is stored in the application. There can be no specific rule about the control mechanisms that should be present in the application, which the auditor should look for. He should obtain an understanding of data processing application by reviewing the related documents and by discussing the same with IT staff and users.

In this article we discuss some general principles about the controls that are usually present in the application system.

User controls: The controls ensure that the data collected and entered into the system is authorised, accurate, complete and correct. The user department implements the controls. The auditor should ensure that there exists a proper control over the source documents before and after they are entered in the system. Once entered, the access should be restricted to authorised individuals and for this purpose logical access controls should be implemented. All the data that has been entered should have been checked with the source data prior to it being processed by the system.

Input controls: Input controls are programmed into the application system to ensure that the data is accurate and complete. They are performed as the data is entered in the application system. The auditor should ensure that the application system has the following features

- Pre-defined format for data to be entered into the input fields. For example, the input field for date should be checked for DD/MM/YYYY format
- Relationships, if any, between the data items have been defined
- All data that could be computed with other data input should be automated and computed and not entered again. For example, the total price should be calculated automatically by the system when the user enters the unit price and the number of items
- Check digit or other similar check is used for verification of key data items to ensure that the data has been entered correctly. For example a check digit is added to an account number so it can be checked for accuracy when it is used
- Verification for accuracy of key data items of a transaction unless which, processing should not be allowed
- Specification of default value where a value in the data field does not change
- Notifying the user when duplicate entries are being made
- Unique reference number for every transaction that is entered
- Verification of sensitive data by a second user

Answer: [d] All of the above.

Module:1

Reference No:M1028

Question: Which of the following a company need not prepare or decide upon after appointing an IS auditor?

- [a] Documents related to processes or procedures
- [b] Area of surprise audit
- [c] Letter foregoing legal course of action related to penetration testing
- [d] Number of days the audit should be carried out

Module 1- Preparing for Security Audit - Part 2

This is the concluding article of a two part series on preparing for security audit. In the first article we discussed the parameters for the audit and choosing of the auditor.

Preparation for Audit: After appointing the auditor, the management must ensure that the basic security issues are being addressed by the company such as backups and off site storage of confidential and sensitive data. They have to oversee that user accounts and dial-in, remote access and usage of Internet has some form of control and reporting.

Documentation: Documentation is very important for the auditor as it helps him to understand the processes and procedures. Documents will have to be produced before the auditor during the course of his task. Hence all processes and procedures should be adequately documented. They should be current. Where the documents are missing make a brief note if possible or state that the documents are missing appending to it the timetable giving the time frame within which the documents will be completed.

- **Surprise audit:** The management must decide whether they would like to inform the staff before hand about the audit or conduct a surprise audit. The advantage of the surprise audit is that any discrepancies will be exposed. But it leads to drain of resources. On the other hand if the staff is informed before about the audit they can schedule their work accordingly so that their work is not disturbed due to the arrival of the auditors.
- **Agreement:** The auditor for the purpose of his audit will ask for all the documents which includes policies, procedure manuals, log books and other records which may be related to his audit. The

management must enter into a non-disclosure agreement with the auditor prior to handling any material.

- **Legal course:** Where penetration testing is required the auditors would ask for a letter stating that the company forgoes any recourse, civil or criminal, against the members conducting the penetration test since penetration testers will be violating the law in conducting the test. If the auditors do not ask for such letter it is advisable to check the credentials of the auditor again or to choose another auditor.

Audit Day: At the commencement of the audit, the management must assist and cooperate with the auditors. They should be ready to answer any questions posed by the auditors.

Senior Management: The matters to be informed to the senior management will depend on various factors pertaining to audit. In cases like penetration testing or a letter to be given to the auditor about non-prosecution et al it is better to inform the senior management

Conclusion: Any findings of the audit report should be analysed. The recommendations of the auditor should be implemented wherever possible and actions should be taken to correct the weakness or loopholes that exist in the system.

The audit exercise should be taken seriously and as a necessary part of the security life cycle.

Answer: [d] Number of days the audit should be carried out.

Module:1

Reference No:M1029

Question: The auditor during the course of audit takes into consideration the materiality of the transaction. Which of the following would not be considered by the auditor to assess the materiality in case of non-financial transaction

- [a] Cost of system or operations
- [b] Cost of errors
- [c] Activities supported by system or operations
- [d] Cost of providing physical access controls to the system

Module 1- Materiality

Materiality is an expression that is of relative significance when it involves the company as a whole. Any expression is a material if its omission or error has a bearing on the decision of the users.

Like financial auditors the IS auditors also consider materiality while conducting the audit. The difference between the two audits is that the financial auditor measure materiality in monetary terms while the IS auditors are involved in both monetary and non-monetary areas e.g., physical access controls, logical access controls, password generation and the like.

IS auditors must take into consideration the materiality aspect while planning for and during the course of audit. This helps them to focus on high risk areas and assess the severity of any errors or weakness found.

Assessing Materiality: How does the IS auditor assess as to what is material? An assessment of materiality depends on the professional judgment of the auditor. But while assessing the materiality the auditor should take into consideration the aggregate level of error which the management and appropriate regulatory agencies are ready to accept. He should also take into account the aggregate effect of all insignificant errors or weaknesses.

Financial transactions: In case of financial transactions the IS auditor should consider the value of the assets controlled by the system or the value of the transactions processed to assess materiality.

Non-financial transactions: In case of non-financial transactions the IS auditor may consider the following to assess the materiality.

- Cost of the system or operations. This would include hardware, software, staff, third party services, overheads or a combination of them
- The activities that are supported by the system or operation. If the activities are critical for the business then such activities can be material
- The cost of errors could also affect materiality. The cost of errors could be in terms of lost sales, warranty claims, irrecoverable development costs, rectification cost, health and safety cost and the like
- The number of accesses/ transactions/ inquiries which are processed per period
- Nature, timing and extent of reports prepared and files maintained
- Nature and quantities of materials handled
- Service level agreements
- Penalties in case the legal and contractual requirements are not complied

Penalties if the public health and safety requirements are not complied

The list is not exhaustive. The auditor should consider materiality in all matters that come within his purview while performing the audit.

Planning: During planning stage, the auditor should focus on material controls. Without material controls it cannot be ascertained that the control objectives have been met.

Audit: The assessment of materiality may be different during the planning stages and during the course of audit. This may arise due to change in the auditor's knowledge or change in circumstances as a result of audit.

Reporting: The report of the auditor would include his findings, conclusions and recommendations. The auditor should take into consideration the materiality of errors that are found or which could arise due to weakness in the controls. The auditor may issue the following types of reports:

Unqualified report: The auditor would issue such a report when he is satisfied with the controls i.e. proper controls are in place and there exists no weaknesses in the controls.

Qualified or adverse report: This is issued when the controls are weak and they do not assure that the control objectives will be met.

The auditor may report on the controls that are weak but though not material when the cost of strengthening such controls is low.

Answer: [d] Cost of providing physical access controls to the system.

Module:1

Reference No:M1030

Question: While appointing an auditor to conduct the IS audit the company need not look into _____ of the auditor?

- [a] Legal capability
- [b] Experience
- [c] Proficiency in different computer languages
- [d] Secrecy bond, if penetration test is to be done

Module 1- Preparing for a Security Audit – Part 1

In this article we outline the strategy for preparing a security audit. We shall discuss matters relating to choosing the auditor, establishing the parameters for the audit, issuing the request for services to matters relating to documentation and practices that are to be prepared for inspection during audit. The steps mentioned above should be altered according to the specific businesses requirements.

This is the first of two part series on preparing for security audit.

Parameters for the Audit: The management should establish the parameters of the audit. The parameters that should be decided are as under

- **Boundaries:** The management should decide on the area of business that is to be audited. It may be the IT department or the web site operations. All decisions of the management should be documented and communicated to the auditor.
- **Objective:** The next step is defining the objective of the audit. The objective could be to satisfy the requirement of a trading partner and hence must meet a given standard. It could also be that the audit is required only for the satisfaction of the management to ensure that the security policy defined is being implemented.
- **Validation whether the current procedures are sufficient:** The management must ask itself as to whether they have taken sufficient security measures. This is where the penetration test comes into picture. Many companies are of the opinion that once the penetration testers fix the insecure areas, they become secure. But this is not true. A good penetration test is very difficult to prepare.
- **While carrying out the penetration test the management should decide whether they want**
 - o Black Box testing where penetration testing is similar to how an external cracker would approach.
 - o White Box Testing where the penetration testers mimic a trusted insider who has some knowledge of the systems.
 - o Clear or Crystal Box Testing where penetration testers mimic a trusted insider who has full knowledge of the systems

Choosing the Auditor: The company must choose an auditor for conducting the audit. The auditor can be financial auditor himself if he has a computer audit division or a security professional. The company's internal audit team may be employed for conducting the audit provided the department is authorised to give official, legally binding stamp confirming to the security posture. This can then reflect accountability to the shareholders, trading partners or industry association. Hence it is also necessary to have audit and IT experts in their team.

The management before appointing the auditor should look for the following

- **Legal capability:** Before appointing the auditor management must ensure whether any body or any authority requires the report should be signed by a person holding a particular designation if the report is required to be submitted to such body or authority.
- **Experience:** Check the CV of every person to be associated with the audit. Since the person will be responsible for improving the processes or policies of security he must have good experience.
- **Secrecy bond:** This becomes important when penetration test is to be performed. Here the testers are required to break into the systems or the network. The company should ensure that the persons who are to perform the audit are trust worthy. A bond may be entered into with the auditors to ensure confidentiality of information. In many cases the auditors employ hackers. If the company does not have any reservations the same must be resolved before the auditors are appointed.

Answer: [c] Proficiency in different computer languages.

Module:1

Question: Which of the following is not a characteristic of audit evidence?

- [a] Relevance
- [b] Reliability
- [c] Sufficiency
- [d] Consistency

Module 1- Audit Evidence

During the course of performing an IS (Information Systems) audit, the auditor first gathers information. This information used to meet the audit objectives is referred to as audit evidence. The evidence should be sufficient, reliable, relevant and useful, and should be supported by appropriate analysis and interpretation. The contextual meaning of 'sufficient', 'reliable', 'relevant' and useful is given below

Relevant audit evidence - Audit evidence is considered as relevant, if it is related to the objectives, and supports the conclusions and findings.

Reliable Audit evidence - The evidence is considered as 'reliable', if the auditor considers it valid, factual and objective.

Sufficient Audit evidence - The evidence is considered as 'sufficient', if it is complete, adequate, convincing and leads another auditor to the same conclusions.

Useful Audit evidence - The evidence is considered as 'useful', if it helps the auditor in achieving the objectives.

If the evidence does not meet the above criteria, then he should obtain additional audit evidence.

Planning

Before beginning the audit, the auditor should decide on types of evidence that has to be collected, and their levels of reliability. The quality and reliability of evidence should meet the audit objectives.

For instance, in some cases, audit evidence from a third party is valued more than the evidence provide by an individual from within the organisation. Further, physical evidence is considered more reliable than representations from the organisation.

Different types of audit evidence that an IS auditor may use are -

- Different processes and other physical assets - They may further include -
 - o Checking different activities, property and information system functions such as inventory in offsite storage location and security checks in the computer room.
- Different types of documents whether in print, or in other media include -
 - o Data extractions and analysis
 - o Transaction records
 - o Listing of programs or data
 - o Logs of activity and controls
 - o Documentation of entire system development process

Representations such as -

- o Written policies and procedures
- o System flowcharts
- o Written or oral statements

- Analysis of information such as -

- o Benchmarking IS performance with other organisations
- o Comparison of number of errors between applications, users, transactions over a period of time

Availability of audit evidence

The IS auditor should also assess the nature of evidence he has collected. He should see whether the evidence is available facilitates substantive testing and compliance testing. He should create a back up files so that the original files that contain the evidence cannot be altered.

Gathering of evidence

The auditor should not select the most appropriate procedures for collecting the evidence. He may choose any of the following procedures -

- Inquiry
- Observation
- Inspection
- Confirmation
- Reperformance
- Monitoring

The above procedures can be conducted either through manual audit procedures or with the help of computer assisted audit techniques

Finally, the evidence should be documented properly. In case, the auditor is not able to gather sufficient audit evidence, then he should make it clear.

Answer: [d] Consistency

Module:1

Reference No:M1035

Question: The audit trails are useful to

- [a] Auditors
- [b] Management
- [c] Users
- [d] All of the above

Module 1- Audit of Application controls - An Overview - Part 3

There can be specific rule about the control mechanism that should be present in the application, which the auditor should look for. He should obtain an understanding of how the data is processed by the application by reviewing the related documents and by discussing the same with IT staff and users.

This is the final of three part series on audit of application controls. In this article we cover management trails.

Management trails record all the changes made to the data as it passes through the stages of initiation,

authorisation, input, verification, processing, output and during the recovery procedure. The management trail or the audit trails are not only useful to the auditors but they are also useful to the users and computer specialist. These trails assist the management in monitoring the effectiveness of the controls and for identifying the source of error.

Source documents: The source documents form the first audit trails because the initial step in processing is to enter data from external sources. The auditor during his audit should ensure the following

- **Data preparation:** The source document used for data preparation should be initialled, signed and identify the person responsible preparing the data for input.
- **Processing:** Manual processing which the source document undergoes, their status and current location must be logged.
- **Retention period:** The source documents are retained as they can be used for recovering the data when it is lost or corrupted. Retention period will depend on the sensitivity of the data and on any legal considerations.

Data processed: The audit trail at this stage will be the outcome of the processing the data from the initial stage i.e. as the source document. The auditor should ensure that

- An audit trail is maintained for all processed data so as to enable the user, IT specialist and auditors to trace the data from its origin to the output. The input and output transactions should be logged to an independent file.
- Management trail records should be maintained till the users are satisfied that the processing was authorised, the processing was accurate and complete and is in compliance with the legal requirements.
- The audit trail to assist in error tracking should record the date, time, user and the source terminal.
- All the processed data should have a reference. The reference helps in tracing the information to and from the source of the data.
- The users should be identified with the specific departmental codes. This helps in tracing all input transactions.
- The data that is used to prepare the specific reports must be retained to help in resolving discrepancies that may arise.
- Audit trails that are maintained should be in readable form. Otherwise, software should be available to read the audit trails, analyse them and produce specific reports.
- Exceptional report is generated when a program control is overridden or bypassed.
- For reconstruction of data files and transactions from particular terminals logging facility in the network should be provided.

After the auditor is satisfied that the control mechanism is in place he should verify the control mechanism itself. The verification process of the control mechanism will depend on the application and the technology in use.

Answer: [d] All of the above

Module:1

Reference No:M1036

Question: Output controls ensure that output is accurate, complete and produced when required. The auditor during the course of his audit of output controls does not look into which of the following:

- [a] All pages of the report are numbered consecutively
- [b] Comparison between the actual data totals and totals of record counts is done at regular interval
- [c] Proper procedure for classification of output exists
- [d] Output of test runs and procedure runs are kept separately

Module 1- Audit of Application controls – An Overview – Part 2

There can be specific rules on the control mechanism that should be present in the application, which the auditor should look for. He should obtain an understanding of data process by application by reviewing the related documents and by discussing the same with IT staff and users.

This is the second of a three part series on audit of application controls. In this article we cover

- Processing controls
- Output controls
- Integrity controls

Processing controls: The purpose of this control is to ensure that the processed data is accurate, complete and approved. This is the responsibility of the user department. The auditor should ensure that

- Reconciliation process exists for reconciling the changes that have been made to databases and the transactions which have been input or captured
- Controls exist to ascertain that the processing has been complete when data is entered into system for processing
- Error correction process exists which notifies the user about the processing error and assists them in locating the same.
- Further processing of transaction does not take place when an error occurs.

Output controls: As in other controls the purpose of this control is also to ensure that all output is accurate, complete and produced when required. The controls that the auditor should look for are

- Proper identification of output controls that include people and procedure viz.
 - User department
 - Data preparation
 - Processing period covered
 - Processing program's identification number
 - Title of the report's content
 - Procedure for disposing the report
 - Level of confidentiality
- All the pages of the report are numbered consecutively. End of the report is identified properly.
- In case of sensitive output such as pre-numbered cheques additional sequence numbers are generated. The differences between the beginning and ending pre-printed number and the beginning and ending of computer generated number should agree and if there is any difference the same is reconciled.
- There exists a proper procedure for classification of output based on the level of sensitivity.
- The access to the sensitive data is limited to authorised users.
- Proper procedure exists for disposal of the sensitive information after they have exceeded their retention period.
- Review is done regularly of the reports to eliminate, combine, rearrange and simplify the reports or to add new reports.
- "Nil report" should be produced where there is no output for a particular run.

- Output of test runs and productions runs are kept separately.

Integrity controls: Integrity controls ensure that data is controlled and the integrity of data is maintained. Integrity controls by themselves do not assure for integrity of data. They should be combined with other controls. The auditor should ensure that

- Comparison between the actual data totals and the totals of record counts and significant data item is done at regular intervals and the deviations are reconciled.
- There has been no alteration to data by any means outside the normal processing cycle by comparing the closing and opening daily control totals of data.
- Report controls should be reviewed by the user department on periodical basis and deviations if any are resolved.
- Special utility software is used to examine the databases to look up for hole in the physical data structure or the logical structure

Answer: [b] Comparison between the actual data totals and totals of record counts is done at regular interval

Module:1

Reference No:M1037

Question: Which of the following step forms part of an approach to IT audit

- [a] Review of systems
- [b] User controls
- [c] Compliance testing
- [d] All of the above

Module 1- IT Audit Approach

The approach to audit can be explained with the help of flowchart.

The steps in the audit process are as under:

Review of the systems: The auditor should try to review the system that will include the hardware and software including utilities and the like. This helps the auditor to plan the approach to audit. He should also review the existing and proposed organisation charts of the IT department and the entire organisation. This helps him to have an idea about the lines of authority, job titles, job description, number of employees and the like. When reviewing the hardware he should gather information regarding the configuration, location of communication channels and terminals, peripherals and the like. With regards to software he should obtain information about the system development process and documentation. The auditor at this stage may decide to continue with the audit or withdraw or rely on user's controls.

Evidence collection: Evidence is collected through observation, interview and review of the documents. The auditor at this stage also may decide to continue or withdraw or rely on users controls.

Review of controls: The auditor in order to review the applications may decide to rely on the internal controls. For this purpose he should review both application and management controls. These controls ensure that the development, implementation and the operation of IT proceed in a planned and controlled manner. Management controls are the fundamental controls that cover all application systems. The absence of the management controls is a serious concern for the auditors. They are protective layers around applications and

can be compared to the layers in an onion. When the management controls are weak, it is not worthwhile for the auditor to review and evaluate the application controls. It is therefore necessary for the auditor to first evaluate the management controls. The auditor should identify the causes of loss within the installation and controls that have been established to reduce the potential loss from these causes. He should determine whether the controls that are established reduce the loss to the minimum level.

Compliance testing: Compliance testing is test of controls used by the auditor to obtain audit evidence regarding the effectiveness on controls and their operation during the audit period. Compliance testing is conducted to determine the efficiency of the system. The auditor to determine the reliability of the system may use computer assisted evidence collection techniques eg. test data generators which are used to determine the validity of input programs. On the basis evidence collected on the reliability of individual controls the auditor must evaluate the internal controls.

User controls: When the auditor cannot rely on internal controls he goes in for reviewing and testing of user controls. User controls are also known as compensating controls. Where the control are weak and if the weakness of the control is compensated by the existing of other control then the auditor may not give much importance to the weakness in the control. For example, if the controls are weak over the transit of source of data to the computer facility but if the same is compensated by the reconciliation with the control totals produced as output from application system programs then the auditor may consider the latter as compensatory control.

Substantive testing: The substantive testing helps the auditor to make a final decision on whether substantive losses have occurred or could occur in processing by obtaining sufficient evidence. The auditor usually uses the following types of substantive tests:

- Identification test of erroneous processing
- Tests to assess the quality of data
- Tests to compare data with the physical counts
- Tests to identify inconsistent data
- Confirmation of data with outside sources

Conclusion: The audit approach to IT audit is more or less the same as that of the manual system.

Answer: [d] All of the above.

Explanation: During the evaluation stage, the auditor evaluates only the management's commitment to the policy.

Module:1

Reference No:M1038

Question: Which of the following is true with regard to a computerised environment?

- [a] Separation of duties is not possible
- [b] A clear line of authority and responsibility exists
- [c] Highly skilled persons are not required to develop, modify and operate the system
- [d] Audit trails are not available by default on all software

Module 1- Differences between the manual and IT environment

With the advent of computers in all the spheres of life, auditing is no exception. The auditors too are required to function in a computerised environment and are therefore required to equip themselves with the knowledge of information technology.

In this article we discuss the differences between the manual and IT environment that would be faced by the auditor during the course of his audit.

- **Separation of duties:** In a manual system, incompatible functions are performed by different individuals and supervisor can overlook the functions being performed by different individuals. In the computerised environment this is not possible. For example, the program may be built into the system to reconcile the invoices received from the creditor and to print the cheque for the amount that is due to the creditor. In a computerised environment most of the duties are performed by a software program hence separation of duties will be in a different manner when compared to manual environment. For example a programmer who writes the program should not run and operate the program on a daily basis.
- **Delegation of authority and responsibility:** The management is required to describe a clear line of authority so that the required person can be held responsible for the tasks done by him. In a manual system, the lines of authority and responsibility can be easily defined. But in the computerised environment it becomes difficult as the same resources are shared by a number of users. For example, when a database management system is used, the same data is accessed by a number of users. In this process, the integrity of data is lost. It is not easy to keep track of the person who has corrupted the data and who has corrected the errors. However establishing an audit trail and analysing the same periodically, as to who had modified the data from which terminal and on which date could solve this problem.
- **Competent and trust worthy personnel:** In the manual system the need for competent and trust worthy personnel was not as high as in computerised environment. In the computerised environment small number of individuals are assigned major responsibilities and highly skilled people are required to perform the functions of developing, modifying, maintaining and operating the computer system.
- **Systems of authorisation:** In a manual system the procedure for authorisation can be easily verified by examining the work of the employees. But in computerised environment the same are embedded in the program. For example the program may be designed wherein the prices for the product may be fed into the program. For examining the authorisation along with the work of the employees the program should also be verified.
- **Audit trail:** In a manual system audit trail is provided through maintenance of adequate documents and records. But in computerised environment there are no documents and records. For example, customer orders received on the telephone may be entered directly in an online system. But the audit trails do exist in the computerised environment provided the systems are designed to maintain the record of all events.
- **Physical assess:** The access to assets and records is restricted both in manual and computerised environment. But the two systems differ in the way they concentrate on the data processing assets and records. For example in a manual system the person wishing to perpetrate a fraud can easily do so as the assets and records are maintained at a single site. But this concentration of data processing assets and records increases the loss that can arise from computer abuse or disaster. For example if a fire occurs and destroys the computer room it would result in a loss of all major master files in the company. Unless adequate backups have been kept it would be unable to continue the operations.
- **Management supervision:** In a manual environment the supervisor can easily supervise the activities of the employees, as often they are located at the same place. In the computerised environment the supervision has to be carried out remotely as data communication is used to enable the employee to be closer to the customer. Supervision is built into the computer system to compensate for the controls that could have been exercised through observation and inquiry.
- **Accountability:** The physical assets should be compared with records to determine if any discrepancies exist. In the manual system the staff prepares the records manually and then physical assets are compared with records. In computerised environment the records are maintained by the system.

These differences may cause a hindrance to the auditor initially. But once he gets accustomed to the IT environment he would not find it difficult to conduct the audit though he may require the use of audit tools.

Answer: [d] Audit trails are not available by default on all software

Module:1

Reference No:M1039

Question: Statistical sampling should be used

- [a] Only when the benefits of sampling exceeds its cost
- [b] There are weak internal controls, resulting which the auditor concludes it is waste to spend on tests
- [c] Audit population has no variables
- [d] A good internal control system exists that highlights errors

Module 1- Audit Sampling

Sampling is a methodology to evaluate a population of data using less than 100% items of the population. It involves selecting a small sample to verify the characteristics of the entire population. Selection of such a sample is based on a certain criteria.

Criteria

For using statistical sampling:

- The benefits (arising out of the sample) should exceed its costs.
- The audit should be purposeful enough to comment on the reliability of the balances appearing in the financial statements.
- Computer assisted audit techniques are available, so it is simpler to use statistical sampling.
- Sampling error should be quantifiable.
- Results of sampling could be extrapolative to give an overall opinion.

For using non-statistical sampling:

- A good control system that highlights errors (maintained by the audit client).
- Weak internal controls, resulting which the auditor concludes it is waste to spend on tests.
- Non-statistical sampling meets the audit objectives.
- Audit population has no variables.

Attributes

- **Unbiased:** The audit sample selected shouldn't be a biased one. It should represent the entire population. When judgemental sampling is used, there is a chance that the items selected are biased and do not represent the entire population. The human nature is to focus on items that are easily accessible. The auditor may focus on such points ignoring the least accessible areas while they may be the ones, with errors. This could give rise to misleading conclusions.
- **Sample size:** The sample size selected must represent the entire population. The size of the sample would be based on either sampling techniques or judgment of the auditor. Sampling technique provides an assurance that the sample size is sufficient to warrant the conclusions expressed. Where possible, statistical sampling should be used.

Statistical and non-statistical sampling techniques are mutually exclusive techniques. Both of them cannot be applied to a particular situation. But there is no difference while planning for the execution of both the sampling techniques. The final decision on statistical sampling, the technique to use and the extent of

application is of the auditor. The auditor will choose the method of sampling based on the audit objectives and after weighing the pros and cons of both the methods.

Reporting

When statistical sampling is used, the auditor must state the levels of precision and confidence of the sample in his report.

Non-statistical sampling is subjective. Since it does not have a statistical basis, it is not meant for cases, which require conclusive statement.

Documentation: The auditor should document the entire sampling done in his working papers. They should include at least the following:

- Type of sampling used
- Items to be sampled
- Characteristics of the population
- Decision on the sample size
- The basis of selecting the sample.
- Where statistical sampling is used, mention of predetermined confidence level and precision level
- Results of test
- Review of the result along with the conclusion arrived at.

Answer: [a] Only when the benefits of sampling exceeds its cost

Module:1

Reference No:M1040

Question: Implementation of Biometric authentication is

- [a] Preventive physical control
- [b] Detective physical control
- [c] Corrective physical control
- [d] None of the above

Module 1- Protection of Information Assets - Part 2

This is the second of a three part series on protection of information assets. In this article we deal with the physical access controls.

Physical access controls are implemented to protect the information assets and other related facilities. Before the controls are implemented, it is necessary to assess the present level of security. This will give a clear picture of the controls that are required.

Types of physical access controls: Physical access controls can be either preventive or detective. Preventive controls are implemented to avoid the occurrence of an undesired event. For example, implementation of biometric authentication. Detective controls are identification of the undesired events after they have occurred. They do not influence the daily activities of the employees. They get activated only in event of security violation. Smoke and fire detectors, visual surveillance systems are a few such detection mechanisms.

The company should divide the area into different zones on the basis of the sensitivity. For example, say Zone 1 as the area, which will be open to the public, Zone 2 as area where all employees are allowed and Zone 3 where access is completely restricted except to those who have permission. After categorising the area into different zones the company should implement access controls depending on the zones.

Authorisation: A list of those employees authorised to enter the restricted areas should be maintained. Any person before entering the restricted zone should record his details. The record should be scrutinised by the security personnel at regular intervals.

Monitoring: The person entering the restricted area should possess access badge containing brief but relevant information about the card holder. The access to the restricted area should be monitored by security guards, intrusion detection system, camera eye or by any such method that is capable of recording the persons entering the restricted zone. This depends on the sensitivity of the access zone.

Backups: Despite best physical access control in place, information loss/ destruction may occur due to mishandling of information assets and information itself by people. Regular back up of information is one way to prevent information loss and for quick recovery. Backup of the information should be taken at periodical intervals depending upon the sensitivity of the information. Backups should not be kept at the same place where the original information is.

Working area: The employees should clean their work area before they leave the office. Also the equipments such as printers, fax machines that is used to print sensitive information should be kept in a restricted area. This will ensure that the sensitive and confidential information does not fall in the hands of unauthorised personnel.

Contingency plan: A contingency plan should be drafted to meet the eventualities arising out of failure of physical security.

Personnel control: The personnel control deals with the employees of the company. The employees must be hired after a careful scrutiny of their background. Employees must sign a contract so that they will not disclose any confidential information that comes into their possession during the course of their employment. They must maintain confidentiality even after they leave the company.

Location control: The company must be located in an area that is not prone to natural disasters. But if located in a sensitive area, measures should be taken to keep the sensitive information and assets at a secure place.

Answer: [a] Preventive physical control

Module:1

Reference No:M1041

Question: Information security risk management would include which of the following as the first step?

- [a] Methodology to control errors
- [b] Analysis of server security policy
- [c] Developing risk evaluation criteria
- [d] Framing trading partner agreements

Module 1- Information Security

Technology has made information flow at a lightning speed across the globe. But security of information is also equally important. Information is considered secure if integrity, reliability, availability, confidentiality, accountability and authenticity of the information are ensured. For this purpose the companies should consider information as an important asset. To maintain the above characteristics the company should perform security risk assessment of information.

The following are important aspects in implementing Information Security

- Framing security policy based on the overall objectives of the company, allocate resources and implement the same.
- Support of top management.
- Assessing information risks and selecting appropriate control measures
- Identifying and value the assets
- Educating and training the employees on information security

Information security risk management is a systematic application of management policies, principles, procedures and practices. Information security risk management system is a documented system describing the policies, practices, assets, threats, risks, control objectives, control procedures and the like. The following framework may give an overview of Information security management system:

1. Establishment of strategic context: Information security risk management should be in line with the overall objectives and strategies of the company. The operational environment should be understood and wherever the risks are shared with other entities, cross responsibilities and issues that might support or impair IS security should be identified.
2. Establishment of organisational context: The management should clearly demarcate the acceptable risks from those that are not acceptable. This should be based on the overall objectives of the company, the infrastructure available and its organisation structure. Such initiatives should be acceptable to both customers and employees alike
3. Establishment of risk management context: This includes
 - o Decisions on whether the review of risk will be limited to a certain project or include all the activates of the company which generate information.
 - o Time frame in which the assessment should be made.
 - o Decisions on whether assessment will be done internally or externally
 - o Assessment of the resources that will be required for review of security. The resources include people to make an assessment, tools that will be used and the like.
4. Developing risks evaluation criteria: The level of risks that a company can accept should be defined. In order to assess the risk the quantitative and qualitative factors that will be considered should be stated. The factors that can be included are the documents of the company like policies, the objectives, legal requirements and the factors that would influence the risk assessment process. The risk criteria selected should cover all the types of risk.
5. Defining the risk activity structure: The risk activity should be broken up into elements. A break up of activity helps in identifying oversight, if any. The structure can be broken up based on information assets, organisation structure or processes, projects and the like.
6. Defining information assets: Information assets are those with a highly valuable and hence require protection. The information assets should not be limited to IT system. An inventory should be made of information that requires protection.
7. Information classification and labelling: Information should be classified and accordingly labelled. The information should be classified based on the level of security needed.

After defining the key components for the information security management a detailed risk assessment should be done. This helps the management to know the present level of security of information and what other steps it should take to protect the information.

Answer: [c] Developing risk evaluation criteria

Module:1

Reference No:M1042

Question: Which of the following is the first step in a Standard Audit Process Model?

- [a] Preliminary review phase
- [b] Test of controls
- [c] Substantive testing
- [d] Audit plan

Module 1- Audit model for IS auditing

Auditors have a generalised, standard audit model, which can be used with a few modifications depending on whether it concerns financial, compliance or tax audits. A few attributes of the standard model:

1. Addresses risk and related control mechanisms to abate risk
2. Reveals important information that enables formulate an opinion
3. Maintains working papers and documents of the work done
4. Flexible, can be adopted to different situations

Therefore the audit model can be extended to an IS audit also. The following are the different phases of an audit model

Phase 1: Audit Plan

An audit plan helps the auditor to identify the risks well in advance. He will also evaluate financial statements that reveal the financial condition, the management's role and any inconsistencies in statements. Risk identification is given importance as his responsibility includes identifying the material frauds and errors in financial statements. The audit plan also helps the auditor in issues like allocating the appropriate resources and scheduling work.

Phase 2: Preliminary review

The preliminary review phase is limited to the evaluation of the organisation. It is a process of identifying the mission, policies and procedures of an organisation, its structure, duties and functions. The type of information systems installed and its role in attaining the organisations mission are studied.

In this phase, the auditor's objective is to determine the fairness of the clients' financial statements. Therefore, the adequacy and reliability of the internal controls have to be evaluated. He must enquire users and supervisors about their roles and policies, system descriptions including databases, centralised information systems, access and program controls, system maintenance and the like.

After conducting the preliminary review phase, an auditor will have a clear idea on the audit objective including the weaknesses in the control. He should also determine the audit resources required for the potential audit.

Phase 3: Detailed review phase

In a detailed review phase, the audit tests are designed by identifying the critical operation. These tests determine the effectiveness of controls. Hence, this phase acts as a small-scale audit enabling an auditor to decide on the proposed audit, whether to accept or not. On the completion of this phase an auditor must be able to prepare an audit programme and decide the test of controls. He will identify areas for detailed compliance testing.

Phase 4: Test of controls

It is a process of testing controls in detail to ensure the effectiveness of internal controls. It is a continuation of the preliminary and detailed review phases. The reliability of the functioning of the system is ensured in this phase. The steps involved are:

- Preparing audit tests required for the organisation
- Conducting tests and
- Evaluating results

Phase 5: Substantive testing

Auditors should examine all documents and vouchers that serve as an evidence to support his arguments. These are referred to as substantive tests. The type of the audit and audit objectives will determine the level of evidence required. The following steps are involved in the design and execution of substantive testing:

- Determine the audit objective
- Design the audit programme and
- Evaluate results

Answer: [d] Audit plan

Module:1

Reference No:M1043

Question: The access to the restricted areas in the company is on the basis of something which the employee has, which he knows or which he possesses. Fingerprints come under which category

- [a] Something which the employee has
- [b] Something which he knows
- [c] Something which he possesses
- [d] None of the above

Module 1- Protection of Information Assets – Part 1

Information is a valuable asset and needs to be secured and protected. Any information must have the following attributes:

- Confidentiality: This implies that no unauthorised person should have access to the information.
- Integrity: Unauthorised persons do not alter information.

- **Authenticity:** Users who use the information and the information assets, are actually the persons they purport to be.

Other aspects associated with information are the people, the hardware and the software that store and process data and information communication equipment, tools and the like. For the protection of all assets and maintaining the above characteristics of information both the physical and logical security should be implemented. They are complementary to each other. Before the company plans to secure the assets it should classify the assets that need protection, identify the threats, analyse the risk and decide on what is the acceptable level of risk. Whatever may be the security feature that may be implemented, the management must ensure that security being implemented is

- Simple
- Comprehensive
- Based on an acceptable standard

Physical security: Physical security is the first line of defence that is implemented for protection of assets. This is made operational by restricting the access to the building or the areas where the assets are kept. The physical threat can be classified into two - the human factor and the non-human factor or natural disaster.

Human factor: In majority of the cases, tampering of information takes place internally. Employees unknowingly may cause harm to the information. But at times it could also be outsiders trying to exploit the loopholes in the security system. The access to the restricted area should therefore be through

- Passwords i.e. something which the user knows
- Badges i.e. what the user has
- Fingerprint i.e. what the user possesses

Natural disasters: These factors are beyond the control of the company. But the company can take steps to combat them. Some of the natural disasters for which the management must take preventive measures are

- **Fire:** Fire can cause damage to the assets. The damage may be either minor or major. The company may install hand held fire extinguishers, smoke detector or fire suppression systems to combat fire.
- **Electric interruption:** In a country like India, many cities face electricity interruption or fluctuations in the voltage. Any interruption of electricity to the computer operations can cause damage to the equipments. For this purpose the company must invest in Uninterruptible Power Supply (UPS), generator or the electrical surge protectors.
- **Lightning:** During a thunderstorm, lightning can cause electrical surge to electrical transmission lines. This can easily damage the electrical equipment. Lightning can also cause fire and damage the structure of the building.
- **Water:** The leakage of water pipe, rain or accidental discharge of the water from the water-based system for sprinkling water in case of fire, can damage the electric equipments and the building. Water detector can be installed for combating such a menace.
- **Environmental disasters:** Computer equipments need a controlled environment. The temperature and humidity can affect the functioning of these equipments. Air conditioning should be provided not only to keep the temperature under control but also to protect the place from dust.
- **Earthquake:** When the company is located in an earthquake prone area, appropriate measures should be taken for continuation of the business after an earthquake occurs and causes damage to the company.

Answer: [c] Something which he possesses

Question: Which of the following is an example of logical access control?

- [a] Location access control
- [b] Security guards
- [c] Entry logs
- [d] Encryption

Module 1- Protection of Information Assets – Part 3

This is the concluding part of the series on protection of information assets. In this article we deal with the logical access control.

The objective of information system is to facilitate sharing of information. But not everyone in the company will have access to the entire information. This restriction on access to information with the use of computer is termed as logical access control.

The logical access controls can be implemented through

- Passwords
- Antivirus software
- Access control software
- Smart cards
- Dial-up access control
- Encryption
- Audit trails
- Intrusion detection programs

Passwords: Passwords are the first line of defence taken by the management to prevent itself from attackers. By virtue of the password, the user is prompted to authenticate for the second time login being the first step to authentication). Hence a company should have a good password policy. (Refer our article on password policy).

Antivirus software: The company should restrict the access of its resources to authorised users only. When the system is not protected there are chances of an outsider causing severe damage through viruses. They are capable of bringing the entire system to a halt. The company should install the anti-virus software to protect itself from viruses. Anti-virus software detects, prevents and removes the virus. The company should also have an anti-virus software policy. (Refer our article on anti-virus software policy). Norton anti -virus is one of the commercial software available in the market,

Access control software: Using this, access to the computer is restricted only to those persons who have authorised login and password.

Smart cards: Smart cards are used for user authentication. The user must enter the PIN (Personal Identification Number) for the purpose.

Dial-up access control: Dial-up access control prevents unauthorised remote access via telecommunication lines. When a user wants to access the network from a remote area, dial up access control verifies the user by calling him back. The user is allowed access only when the call is from a valid phone number. The phone

numbers should be changed at regular intervals.

Encryption: Encryption is conversion of plain text into codes. It protects the sensitive information that is stored in the system or which is being transmitted over the network. But encryption does not protect loss of data. The management should not rely on encryption solely for the purpose of information security.

Audit trails: Audit trails help the management in tracing the transaction from the input to the final output and vice versa. Unauthorised attempts if any, will be recorded by the audit trail. Security officer can review the audit trail to identify the origin of the attempt.

Intrusion detection system: Intrusion detection system analyses the possible attacks from inside and outside the organisation. Intrusion detection system can be host based, network based hybrids and the like. To protect the information assets the company should analyse all the possible risks that the assets can be exposed to and take steps to prevent them.

Answer: [d] Encryption

Module:1

Reference No:M1045

Question: The auditor should report the existence of an irregular and illegal act to which of the following?

- [a] Only management
- [b] Management and third parties
- [c] Management and third parties under certain exceptional conditions
- [d] To anyone who is interested

Module 1- Auditor and irregular and illegal acts

During the course of audit the auditor would come across many irregularities and illegal acts. In this article we discuss how the auditor should consider such acts while performing his audit work.

The auditor is not responsible for detecting irregular and illegal acts. It is the responsibility of the management. However his audit plan is liable to change if he suspects any irregularities. He should then investigate and report the same.

The management prevents and detects such errors by framing suitable policies and procedures, and by implementing and monitoring internal controls. The auditor before he commences the audit should obtain an understanding of the policies, procedures and controls.

Some of the examples of irregularities and illegal acts that the auditor may detect during the course of audit are:

- Any fraudulent act to obtain an illegal advantage
- Non-compliance with the applicable laws and regulations
- Non-compliance with the contract and agreements entered by the company with third parties
- Alteration in the records or documents
- Omitting certain information from records or documents
- Carrying false transactions
- Misappropriation of assets
- Any other intentional acts

The list is not exhaustive. . It would however not include any act arising due to the failure of the company to adhere to its policies or improper conduct of its functions.

Planning

The auditor usually plans his audit by first obtaining an understanding of the organisation and performing risk assessment. The auditor should study the internal control environment, policies and procedures, the related laws and regulations that are applicable to the company. Based on this understanding the auditor can get an insight of the areas that are prone to irregularities or those susceptible to illegal acts. He should perform the risk assessment by taking into account all the factors that

- Effect the financial statements
- Do not effect the financial statements but in general effect the organisation as a whole

Employee dissatisfaction, layoffs, outsourcing, irregularities and acts that are common to the industry give the auditor more clarity on the risk profile of the company.

Based on the risk assessment the auditor should design the nature, timing and extent of the audit procedure.

Procedure to be followed when irregularities and illegal acts are detected

When the auditor comes across an irregular or an illegal act he should consult the appropriate authority in management. Whenever required, he should solicit legal advice on the matter. He should also assess the effect on the subject matter of engagement and on his report. He should perform additional procedures to estimate the effect on the company's financial statements and reputation, possibility of management's involvement, effect on the public interest and the like.

Reporting

The auditors' responsibility is to report the events and the circumstances pertaining to it. It also depends on the materiality of the act. He should report to the appropriate management higher than the one involved. If he suspects that all the levels of management are involved then he must report to the board of directors or the audit committee. The auditor should not report to any third person except under the following circumstances:

- When required by the external auditor
- Compliance with law
- Court order
- Government order

Answer: [c] Management and third parties under certain exceptional conditions

Module:1

Reference No:M1046

Question: Which of the following is not an element of systematic risk assessment process?

- [a] Identifying key areas of risk which are important to management
- [b] Grouping of risk factors into categories based on similar characteristics
- [c] Decomposing complex global judgments into component factors
- [d] Assigning weights to risk factors

Module 1- Risk assessment and internal audit - Part 1

Risk assessment is a process of estimating the risk associated with each auditable unit within the organisation. Risk assessment is undertaken to focus attention on significant audit areas and to allocate scarce resources to the most important audit areas.

There are two fundamental ways of establishing risk - non-systematic and systematic. Systematic approaches involve systematic decomposition of risk into individual factors which are assessed individually, then combined into an overall score reflecting an audit unit's riskiness. The process requires

- Identification of key areas of risk important to management
- Grouping risk factors into categories based on similar characteristics and
- Assigning weights to the risk factors indicating their relative importance in a model for setting audit scope (frequency, intensity and timing).

The non-systematic risks are based on the individual's judgment. This method is more onerous. This method should be usually applied for

- Decomposing complex global judgments into component factors
- Assess these specific areas of risk and concern

Key audit decisions aided by risk assessment

The following are the areas where the auditor for making decision can apply the risk assessment:

- **Audit Frequency:** Every unit of the company cannot be audited every year. But the audit should be planned in such a way that all units are covered in a span of three to four years. But the auditor needs to decide on the units that should be more frequently audited than the others. This is possible in two ways:
 - Fixed audit frequency:* This method is based on the assumption that there are certain natural frequencies that occur in each audit unit. If the frequency can be known then the audit can be planned accordingly. But the disadvantage with this method is that the audit firm would be tempted to carry out the audit either at the peak level or due date. When the fixed frequency is not arrived at properly it may lead to over audit of the concerned unit.
 - Conditional audit frequency:* Under this method all the auditable units are monitored at regular intervals. The timing of audit can be derived by either analytical review method or risk assessment method.
 - o Analytical review method: Key factors and their threshold level are decided and the units are monitored along those lines. When the key factors fall below this level the auditor would be alerted about the audit of this area.
 - o Risk assessment method: This method is similar to the earlier one except that the auditors focus their attention on monitoring risky areas.
- **Audit intensity:** The intensity of audit would depend on various factors such as time, sample size, available skills and the like. The risk level of the audit would help the auditor to determine the intensity of the audit. The riskier the audit the greater the intensity.
- **Audit Timing:** Audit timing can be fixed, random or conditional.
 - o Fixed audit timing - The audit is carried on at fixed times
 - o Random timing - Timing is unpredictable. The auditee has no idea about the timing of audit. E.g. Surprise audit
 - o Conditional timing - The units are audited when the controls fall below the threshold level.
- **Internal audit department size and capability:** A risk assessment can be done whether the internal audit department size is in accordance with the risks that the company faces.

Answer: [c] Decomposing complex global judgments into component factors

Module:1

Reference No:M1048

Question: Which of the following audit technique is used to read and print the information contained in the computer?

- [a] Test deck
- [b] Computer Assisted Audit Techniques
- [c] Integrated test facility technique
- [d] Security system software

Module 1- Audit model for IS auditing - 2

With the wide range of software available for auditing, computers are being increasingly used for the purpose. This article presents a brief explanation of tools and techniques. Computer aided audit tools and techniques assist an auditor to conduct compliance tests, substantive tests and determine the adequacy of controls.

1. Test deck: Test deck checks the logic of the programme. For example, to test the accuracy of pay roll programme logic, a group of transactions are developed by an auditor. The transaction would cover all scenarios. Once the test deck is fed into the program, the output can be analysed to find out how the program has handled different scenarios. For example, it would help the auditor to assess the decisions in payroll programme handled by computer programme, is adequate. But it doesn't assure that the test deck run in a programme by the auditor and the one used by the firm are same.

2. Integrated test facility technique: It is the advanced model of Test deck. In this method, offline program is not used. Instead, the test transactions are inserted in live transaction processing. Then the results are compared with those calculated manually. This process ensures that the correct software is tested. But this process requires identification and deletion of test transactions regularly from the client's system.

3. Computer Assisted Audit Techniques: Computer Assisted Audit Techniques or General Audit Software are used to perform the following functions:

- To read the information contained in the computer file and to print what an auditor requires.
- To select, count and classify the information contained in a computer file.
- To compare the information between two computer files.
- To select and print a random sample. A mathematical formula is used to determine the sample size, after identifying population size based on all significant parameters.
- The end result of the general audit software can be compared with the system output if the processing techniques are simple

4. Inquiry Language of a Data Base System: The query feature in the Database system can be a useful tool.

5. Security System Software: A record of the person who accessed the data files is provided. It helps to determine the adequacy of controls over data base system and also help identify the terminals and passwords which were used for access but was denied by the system.

6. Program Logic Software: It provides a flow chart of the computer programme logic enabling the software logic review.

Evidence reliability in systems auditing: The following are the most reliable forms of evidence to the auditor:

- Personally checked and evaluated documents
- Documents supplied by third parties
- Documents produced within the organisation if there exist strong internal controls
- Documents produced for the use of third party rather than documents generated for self-purpose.
- Oral evidence when combined with other forms of evidence like client reputation.

Information Technology has its good impact on business however they also have impact upon reliability of evidence. IT has reduced the physical documentary evidence, redundancy of data and the like. Hence auditor should look for reliable general controls. He should also assure that databases contain all significant documentary evidence by evaluating the controls, as much of them may not be printed.

Another area causing concern is the role of laser printer and copying machines. It would not be difficult to create documentary evidence, which replicate the original and look authentic. Auditor should look for "consistency" in the trend, data, management, operating results and the like. In addition, the auditor should carry out a lot of analysis on data to ensure the data consistency.

Answer: [b] Computer Assisted Audit Techniques

Module:1

Reference No:M1049

Question: The decision of audit committee regarding the trade off between the performance non-audit role and audit role by the IS auditor will be influenced by which of the following factor?

- [a] Availability of alternative person to perform either role
- [b] Ability of IS auditor to educate the IS team
- [c] Career development and future planning for IS auditor
- [d] All of the above

Module 1- Performance of non-audit functions by IS auditor

The expertise and knowledge of the auditor can provide valuable contribution to the efficiency and effectiveness to the company's IS investments. The IS auditor may have to perform many non-audit functions in the company.

The non-audit role that the auditor is usually expected to carry out in the company are

- Define the IS policies of the company
- Evaluate and implement technologies
- Decide on whether applications should be developed in-house or purchased
- Design and implement security and control features in the application and system
- Establish best practices and procedures in IT functions

The IS auditor can involve himself in non-audit functions on part time or full time basis. He can be involved on consultation basis or as part of IS project teams.

Audit charter

Audit charter should state that the IS auditor can be involved in non-audit functions. It should state the

nature, timing and extent of such roles. Before taking up non-audit functions the auditor should ensure that his role is in conformity with the audit charter.

Independence

When the auditor involves himself in the non-audit functions and subsequently performs the audit of those IS functions, his independence is impaired. Therefore, prior to taking up non-audit functions the auditor should analyse the potential effect on his independence on the current and future IS audits as well as non-audit functions. He should inform the audit committee or equivalent governing body about the potential impairment. While doing so, the auditor should also give his recommendation on the additional measures to be taken by the organisation to safeguard his independence. This include

- Having additional staff members who did not have any role in the IS function
- Considering management and staff of other functions or an outside agency
- Carrying out the peer review of audit function by IS audit staff or outside agency when the audit and non audit functions are carried out by the same person

Audit committee

The decision of audit committee regarding the trade off between the performance non-audit role and audit role by the IS auditor will be influenced by the following factors

- Availability of alternative person to perform either role
- Ability of IS auditor to educate the IS team
- Career development and future planning for IS auditor
- Risks involved in performing both the roles by the same person
- Requirements of external auditors or other regulating body
- Provisions in the audit charter

Critical factors

The critical factors that can help in determining whether the independence and objectivity will be impaired by performing both the roles by the IS auditor are

- Nature, timing and extent of the non-audit roles. The greater the involvement of the auditor in decision making process in non-audit functions, the higher is the level of impairment of independence
- Existence of any fact that may affect the independence of the auditor
- Commitment of the auditor to report weaknesses and errors in the IS function despite his involvement as a non auditor
- IS auditor's freedom to determine the scope and conduct of the audit
- Disclosure by the auditor of his level of involvement in the non-audit functions

Monitoring:

Where there is a possible threat for impairment of independence of the IS audit, the management should closely monitor the conduct of audit.

Reporting:

The auditor should include the following in his audit report

- Names and responsibilities of IS audit staff involved in non-audit role
- Nature, timing and extent of involvement in non-audit functions
- Reasons for such involvement
- Steps taken to ensure that independence and objectivity are not impaired
- Acceptance by audit committee or the governing body of both the functions.

Answer: [d] All of the above

Module:1

Reference No:M1050

Question: _____ agreements define the contracts relating to the utilisation of services of one department by the other in the company.

- [a] Service level agreement
- [b] Outsourcing contracts
- [c] Property contracts
- [d] Insurance contracts

Module 2 - Implementation block - IT control architecture

In our earlier article, we had introduced the concept of Information Technology Control Architecture. We had broken the entire architecture into 3 blocks- planning, implementation and review. In this article we have dealt with the planning block. We have briefly described the various tasks that constitute the planning block.

The tasks

The various tasks are as under

1. **Develop/ acquire and maintain system software:** The organisation before acquiring or developing a system must ensure that the decision is based on feasibility study. The implementation of the system should pass through the phase of designing the controls and the required audit rails, acceptance of the system by the users, deciding about the maintenance of the system, implementation of the required hardware and software.
2. **Develop/ acquire and maintain application software:** The application software that is developed or acquired must satisfy the business needs of the company. The development and acquisition must be broken into functional steps that allow for the monitoring and control at each step. The different stages can be requirements stage, design stage, testing, implementation and post implementation review.
3. **Maintenance of hardware and software:** The maintenance of hardware and software should be based on a clearly defined plan. The plan should include
 - Assessment of the available hardware and software
 - Review of the change procedures
 - Preventive maintenance
 - Review of the security controls
 - Maintenance of the support functions
4. **Maintenance procedures:** The company in accordance with the vendor specification must maintain the acquired systems and applications. The vendor should provide the user and operational manual and the training guide for the users.
5. **Installation of acquired/ developed system:** The installation procedure should include the following steps
 - Planning
 - System and data conversion
 - Users approval
 - Testing - unit, parallel, regression and system testing

- Moving the system to production environment
 - Post implementation review
6. **Change Management:** A change management procedure should be followed before making changes to the existing system to ensure that the existing procedures are not disturbed. The emergency procedure should also be included. All the changes that have been made during the emergencies should be documented.
 7. **Service level agreement:** Service level agreements are contracts that define the use of services of one department by the other. The service level agreement should provide the basis for measuring, monitoring, and charging of the services provided.
 8. **Outsourcing:** The outsourcing contract entered with the third parties must adhere to organisation policies. The contract must include the aspects of ownership of data, security requirements, monitoring and reporting.
 9. **Performance and capacity management:** Performance and capacity management includes the optimal utilisation of resources and storage. It includes the analysis of the available resources, forecasting the needs, scheduling, utilising, monitoring and reporting..

Answer: [a] Service level agreement

Module:1

Reference No:M1051

Question: Configuration management includes

- [a] Status accounting
- [b] Identification
- [c] Control
- [d] All of the above

Module1 - Implementation block -IT control architecture

In our earlier article, we had introduced the concept of Information Technology Control Architecture. We had broken the entire architecture into 3 blocks- planning, implementation and review. In this article, we have dealt with the implementation block. We have briefly described the various tasks that constitute the implementation block. This is the second and concluding part of the series on tasks involved in implementation block.

The tasks

The various tasks are as under

1. **Business continuity plans:** The various aspects involved in this task are:
 - The essentials of a continuity strategy
 - The components it should have
 - The testing, training and maintenance
 - Backup strategies
 - Back-up sites

Security management: The scope of this activity includes:

- Effective security strategies
 - Access control mechanisms
 - User account management, its review and access rights management
 - Handling of security violation
 - Incident management
 - Cryptography
 - Firewall management
 - E-commerce security
3. **Cost management:** This includes the costing procedures adopted by the company, identification of chargeable items and billing & charge back procedures.
 4. **Training:** The various activities/processes covered under this task include
 - Scope of the training needs
 - Training procedures and management
 - Security awareness training
 5. **Help desk:** The activities relate to procedures involved in the customer problem management. This includes recording procedures of customer queries, escalation procedures, clearance of queries and trend analysis
 6. **Configuration management:** This covers the various stages involved in a configuration like configuration identification, baseline management, status accounting, control, and management procedures.
 7. **Problem management:** This pertains to the procedures involved in problem solutions. This includes the identification of the problem, its impact analysis, and its solution identification and emergency procedures. It also includes the issues involved in maintenance of audit trails.
 8. **Data management:** The components of data management include input controls, processing controls and output controls. Input controls include control activities involved in source documents, data validation techniques, and maintenance of data integrity. Processing controls include editing procedures and processing error handling. Output controls include adequate distribution procedures, balancing and reconciliation. This activity also includes protection of data during transmission, storage management, library controls, backup procedures, and protection of stored data.
 9. **Physical and environmental security:** This pertains to the activities involved in managing the facilities of the IT infrastructure. Facilities management involves maintaining the physical security of the infrastructure, the various methods that can be used to control access to the systems, protection measures adopted against environmental hazards and power disruptions.
 10. **Operations management:** The scope of this task covers the procedures and documentation policies that are adopted by the organisation for the operations management, job-scheduling procedures, and log maintenance and remote operations.

Answer: [d] All of the above

Module:1

Reference No:M1052

Question: Which one of the following is not a control principle?

- [a] Confidentiality
- [b] Integrity
- [c] Availability
- [d] Policies

Module1 – IT control Architecture

IT Control & objectives

IT related policies are framed, activities are undertaken and organisational structures are designed by the management to achieve the objectives and goals of enterprise.

Control Principles

The structure of the control objectives framework is built on the foundation of 6 basic information principles. These principles describe the essential attributes of the information that is received, processed and generated by the systems. These principles are as under:

Confidentiality: An attribute of information that prevents:

- its existence being known and/or
 - its content being known.
- to unauthorised individuals, entities, or processes.

Integrity: An attribute of information that ensures that the data is accurate, complete and validated with regard to business objectives.

Availability: An attribute of information, which ensures its timely receipt in order to serve the needs of business requirements.

Effectiveness: An attribute of information, which ensures that data generated by the Information systems achieves the business objectives in a timely manner.

Efficiency: This attribute ensures that IT resources are being utilised in an optimal manner.

Compliance: The last but not the least, this attribute ensures compliance with any laws the business is subject to.

Information Technology Resources

For the above attributes to be achieved, it requires the utilisation of the resources of the business. We have explained below five resources that the business may use.

Data: Any input, which is converted to information. It could exist in various forms-text, graphics, sound, etc. It could be generated either internally or externally.

Technology: A resource that is utilised for conversion of data into information that helps the management in decision making. Technology could be of various kinds and types. It could be application soft wares, system soft wares, hardware, database systems, networks, multimedia and the like.

Support: All the utilities that support or facilitate the generation of information. It also includes the resources, which house the Information Technology.

Human Factor: All those personnel who facilitate the entire Information generation process constitute this resource.

The Information Technology Control Architecture

In this section, we have introduced the concept of Information Technology Architecture. In order to design the control framework we have broken the entire IT process into three blocks. Each block has been divided into various activities that constitute that block. The three blocks have been described below:

Planning block - This block constitutes the activities of

- Identification of new IT initiatives
- Planning of strategies to realise the visions
- Communication of the plans to the concerned audience
- Management of those plans
- planning for the required technology, support and personnel that will be required to realise the vision.

Implementation block - This block constitutes

- Development/ acquisition of solutions for the above plans
- Implementation of the solutions
- Integration of the process with the existing system and business
- Maintenance of the existing systems
- Setting up of support processes

Review block - This block constitutes

- Regular monitoring of the control processes and solutions
- Audit

Conclusion: Objective in designing the control framework is to provide the right information at the right time, to the right people utilising the right resources.

Ultimately, trade-off has to be done between productivity, performance and price. To achieve our objective we have divided the above blocks into different tasks. For each task, we have defined the set of control activities that are covered in subsequent articles.

Answer: [d] Policies

Module:1

Reference No:M1053

Question: _____ is a component of IT organisation structure?

- [a] Data classification schemes
- [b] Technology acquisition plans
- [c] IT steering committee
- [d] Cost benefit analysis

Module1 – Planning block – IT control architecture

In our earlier article, we had introduced the concept of Information Technology Control Architecture. We had broken the entire architecture into 3 blocks- planning, implementation and review. In this article, we have dealt with the planning block. We have briefly described the various tasks that constitute the planning block.

The tasks

The various tasks are as under

1. **Framing of Long term and short term IT plans:** Various technologies are available in the market that can be implemented in business. The management should adopt those technologies that will fulfil the business requirements. These require framing of suitable long-term plans. Based on these plans, short-term operational plans are formulated. And these plans need to be managed, communicated, monitored periodically and evaluated.
2. **Building the information architecture framework:** This task consists of converting the requirements of the organisation into specific data needs. This conversion requires the framing of information architecture, building the organisational data dictionary, data classification schemes and deciding on the security strategy.
3. **Define the technological infrastructure:** Once the information structure has been framed, the next logical step is to build technological infrastructure. This task involves planning for technological infrastructure, monitoring latest trends and legal implications, preparing contingency plans, technology acquisition plans, defining standards and the like.
4. **Building the IT organisation structure:** Like any other functional division of an organisation, even Information technology requires deciding on some organisational issues. The various organisational issues include
 - Setting up and the functioning of IT steering committees
 - Positioning of the IT function
 - Staffing related issues like roles and responsibilities, supervision, segregation of duties, Key personnel, staff related policies and procedures and relationships
 - Security and ownership issues like data ownership, system ownership and the like.
5. **Policies and strategies- Communication and management:** An effective IT control framework must include policies and procedures. The policies and procedures should include all the activities of the IT function the most important being security and internal control policy. The company should have a standard procedure for communication, implementation, maintenance, compliance and quality commitment. The management should be actively involved in all the stages of policy framework.
6. **IT funding – Cost** also plays a very important role in the IT function. An operational IT budget should be prepared for each year. A cost benefit analysis should be carried out for each IT activity. A continuous monitoring should be done to ensure that cost incurred is lower than the benefits accruing.
7. **Managing the human factor –** The organisation should have a comprehensive human resource policy which defines the following issues
 - Recruitment & promotion
 - Training

- Cross training
 - Job performance evaluation
 - Job change and termination
8. **Legal and contractual compliance** – The organisation should ensure compliance with external requirements that could be both legal and contractual. In order to achieve this, the company should have adequate procedures and practices in vogue. For instance, legal external requirements could include safety measures to be taken or e-commerce related issues.
9. **Risk management** – Risk management procedure should include all the IT activities. Risk management procedures should include identification, impact, mitigation and risk acceptance.
10. **Project management** – The issues involved in project management include
- Defining the project
 - Approvals
 - Preparation of master plan
 - User involvement
 - Overall framework
 - Testing
 - Training
 - Post implementation
11. **Quality management** – The organisation should have in place extensive quality assurance standards. It should put in place adequate procedures to ensure adherence to company's quality standards.

Answer: [c] IT steering committee

Module:1

Reference No:M1054

Question: The management generally should obtain external assurance for which of the following IT areas?

- [a] Security and control
- [b] Effectiveness of IT functions
- [c] Legal compliance
- [d] All of the above

Module1 – Review block – IT control Architecture

In our earlier article, we introduced the concept of Information Technology Control Architecture. We had broken the entire architecture into 3 blocks- planning, implementation and review. Subsequently we dealt with planning block and implementation block. In this article, we deal with the review block. We have briefly described the various tasks that constitute the review block.

The tasks

The various tasks are as under

1. **IT function review:** The entire IT review function can be broken up into three stages. The first stage involves collection of data required for monitoring. The second stage involves assessing the performance of individual IT activities. This involves setting up performance standards, metrics, benchmarks and evaluating the activities against the set standards and the like. The performance assessment can be classified into two categories. The first category being functional performance and the second being customer satisfaction. The functional performance should be evaluated based on critical success factors defined by the management. The customer satisfaction should be assessed on the basis of defined service level to be achieved.
2. **Internal control assessment:** The scope of this task includes monitoring the control objectives for internal control framework, control framework implementation and monitoring process. The control objectives defined should ensure that internal control framework is functioning as per the business requirements. The internal control monitoring process should have a reporting mechanism to ensure that the functioning of the internal control is reported on timely basis for effective corrective actions.
3. **External assurance:** Management should obtain external assurance covering the following three areas
 - Security and control
 - Effectiveness of IT functions
 - Legal and contractual complianceExternal assurance must also be undertaken for those IT services that are outsourced. It should be ensured that the external party that is providing the above services is competent enough to provide expert views on the IT services. Ideally, the management should obtain external assurance of IT services before implementation. The external assurance must be taken on a regular basis.
4. **External audit:** The management should define the audit charter for the areas that will be subject to external audit. The management should ensure that the external auditor has no interest in the organisation and is capable of providing an independent review. Where the laws and regulations of the country require that the certificate should be obtained from a qualified member of a recognised body, the management must ensure that the auditor satisfies the same. The management should ensure that audits are conducted for each of the IT services on a periodical basis. The audit should be conducted in accordance with set standards and best practices. The approach adopted by the auditors should provide enough evidence to support the findings, views, and opinions given by the auditors. It is the responsibility of the management to ensure that the recommendations of the auditors are taken into consideration and implemented wherever possible.

Answer: [d] All of the above

Module:1

Reference No:M1055

Question: Which of the following is not an element of risk while conducting risk assessment for Information security?

- [a] Asset value
- [b] Threat frequency
- [c] Threat exposure factor
- [d] Threat impact

Module1 – Information security – Risk Management

In the past, computers were located in a central place called EDP centre or data centre. documents for processing were received by the centres and output was sent to user departments after processing. However the computing environment has changed from centralised to distributed computing. The management of such distributed computer operations is more complex. Risk identification and management have become far more complex since the employees in the entire organisation have to perform certain duties in information processing.

Risk awareness

In order to minimise the risk, management should understand what constitutes the risk. Unless the elements of risk are properly assessed, one cannot take the measures to mitigate it. Businesses have different choices to handle the risk.

1. Accept the risk,
2. Take measures to reduce it to minimum or
3. Transfer the risk (through insurance which compensates the risk)

The following questions have to be addressed in the Risk Management process

- What are the threat events?
- What is the impact of threat?
- Frequency of the threat
- Accuracy of the answers given for above questions

Then the management has to determine the cost effectiveness of the risk mitigation.

Before undertaking Risk Management policy the following terms need to be clearly understood:

Annualised loss expectancy: Annualised loss expectancy is essential for effective risk identification and budget planning. It is calculated as follows

Annualised loss expectancy (ALE) = Single loss expectancy (SLE) x Annualised rate of occurrence (ARO)

For example, if SLE is \$ 500,000 and its rate of occurrence is 1/500 years, then $ALE = \$ 500,000 \times 1/500 = \$1,000$

Annualised rate of occurrence: It refers to the expected frequency of the threat occurrence. If the threat is likely to occur once in 100 years it is represented as 1/100 or 0.01. For example, if misuse of resources by an employee is taken as a threat, the rate of occurrence depends on the number of employees and the frequency at which they commit the mistake. For instance, if 50 employees misuse the system once a year, the annual rate of occurrence is $50 \text{ employees} \times 1 = 50$.

Single loss expectancy: By multiplying the asset value and the exposure factor, single loss expectancy is derived.

First step in the Risk management process is to develop an **Information Risk Management policy**. The policy should state the objectives, scope, responsibilities and the methodology and must be communicated across the parties related to the risk management.

Second step is to establish an IRM (Information Risk Management) team. The team must contain senior management who take the responsibility of IRM. An IT generalist will execute the risk assessment tasks.

Third step is to establish a methodology for IRM and the tools necessary to achieve this. The starting point would be to assess the current status of integration security vis-à-vis risk management. The next step is to assess the risk strategically so that the future spending on IT environment is considered appropriately.

Benefits of risk assessment:

1. It enables to understand the risk, its value, threats that may occur, and the mitigation costs.
2. It provides a strategic approach to mitigate risk.
3. It enables to evaluate the alternative approaches
4. It takes short time to complete the process.
5. It provides a statistical basis for the recommendations made by the security professionals.
6. Risk assessment serves as a basis for determining the information security budget.
7. It provides a cost effective IT environment
8. Quantitative risk assessment program minimises the exposure to liability and insurance costs.

Elements of risk

Elements of risk can be measured through qualitative and quantitative metrics. Before understanding the qualitative and quantitative methods, elements of risk metrics need to be understood. The following are the elements of risk:

1. Asset value
2. Threat frequency (how frequently threat could occur)
3. Threat exposure factor (a measuring factor for impact of loss on the value of the asset)
4. Safeguard effectiveness (a measure to reduce the risk expressed in terms of degree)
5. Safeguard cost (cost of the safeguards chosen to implement)
6. Uncertainty

If the above elements are capable of being quantified and expressed in terms of objective metrics, the risk assessment follows quantitative approach. If they are expressed in subjective terms, risk assessment follows qualitative approach.

Answer: [d] Threat impact

Module:1

Reference No:M1056

Question: The overall objective of framing long term and short term IT plans is

- [a] To meet the business requirements
- [b] To increase the effectiveness of resource utilisation
- [c] To increase the revenue
- [d] To ensure optimal utilisation of resources

Module 1 - Control objectives for planning block

Framing of Long term and short term IT plans

Introduction

As in any functional area, planning is a pre-requisite for the IT function. Long term plans need to be defined

before embarking on any IT project. Based on these Long terms plans, short operational plans need to be formatted for each specific operation contained in the IT project.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To meet the business requirements.	To ensure effectiveness and efficiency of the IT services with regard to business needs.	1. Business objectives 2. Current technologies available 3. The level of the IT function in the organisation 4. Feasibility studies 5. Current IT infrastructure 6. Risk assessment 7. Management support.	• Data • Technology • Support • Human factor

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **Management involvement:** The management is responsible for framing and implementing IT plans, be it long term or short term. In framing such policies, care should be taken to ensure that the plans satisfy the needs of the business.
- **Review of present systems:** Before framing and implementing any plans the existing system should be reviewed with regard to
 1. Functional capability
 2. Cost
 3. Stability
 4. Performance of the technology
- **Formulation of long-term plans:** The IT management takes care of the actual formulation of the plans based on the broad guidelines given by the top management. The plans should be based on a structured approach. The plans must ensure that requirements of the various categories of the users

are met by the IT initiatives. In order to achieve this, every planning process must have an inbuilt mechanism to collect inputs from the ultimate users regarding their requirements.

- **Structure of long term plans:** The structure of the long term plans should take into consideration the following

1. Risk evaluation results
2. Organisational structure
3. Costs
4. Current IT trends
5. Legal requirements
6. Business process re-engineering
7. Staff
8. In-house or third party servicing
9. Data
10. Application systems
11. Critical success actors of the technology

The plan should refer to other detailed plans for other operational issues.

- **Formulation of short-term plans:** The long term plans should be regularly transformed into short-term plans. Appropriate IT resources should be allocated for proper implementation of the short-term plans. Feasibility study should be conducted on regular basis to ensure that the short-range plans are executed at the right time.
- **Communication:** All plans should be communicated to the required personnel in the organisation.
- **Evaluation and review:** The planning process should have an inbuilt mechanism to obtain the feedback from the users. These feedbacks could be utilised for further planning.
- **Changes:** A change management process should be in place for every plan that is developed. The process should ensure that the plans are modified as per the changing environment.

II. Operational Controls

Not applicable for this activity.

Answer: [a] To meet the business requirements

Module:1

Reference No:M1057

Question: Which of the following is not an advantage of qualitative method?

- [a] Provides a statistical basis for the process
- [b] Simpler calculations
- [c] Monetary value of information need not be determined
- [d] Quantitative threat frequency and impact data is not required to be find out

Module 1 - Information security - Risk Management - II

The first part of the article on Risk Management dealt with the introduction and benefits of risk assessment. Qualitative and quantitative methods, its merits and demerits, staff involvement in risk assessment, asset valuation are discussed in the present article.

Qualitative and quantitative approaches for Risk assessment

Qualitative elements: The risk metrics elements include asset value, threat frequency, threat exposure factor, safeguard effectiveness and cost, uncertainty and the like. The elements that can be expressed in monetary value are Asset value and safeguard cost. Rest are all expressed in terms of rate of occurrence, percentage of loss, rate of effectiveness and the like.

The traditional method of calculating Annualised loss expectancy is as follows:

Annualised loss expectancy = (Asset value x Exposure factor) x Annualised rate of occurrence

For example, if the Asset value is \$20M, exposure factor 40% and 1/10 is the annualised rate of occurrence, then the Annualised loss expectancy will be \$800k that is

$$(\$20M \times 40\%) \times 1/10 = \$800k$$

But this method ignores safeguard effectiveness and uncertainty, the essential key risk factors. Further the low frequency and high frequency threats are not clearly differentiated in the above approach.

Merits of qualitative methods

- Simpler calculations
- Monetary value of information need not be determined
- Quantitative threat frequency and impact data need not be found
- Cost of risk mitigation measures are not necessary to estimate.
- Only an indication about significant risk areas is required to be supplied

Demerits of qualitative methods

- Objective metrics are not used in risk assessment. Only subjective processes and metrics are used.
- In the absence of objective monetary values for information, accurate estimation of value of risk is not possible.
- Cost benefit analysis is not based on objective processes and metrics
- Evaluating the management performance is not possible

Quantitative elements: The risk elements are divided into Low, Medium and High categories in order to measure in quantitative terms.

Merits of quantitative methods:

1. Statistical basis is provided for the complete process.
2. Monetary values of information is provided to understand the expected loss clearly
3. Cost benefit analysis is done on an accurate basis.
4. It helps to evaluate the performance of risk management
5. As results are expressed in monetary terms, management can better understand the risk.

Demerits of quantitative methods:

1. Complex calculations: It is difficult to understand the methodology and there are chances for misinterpreting the results.
2. Undertaking a quantitative risk assessment require an automated risk management tool.

3. Gathering information about IT environment, required for assessment, is difficult.
4. Users have to accept the automated tools developed by the vendors.

Staff involvement

Staff involvement is essential in risk assessment in order to value the intangible information asset and to conduct vulnerability analysis.

Valuing intangible information asset: Organisational staff needs to contribute considerable time for valuing the intangible information assets. Involvement of internal staff in the process also ensures the confidentiality, availability and integrity of information.

Conducting the vulnerability analysis: This function involves identifying and analysing the vulnerabilities.

Asset identification and valuation

In order to make a proper budgetary decision, identification and valuation of assets is essential.

Tangible Assets: Tangible assets comprise hardware, media, supplies, IT facilities and the like. Replacement cost is considered for valuing the tangible assets. These values are available with the asset management groups.

Intangible Assets: The intangible or Information assets will not have any physical presence. They are valued on the basis of replacement cost of data and software and the cost of confidentiality, integrity and availability of information.

Answer: [a] Provides a statistical basis for the process

Module:1

Reference No:M1058

Question: Which of the following is not a step involved in risk mitigation process?

- [a] Safeguard analysis
- [b] Safeguard costing
- [c] Threat analysis
- [d] Safeguard cost-benefit analysis

Module 1 – Information Security – Risk Management – III

The present article discusses the management's role in risk assessment and the process of risk mitigation analysis.

Management's role

The decision to undertake risk assessment is based on the organisational culture. It plays an important role in deciding on the qualitative or quantitative methods to be used. An organisation with an aggressive management culture will not take any preventive measures to minimise the cost.

On the other hand, a large organisation will prefer to undertake risk assessment by determining the monetary value of the information, conducting cost benefit analysis and also by figuring expected loss.

Management support and guidance in risk assessment enables more benefits from the risk assessment

process. It also helps the management in understanding the concept, implementing the quantitative approaches and provides a credible base for budgetary support.

Risk mitigation analysis

Upon completion of risk modelling and identifying the status of information security, management will have a clear idea about the risks that have to be mitigated. The following three steps are involved in the risk mitigation:

1. Safeguard analysis and expected risk reduction: The risk manager has to first identify the safeguards to mitigate the risk and analyse them for its ability to mitigate the risk. The concentration is more on the threats with greater vulnerability.

2. Safeguard Costing: The next step is to estimate the cost of selected safeguards. They need not be precise but should be fairly accurate. The following two methods are used to determine the safeguard cost:

- **Cost per square foot method** - For example, if the cost per square foot is \$100 and the total square feet is 10,000, total cost of safeguard comes to \$1,000,000. It is divided by the life expectancy of safeguard (let 10 years) to get annual cost. The annual cost will be \$100,000. Annual maintenance cost (say \$50,000) is added to this to get average annual cost. Hence average annual cost will be \$150,000.
- **Time and material method:** Under this method, cost of labour for the total labour hours plus materials required for an automated tool is divided by life expectancy of safeguard. This gives the annual acquisition and implementation cost. Annual average cost is found out by adding the annual maintenance cost to the above.

3. Safeguard cost- benefit analysis: It is the last step in the risk mitigation. Here the benefits derived from the safeguards are compared with the costs involved. If one or more threats are mitigated by a single safeguard, net benefits need to be calculated carefully. For this, the risk of all threats before and after implementation of safeguards is determined and the net benefit is calculated by deducting the later from the former.

If more than one safeguard is used to mitigate more than one risk it is necessary to find out the amount of collective safeguards used to mitigate one risk. It is calculated with the following formulae

$$AALE (B) - AALE (A) = GRRB - SGAAC (SG 1-n) = NRRB$$

Where AALE (B) = Average annual loss expectancy before safeguards

AALE (A) = Average annual loss expectancy after safeguards

GRRB = Gross risk reduction benefit

SGAAC = Safeguard average annual cost

NRRB = Combined benefit of a collective safeguards for a specific threat.

Answer: [c] Threat analysis

Module:1

Reference No:M1060

Question: For which of the following areas is external assurance not necessary?

- [a] Legal and contractual agreements
- [b] Service providers
- [c] Internal controls and security
- [d] Competency of external party

Module 1 – Control objectives for review block

External assurance

Introduction

An opinion of an external party on the functioning of the organisation increases the confidence of the customers, third party providers and other external agencies on the functioning of the organisation. The management therefore appoints an external third party for its view on the functioning of the organisation and the related matters.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To obtain third party assurance at regular intervals.	To ensure effectiveness, efficiency, confidentiality, integrity, availability, reliability, and compliance attributes of information.	1. Certificates from external party 2. Assessment by external party on effectiveness of IT function 3. External party assurance regarding compliance with laws and agreements 4. Review of functioning of service provider 5. Competency of external party 6. Prior audit involvement.	• Data • Technology • Support • Human factor

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **Security and control:** The management must obtain independent external party certificates on a regular basis with regard to security and internal controls of IT functions and also before implementing any new vital IT functions. The certificate must also be obtained on regular basis on security and internal controls related to service providers.
- **Effectiveness of IT function:** An external evaluation on the effectiveness of the IT functions of the organisation and of the IT service provider must be obtained on a regular basis by the management.
- **Legal and contractual compliance:** The organisation should ensure that the legal and contractual agreements that are applicable to it are complied with. This assurance can be obtained by review of compliance by an external party. The management must obtain an independent assurance even in respect of compliance by service providers.
- **Competency of external party:** To ensure that the review of the IT functions is performed in an effective and efficient manner, the management must ensure that the external party possesses the required knowledge, skills and experience.
- **Prior audit involvement:** The third party involvement should not be limited to evaluation after the implementation of the IT activities. Their participation can be sought even during other stages like planning and installation and other stages.

II. Operational Controls

Not applicable for this activity.

Answer: [d] Competency of external party

Module:1

Reference No:M1061

Question: Which of the following is true with regard to control objective on external audit?

- [a] The management should implement the recommendations of the auditor.
- [b] The management need not ensure that the appointed auditor possess the required skill, expertise and knowledge to perform the audit.
- [c] The management should ensure that audits are conducted for each of the IT services on a periodical basis.
- [d] The management should define the audit charter for the areas that will be subject to external audit.

Module 1 – Control objectives for review block

External audit

Introduction

An opinion of external auditor increases the confidence of the management on the IT functioning of the organisation. It also ensures that the best practices and those feasible for the organisation are adopted and any weaknesses are addressed at the earliest.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To provide for the audit of the IT functions at regular intervals.	To ensure effectiveness, efficiency, confidentiality, integrity, availability, reliability, and compliance attributes of information.	1. Independence of auditor 2. Conduct of audit by competent personnel 3. Findings and recommendations 4. Follow up 5. Evaluation of the impact of audit recommendations	• Data • Technology • Support • Human factor

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **Audit charter:** The management should define the audit charter for the areas subject to external audit. A periodical review of the charter by the management would ensure that the independence of the audit function is maintained.
- **Independence:** The management should ensure that the external auditor has no affiliation in the organisation and is capable of providing an independent review.
- **Ethical standards:** The audit function should adhere to the applicable ethical standards.
- **Qualification:** The management must ensure that the appointed auditor possess the required skill, expertise and knowledge to perform the audit. The audit staff should also possess the required technical expertise. Where the statutory requirements stipulate the need for a certificate from a member of a particular body and with the required qualification, the management must ensure its fulfilment.
- **Periodical review:** The management should ensure that audits are conducted for each of the IT services on a periodical basis. The different IT services should be prioritised for the conduct of the audit.
- **Conduct of audit:** The audit function should be performed by obtaining relevant and reliable information. The audit should provide the management with a correct picture on the functioning of the organisation.
- **Reports:** The report of the auditor should state
 - o Scope of the audit
 - o Audit period
 - o Nature and extent of audit
 - o Findings and recommendations

- o Qualifications and reservations, if any
The report should be distributed only to the concerned persons.
- **Follow-up:** It is the responsibility of the management to ensure that the recommendations of the auditors are taken into consideration and implemented wherever possible. The auditor should also assess whether the findings and recommendations of the audit have been implemented.

II. Operational Controls

Not applicable for this activity.

Answer: [b] The management need not ensure that the appointed auditor possess the required skill, expertise and knowledge to perform the audit.

Module:1

Reference No:M1062

Question: Reliability of system assurance ensures to the users of information generated by the system that the information is

- [a] Timely
- [b] Current
- [c] Accessible
- [d] All of the above

Module 1 - Systems Reliability Assurance and auditor

Increased competition warrants the management to immediately respond to the market threats and opportunities. This is possible only when the management is armed with reliable information at the time. The Report of the Council of Sponsoring Organisations of the Treadway Commission (COSO) states that the quality of information generated by the systems affects the ability of the management to make appropriate decisions regarding the company's activities. According to the report, the quality of information is affected by whether information is

- Timely i.e. is the information available when required?
- Current i.e. is it updated?
- Accurate i.e. is the information correct?
- Accessible i.e. is the information available to the required persons?

The management, board and outsiders need the information that has the above characteristics. The IS auditor can provide the required system reliability assurance.

Assurance services provided by auditor

The auditor can assure the reliability of the system through performing tests related to the integrity of information system. For this purpose he would analyse the causes of defects in the data and find out whether the system is taking care of them. The auditor can rely on error detection and correction techniques. But they assure the accuracy of information but not whether the information is delivered on time. It is time consuming to follow the conservative procedure of "inspect, accept/ reject and rework". The modern approach is a continuous improvement to eliminate all possible defects in reliability-by-design model.

Systems reliability comprises two general services - management service and external service.

Management services: These services assure the quality of the information that is produced by the system for use by boards and management. The assurance is not limited to financial statement but extends to non-financial information as well. For management decision making, much of the important information comes from

customers/ suppliers data, ordering and inventory, contract related data, competitors and market data. The auditor ensures that the system has properly built in controls for detection of errors.

External services: These services assure the quality of financial information generated for both internal and external purposes. The auditor may either conduct regular or continuous audit. He can embed some controls in the system or conduct regular enquiries into client processing systems and databases. For example electronic sensors and software agents can be used by the auditor, which can be embedded into the client's system. Errors or exceptions will trigger an alarm to draw the auditors' attention.

Other assurance services that can be performed by the auditor

Risk assessment and business performance measures: These services ensure that the business objectives are achieved through information system. Risk assessment service focuses on identification of objectives and the related risks. On the other hand, performance measures would focus on objectives, critical success factors for achieving those objectives and their measurement.

Electronic commerce: When the auditor is involved in the assurance of electronic commerce, the users would be assured of the reliability of information in the entire chain of electronic information. The assurance of electronic commerce information means the assurance regarding the security and integrity of all the networks that are involved in public exchange of information.

Benefits

Internal users: The system assurances integrate the systems and the business operations. The users are assured about the reliability of the financial information as well as non-financial information.

External users: External users who rely on the information generated by the company for various purposes can be assured that the information generated is reliable.

Answer: [d] All of the above

Module:1

Reference No:M1063

Question: A certain level of risks could be accepted because

- [a] Uncertainty involved in the risk management process
- [b] Cost effectiveness
- [c] Management policy
- [d] All of the above

Module 1- Control objectives for planning block

Risk Management

Introduction

Every organisation has to set up a risk management process, which establishes procedure for risk identification, analysis of impact and time based cost effective risk mitigation procedures.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources

To support decision making process of management and threat prevention process in IT function	To ensure effectiveness,efficiency, confidentiality, integrity, availability and compliance attributes of information	1. Definition of different kinds of risks 2. Risk acceptance levels 3. Risk assessment procedure 4. Risk ownership 5. Types of risks faced by the organisation 6. Impact of risks	• Data • Technology • Human factor • Support

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **Risk assessment framework:** The management should take the lead and responsibility to establish a systematic methodology to manage risks. The methodology should provide for both global level and specific level risk assessment framework. Risk assessment process should be made mandatory for new project and on regular basis for existing IT systems. Audits, inspections should be made part of risk assessment and re-assessment procedures. Security specialists should be involved in identification of vulnerabilities and IT specifics and suggesting of control measures.
- **Identification of risks:** The risk identification process should involve all elements of risk namely assets, threats, vulnerabilities, controls and the likelihood of risks. It should take into consideration all kinds of risks. The risks must be ranked and should list all the sources of risk identification.
- **Risk impact analysis:** The risk assessment process should result in an impact analysis. The impact should be measured both in terms of quality and quantity.
Risk action: The risk assessment framework should include a risk action plan. The counter measures for the risk should be adopted either in terms of risk mitigation measures, risk reduction measures or risk acceptance.
- **Risk acceptance levels:** The risk assessment framework should also provide for a risk acceptance mechanism. The acceptance could be based on either identification process, element of uncertainty involved in risk management, or cost factors. The accepted risk could either be offset by insurance, negotiated liabilities and the like.
- **Risk control measures:** While adopting control measures, care should be taken to adopt the most cost effective and highest return control measure. It should include a balance of preventive, detective and corrective control measures. Time frame also needs to be considered. For controls to be effective they have to be adequately communicated and regularly evaluated with regard to changing circumstances.
- **Risk-organisational commitment:** Risk management should be made part of all IT strategic plans and Internal control mechanisms and should be utilised as tool for implementation of the same.

II. Operational Controls

Not applicable for this activity.

Answer: [d] All of the above

Module:1

Reference No:M1064

Question: The MIS related to IT function review should have the details of

- [a] The extent to which IT objectives are met
- [b] Status of deliverables
- [c] Compliance with performance standards
- [d] All of the above

Module 1- Control objectives for Review block

IT Function Review

Introduction

A monitoring process has to be defined and established to ensure proper functioning of IT services. The monitoring process should consist of a systemic record of significant and relevant transactions, comparison of the recorded transactions with the performance benchmarks or standards and timely rectifications of deviations if any.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To ensure optimal performance of the IT services as per the standards set.	To ensure effectiveness, efficiency, confidentiality and integrity of the information. To also ensure legal compliance and availability of the information.	1. Benchmarking procedures 2. Reporting procedures 3. Historical data 4. Actual performance records 5. Customer satisfaction evaluation	• Data • Technology • Human factor • Support

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by

the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **Recording of data:** Performance benchmarks and standards should be created for the individual IT functions and a recording mechanism should be established to collect the data required for monitoring. Performance standards can be set up at a global organisational level or at an individual level. Adequate control measures also should be adopted to establish the reliability and appropriateness of the performance benchmarks and standards. Data collection mechanism should also provide for generation of the exception reports.
- **Performance analysis:** A variance analysis between the standards and actual performance should be done on a continuous and regular basis. Unfavourable results should be analysed for identifying the cause and for timely corrective actions.
- **Assessment of customer satisfaction:** At periodical intervals, management should also undertake customer satisfaction assessment to ensure the right level of services to the customers. This exercise should be undertaken to identify the shortfalls in the levels of the customer service and establishment of improvement measures.
- **Reporting:** MIS reports should be prepared and submitted periodically. The reports should have the following minimum components.
 1. Mention to what extent the planned objectives of the IT function is being met.
 2. Deliverables as per schedule
 3. Meeting the performance standards.
 4. Mitigation of risks

On review the management should undertake appropriate action as relevant.

II. Operational Controls

Not applicable for this activity.

Answer: [d] All of the above

Module:1

Reference No:M1065

Question: ----- is a control objective of the IT task of internal control assessment.

- [a] Review of internal control
- [b] Timeliness of control operations
- [c] External independent assurance
- [d] All of the above

Module 1- Control objectives for Review block

Internal Control Assessment

Introduction

The management should establish and adopt an internal control monitoring mechanism, which regularly

assesses the effectiveness and adequacy of the process and contains reporting procedures to keep the management up-to date on a regular basis.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To ensure the compliance of the internal control standards and procedures set by management..	To ensure effectiveness, efficiency, confidentiality and integrity of the information. And also to ensure legal compliance and availability of the information.	1. Continuous internal control monitoring framework 2. Internal control standards 3. Internal control job responsibilities 4. Reporting procedures 5. Assessments6. Exception reports	• Data • Technology • Human factor • Support

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

Review of internal control: A framework should be set up by the management for internal control monitoring. Ideally the framework should contain details about the role of management in the monitoring activities, supervisory activities, variance analysis between standards and actuals, reconciliations of the deviations and the prompt actions on the deviations. Further, the framework should also ensure that the deviations are communicated to the concerned personnel and their immediate higher authorities. The deviations should be escalated to the senior management based on the enormity of the situation.

Timeliness of control operations: The internal control procedures must warrant , errors and non-complying procedures to be brought to the notice of to the right audience in time, to enable prompt corrective actions. The error reporting should be brought to notice before it impacts the functioning of IT services. The management should determine the level of reporting and ensure that exceptions are reported to the affected parties.

External independent assurance of security and internal control: Independent assurance is an essential component of internal control framework. The management to ensure the effective functioning of the internal control framework should obtain periodical external assurances. The assurances can be obtained either by independent audits or self-assessments. The assurances should be obtained periodically and continuously. The audit should be performed to examine if the security

and the internal controls are functioning as required.

II. Operational Controls

Not applicable for this activity.

Answer: [d] All of the above

Module:1

Reference No:M1066

Question: Which of the statements is true with regard to the IT audit framework?

- [a] Risk assessment does not form a part of the audit strategy
- [b] Audit framework is based on the control framework
- [c] The approach of the auditor is not based on business requirements
- [d] All of the above

Module 1- Audit Framework

General Audit Process

In our earlier series of articles, we had outlined a control framework for various IT functions. We had defined a series of specific controls and the overall control objective for each of the IT tasks classified. Now to evaluate the functioning of the control framework, we are defining an audit framework.

This framework is based entirely on the control framework.

The complete structure of the framework is divided into three layers. The outer layer works at a conceptual level and provides an outline on which the auditor can base his audit. It consists of four components:

- a) The IT control framework
- b) The audit preparation guidelines
- c) The audit process approach
- d) The control compliance process

The second layer provides a working guideline for the auditor to conduct the audit

The third layer acts as a support layer, that specifies additional audit requirements with regard to the IT environment of the organisation -.

I. Conceptual layer

1. IT control framework: The IT control framework has been dealt with in a separate article.
2. Audit preparation guidelines: The audit guidelines give an idea on how to get started. Its objective is to help the auditor in determining the scope of the audit. To achieve this objective, first the auditor should identify, evaluate and investigate
 - Organisation functions
 - IT activities that support them

- IT organisation
- Business risks.

The auditor should then gather the relevant information based on the points mentioned above. And determine the associated inherent risks and the control measures taken to mitigate them. This can be done through

- Studying recent changes in the organisation functions and their impact on IT functioning
- Studying recent changes in the IT functions
- Keeping tabs on recent happenings in the organisation with regard to control environment of the business
- Keeping an eye on the IT control framework adopted by the management
- Studying the latest audit or other certification reports
- Going through latest results of the management, if any

Based on the above information, the auditor needs to select the relevant IT task and the associated resources to audit.

The final step is to devise an audit strategy.

Answer: [b] Audit framework is based on the control framework

Module:1

Reference No:M1067

Question: In which area should the auditor gather information before commencing the audit?

- [a] Established policies
- [b] Audit plans
- [c] IT opportunities in the organisation
- [d] Detective risk

Module 1- Audit process approach

In the earlier article, we had defined the entire audit framework. It consists of three layers. The first or the conceptual layer includes:

- The IT control framework
- The audit preparation guidelines
- The audit process approach
- The control compliance process

The audit preparation guidelines and the control compliance process have been dealt with in the earlier articles. In this article, the focus is on a standard approach to the actual audit process. Based on this standard approach, detailed audit guidelines for different IT tasks have been provided in the subsequent articles.

The standard approach

Here the entire audit process has been split into two stages:

1. Preliminary assessment stage

2. Audit stage

Preliminary assessment stage

This stage consists of 2 processes

I. Preliminary understanding

In this process, a preliminary understanding of the IT activity defined, its business requirements and related organisational issues is essential. And an understanding of the control measures adopted is also required. This can be done by interviewing the staff concerned. In particular, the following aspects of the business require to be focused on:

- Business needs
- The organisation framework with individual roles
- Policies established
- Procedures adopted
- Legal requirements to which the organisation is subject to
- The control activities
- Reporting procedures

The information gathered needs to be documented and validated by performing a structured walk through.

II. Preliminary analysis

After obtaining a basic understanding of the process and control measures, the next step is to analyse their effectiveness and reliability. This step provides a basis for the auditor to decide the areas that are to be tested, and the types of tests that have to be conducted.

The control activities have to be analysed based on the following attributes.

- Standard documented procedure
- Deliverables
- Clearly defined duties and responsibilities
- Industry practices
- Key performance factors
- Compensating controls

After the preliminary analysis, the auditor needs to conclude the degree of reliability of the control activities to meet the control objective.

Audit stage

This stage consists of 2 processes

I. Test of controls

This step needs to be performed to confirm whether the defined controls have been implemented and are functioning well. This in turn depends on

- Obtaining evidence
- Reviewing the deliverables

Based on the outcome, the auditor can decide on the areas where the controls are weak and require further tests to be done, before an opinion can be formed on the functioning of the IT tasks in the organisation.

II. Substantive testing

Substantive tests are performed when the auditor is not satisfied with the results of the tests of controls. A detailed analysis of areas where controls are weak has to be performed. This could be done through either analytical techniques or other methods. This step is undertaken as to substantiate the auditor's view that control objectives are not being met, or not exist. The control weaknesses observed have to be documented. In and their fallout will have to be assessed.. In order to reiterate the view point, comparative benchmarks can also be given.

Answer: [a] Established policies

Module:1

Reference No:M1068

Question: Which of the following statement is false, with regard to the audit guideline on long and short term IT plans?

- [a] The auditor ensures the existence of a structured planning approach
- [b] The senior management approves the plans
- [c] The planning process need not be reflected in the minutes of IT steering committee
- [d] The auditor has to identify lapses in the plans, if it does not meet organisational and IT objectives

Module 1- Audit working guideline

Framing of long term and short term plans

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Framing of long term and short term IT plans	1. Management involvement 2. Review of present systems 3. Formulation of long-term plans 4. Structure of long- term plans 5. Formulation of short-term plans 6. Communication 7. Evaluation and review 8. Changes	Not applicable for this activity

Audit Process

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. CEO	1. Policies and procedures
2. COO	2. Roles and responsibilities
3. CFO	3. Business objectives
4. CIO	4. IT objectives
5. IT steering committee member	5. Short term and long term plans
6. IT management	6. Reports and minutes of steering committee meetings

Preliminary analysis

The next step is analyse the effectiveness of the control measures adopted and the degree of reliability that can be placed on the control measures. This can be done through

1. Ensuring the existence of a structured planning approach
2. The planning process should include
 - Compliance of the plans with the business objectives
 - Compliance of the plans with the IT objectives
 - Feasibility studies
 - Risk analysis
 - Checking the optimal investment for IT
 - Keeping the IT initiatives in line with organisational changes
 - Analysis of alternative solutions
3. Approval of the plans by the senior management
4. Assessment of existing information system -strengths and weaknesses, degree of complexity, automation, cost.

Tests of controls

A clear picture of the functioning of the controls can be gained by

- Obtaining evidences
- Reviewing the deliverables

Tests: The following tests have to be done, before an opinion is formed on the functioning of IT tasks in the organisation.

1. Planning process is reflected in the Steering committee meetings
2. Existence of defined deliverables
3. Long term and short term plans contain the following components

- Hardware plans
- Software plans
- Support facilities
- Personnel details
- Training
- SDLC methodology
- Business Resumption Plans

Tests should be performed to ensure that control measures identified in the preliminary analysis section are in place

Substantive testing

This step is undertaken so as to substantiate the auditor's view of controls objectives either not being met or not existing. The control weaknesses observed and its impact will have to be documented. In order to further substantiate the viewpoint, comparative benchmarks can be identified.

Identification of shortfalls

The auditor should identify:

- Plans not meeting organisational and IT objectives
- Failure to meet costing and time schedule
- Failure to identify business and IT opportunities

Answer: [c] The planning process need not be reflected in the minutes of IT steering committee

Module:1

Reference No:M1069

Question: To ensure that a reasonable basis exists for risk measurement, the auditor should verify whether

- [a] Quantitative or qualitative approaches have been used
- [b] Mathematical calculations and other tools have been utilised
- [c] Probability and frequency analysis of risk occurrence has been done
- [d] All of the above

Module 1- Audit working guideline

Risk Management-1

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Risk Management-1	1. Risk assessment framework 2. Identification of risks 3. Risk impact analysis 4. Risk action 5. Risk acceptance levels	Not applicable for this activity

	6. Risk control measures 7. Risk -organisational commitment	

Audit Process

The audit process has been covered in a two part series. This article is the first part, and focuses on preliminary understanding and analysis.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. Senior IT staff 2. IT staff associated with risk management 3. Risk management staff 4. Select IT users	1. Policies and procedures of risk management 2. Business risk assessment reports 3. IT risk assessment reports 4. Operations risk assessment reports 5. Risk measurement basis used by the organisation 6. Insurance coverage for residual risk 7. Expert opinions 8. Peer reviews 9. Inputs from risk management database-if any maintained.

Preliminary analysis

The next step is to analyse the effectiveness of the control measures adopted, and their degree of reliability. This can be done by ensuring that the risk management plan/procedure provides for the following details

1. The framework for identifying and managing risk factors of the IT function.
2. The risk assessments conducted at both organisational or IT departmental level and system specific level
3. Risk identification sources ,including internal and external factors based on audit reports, inspection reports and the like that are already available.
4. Change management procedures for system changes
5. Management procedures such as
 - Continual review of risk assessment and management framework adopted by the company.
 - Risk identification procedures -the probability of risk, the frequency, and associated threats .
 - A formal basis to identify, measure, and select control measures for potential risks.
 - A risk action plan to mitigate the identified risks
6. Documentation that contains a detailed description of the risk management framework, exposures identified, corresponding risks and mitigating factors.

7. The residual risk to be accepted based on the organisational policy, cost considerations, and the uncertainty involved in the risk assessment methodology.
8. Adequate insurance cover to offset the residual risk.
9. Communication of the purpose for adopting control measures

The second part that follows deals with the test of controls and substantive testing.

Answer: [c] The planning process need not be reflected in the minutes of IT steering committee

Module:1

Reference No:M1070

Question: To substantiate his view of control objectives either not being met or not existing, the auditor should

- [a] Identify risks that have not been adequately addressed
- [b] Review the risk assessment approach adopted by the management
- [c] Benchmark risk assessment framework with industry standards
- [d] All of the above

Module 1- Audit working guideline

Risk Management-2

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Risk Management-2	1. Risk assessment framework 2. Identification of risks 3. Risk impact analysis 4. Risk action 5. Risk acceptance levels 6. Risk control measures 7. Risk -organisational commitment	Not applicable for this activity

Audit Process

The audit process has been covered in a two part series. The first part covered the preliminary understanding and analysis. This article is the second part, and deals with the test of controls and substantive testing.

Tests of controls

A clear picture of the functioning of controls can be gained by

- Obtaining evidence

- Reviewing the deliverables

Tests: The following tests have to be done, before taking a stand on the functioning of the IT department :

1. A check on risk assessments to ensure that they comply with the risk management strategies developed by the senior management.
2. A check on documents to verify whether it aligns with the documentation strategy
3. A verification of quantitative and quantitative measurements defined for risks identified.
4. A verification of management involvement and awareness in the risk management process
5. An assessment of whether reports have been sent and approval obtained from the management for the risks identified
6. A check on user involvement and awareness in the risk management process
7. A verification of approval from relevant personnel for acceptance of residual risks
8. A check on whether risks have been prioritised and suitable control measure have been identified.
9. An assessment of the risk action plan, whether it is current and cost-effective
10. A check on whether residual risk has been covered by adequate insurance.

Substantive testing

This step is undertaken to substantiate the auditor's view of control objectives either not being met or not existing. The control weaknesses observed and its impact will have to be documented. In order to further validate his viewpoint, the auditor can

1. Identify comparative benchmarks from similar organisation/ industries
2. Use industry best practises or international standards to review the adequacy of the risk assessment approach.
3. Undertake detailed review of the risk assessment approach

Identification of shortcomings

The auditor should identify

- Unidentified risks
- Unmeasured risks
- Risk exposures that have not been appropriately addressed
- Out of date risk action plans, risk identification procedures and risk lists
- Adoption of risk counter measures that are not cost-effective
- Non-acceptance of residual risks
- Residual risks without adequate insurance.

Answer: [d] All of the above

Module:1

Reference No:M1071

Question: Which of the following statements is "TRUE " with regard to the audit guidelines on the function of Internal control assessment reporting?

- [a] Reports need not include records of errors and inconsistencies
 [b] Reports should ideally satisfy the requirements of a audit committee

[c] Reports should include the problems faced by all the users.

[d] All of the above

Module 1- Audit working guideline

Internal Control Assessment

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Internal Control Assessment	1. Review of internal control 2. Timeliness of control operations 3. External independent assurance of security and internal control	Not applicable for this activity

Audit Process

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. CEO 2. CIO 3. IT management 4. Quality management 5. Internal and external audit management 6. IT users 7. Audit committee members	1. Organisational and IT Policies and procedures relating to Review and monitoring processes. 2. Audit reports, user reports, user satisfaction surveys, System development project reports, audit committee meetings and any other assessments of IT internal controls. 3. Policies and procedures relating to review of internal controls and review frequency. 4. Specific policies relating to security and internal control review

Preliminary analysis

The next step is to analyse the effectiveness of the control measures adopted and the degree of reliability that can be placed on the control measures. This can be done by ensuring that

1. Appropriate data is identified for review purpose
2. Adequate reporting mechanisms exists for internal controls
3. Managerial review is conducted of the performance of the internal control
4. The feedback process is adequately controlled to ensure reliability
5. Records of all internal control errors, inconsistencies and exceptions are maintained

6. Adequate response for recommendations made by external audit authorities, quality control departments, and internal audit divisions exists.
7. Targets are set for internal improvements and outcomes.
8. An analysis of the user satisfaction is made.
9. A reliable and adequate reporting mechanism exists to provide inputs to the external auditors, senior management and internal audit teams
10. Reports are generated in time in compliance with the existing policies and procedures expected for various IT functions.

Tests of controls

The assurance of the functioning of the controls can be gained through

- Obtaining evidences
- Reviewing the deliverables

Tests : Before the auditor takes a stand on the functioning of IT tasks in the organisation, he should check whether

1. Internal control monitoring reports are regularly generated
 2. The management is reviewing the internal control reports and corrective recommendations are undertaken.
 3. Employees are made aware of the policies and procedures regarding internal control reporting.
 4. The quality controls are applied for each of the following phases of the internal reporting mechanisms
- Collection of performance details.
 - Analysis of performance details.
 - Management recommendations.
 - Analysis of the user satisfactions surveys.

Tests should be conducted to ensure the above identified control measures in the preliminary analysis section are functioning.

Substantive Testing

This step is undertaken to substantiate the auditor's view of controls objectives either not being met or not existing. The control weaknesses observed should be adequately documented. A study of the potential impact will have to be conducted and documented. In order to further substantiate the viewpoint comparative benchmarks from similar organisations and industries can be identified. Further the following tests can be conducted.

- Review of the organisation's internal control framework to examine the adequacy of coverage
- Whether apt data is being monitored
- Actual vs. targeted internal control review of the IT tasks
- Actual vs. targeted user satisfaction
- The extent to which improvements suggested are being implemented
- To examine whether the audit committee is satisfied with the internal control reports and the extent.

Identification of shortcomings

The auditor should identify

- Additional areas for internal control areas with regard to regulatory requirements, audit requirements and the management.
- Authority, accountability and responsibility and competency of the staff involved in monitoring functions of all IT tasks.

Answer: [b] Reports should ideally satisfy the requirements of a audit committee

Module:1

Reference No:M1072

Question: Which of the following statements is "TRUE " with regard to the audit guidelines on the Function of IT function review?

- [a] The involvement of management is not mandatory in the monitoring process
- [b] External auditors are not part of the monitoring process
- [c] The monitoring process includes analysis of user satisfaction
- [d] All of the above

Module 1- Audit working guideline

IT Function Review

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
IT Function Review	1. Recording of data 2. Performance analysis 3. Assessment of customer satisfaction 4. Reporting	Not applicable for this activity

Audit Process

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. CEO 2. CIO 3. IT management 4. Quality management 5. Internal and external audit management	1. Organisational and IT Policies and procedures relating to review and monitoring processes. 2. Audit reports, user reports, user satisfaction surveys, and system development project reports. 3. IT tasks planning documents, which list out the performance requirements for each user and the actual performances

6. IT users 7. Audit committee members	against those plans.

Preliminary analysis

The next step is to analyse the effectiveness of the control measures adopted and the degree of reliability that can be placed on the control measures. This can be done by ascertaining that

1. The relevant and accurate data for review is identified
2. Key performance indicators are identified and actual performance is measured against the set standards.
3. Adequate internal reporting mechanisms exist
4. Managerial review of the performance of the IT resources is conducted
5. The feedback process is adequately controlled to ensure reliable feedback.
6. Adequate response for recommendations made by external audit authorities, quality control departments, and internal audit divisions exists.
7. Targets are set for performance improvements and outcomes.
8. An analysis of the user satisfaction is made.
9. A reliable and adequate reporting mechanisms exists to provide inputs to the external auditors, senior management and the internal audit teams
10. Reports are generated in time and comply with the policies and procedures expected for various IT functions.

Tests of controls

The assurance of the functioning of the controls can be gained through

- Obtaining evidences
- Reviewing the deliverables

Tests : Before the auditor takes a stand on the functioning of IT tasks in the organisation, he should check whether

Tests should be performed to ensure the control measures in the preliminary analysis section are adopted

1. Performance monitoring reports are regularly generated
2. The management reviews the performance reports and corrective recommendations are undertaken.
3. Quality controls are applied for each of the following phases of internal reporting mechanisms
 - Collection of performance details.
 - Analysis of performance details.
 - Management recommendations.
 - Analysis of the user satisfactions surveys.

Substantive Testing

This step is undertaken so as to substantiate the auditor's view of controls objectives either not being met or not existing. The control weaknesses observed will need to be adequately documented. A study of the potential impact will have to be conducted and documented. In order to further substantiate the viewpoint,

comparative benchmarks from similar organisations and industries can be identified. Further the following should be established

- Whether apt data is being monitored
- Actual vs. targeted performance
- Actual vs. targeted user satisfaction
- The extent to which improvements suggested are being implemented

Identification of shortcomings

The auditor must identify the authority, accountability responsibility and competency of the staff involved in monitoring functions of all IT tasks.

Answer: [c] The monitoring process includes analysis of user satisfaction

Module:1

Reference No:M1073

Question: Which of the following is referred as Continuous auditing?

- [a] Auditing a particular subject on real time basis
- [b] Auditing the operational efficiency
- [c] Auditing the internal control efficiency
- [d] Auditing a particular subject at the end of the year

Module1 – Continuous auditing – 1

Continuous auditing is not a new concept. Yet each organisation perceives it differently. Its implementation leaves much to be desired irrespective of the amount of time and money invested.

Meaning

Continuous auditing is a process through which an auditor evaluates the particular subject and thereby generates audit reports on real time basis. As these audit reports are actually a third party certification, users get more reliable information on real time basis. When such financial information is made available, it also influences the market reactions on market capitalisation, stock value, cost of capital and the like.

In the traditional method, the scope for market influence on the information contained in the audit report is less due to

1. The time gap between the audit and reporting.
2. The deficiencies identified in the control systems can be rectified even by the management during the time gap.

Difference between continuous monitoring and continuous auditing

Continuous monitoring systems (CMS) enable organisations to monitor and obtain the information relating to systems, data types and process performance. For instance, the CMS developed to evaluate the accounts payable activities try to find out the double payments and amount of payments made with the help of invoice numbers and invoice files.

CMS is different from continuous auditing in the following manner:

1. **Audit report:** It does not generate any audit report.
2. **Evidence:** The opinion expressed in the report must be backed by substantial evidence and it should be obtained from direct observation. Further the evidence so collected should minimise the risk for an auditor in case of any legal proceedings against him. But the information gathered through CMS is indirect, as it is not obtained from direct observation. However, monitoring and testing the processes and systems by an IS auditor fetch direct evidence.
3. **Management function:** Evaluation of process performance is the function of management. Hence the auditors' independence is questionable if he is involved in such management function called continuous monitoring.

Feasibility of continuous auditing

Continuous reporting is hardly followed by companies. The reasons for low level of continuous reporting are due to lack of demand for such reports, and the complexities involved with technology and the related cost/benefit aspects. There is a wrong opinion among organisations that the benefits would not commensurate with the cost incurred on generating reports regularly. They have to look into the particular aspects like performance measures and generate detailed reports for that aspect. In the initial stages, organisations should start with the audit of small aspects that are useful to investors and users.

Processes and technology are the two factors, which can make continuous auditing simple and possible.

Processes: To make the continuous audit a success, there are few prerequisites. The process, systems and controls should be in place and they must be reliable and efficient.

Technology: Testing the process functioning and controls efficiency should not disturb its operation. This is possible with the help of relational databases, socket layer technology, VPNs and electronic audit tools.

Answer: [a] Auditing a particular subject on real time basis

Module:1

Reference No:M1074

Question: Which of the following is the main duty of IS auditors in Continuous auditing?

- [a] Defining the scope of the continuous audit programme
- [b] Evaluating the effectiveness of controls
- [c] Setting an environment required for continuous auditing
- [d] Finding the new set of testing methods

Module1 - Continuous auditing - Implementation -2

Introduction

Continuous auditing is a process through which an auditor evaluates the particular subject and generates audit reports on real time basis. Real-time reporting enables users to derive considerable benefits and improves their decision-making ability. The requirements for effective execution of continuous auditing and comparison with continuous monitoring are dealt in the article titled "Continuous Auditing". This article discusses the IS auditor's role in continuous auditing and its implementation procedure.

IS auditors role in continuous auditing

Continuous reporting system requires effective controls over IT systems. IS auditors' main duty is to evaluate the effectiveness of controls. It requires adequate knowledge of the controls and the skill to evaluate. Hence IS auditors play an important role in continuous auditing.

Need to evaluate the controls: IS auditor often depends on the systems, controls and processes of the organisation to generate audit reports. Therefore, it is essential to evaluate the efficiency of the controls over the existing IT systems.

Continuous audit implementation

The following aspects have to be considered before implementing continuous auditing:

Defining the scope: It is essential to define the scope of the continuous auditing since it covers the financial statements of the entire organisation. Continuous auditing is favourable when the scope of the activities can be easily identified and measured (for example, production, sales and shipment activities). If the scope is based on estimations and judgements, continuous auditing becomes difficult.

Evaluating the environment: Environment evaluation includes evaluation of processes and controls. Strong processes and controls enables an IS auditor to evaluate the systems and test the data to provide timely information despite the absence of organisation wide information systems. On the other hand, weak controls and processes necessitate more time for testing, which eventually increases the cost and delays the reporting.

Testing methods: The controls are evaluated with the help of test of controls and substantive tests. An IS auditor should conduct testing by selecting samples from the data in order to complete the work before deadline. In addition, controlled monitoring system also provides information about the operation of controls.

Determining the period: There are two time periods viz. reporting period and report issuance period. The former deals with the length of the period for which the report has to be generated to provide sufficient information to the users. The latter represents the time required to generate the report. It is based on the number of factors like systems, time required for data entry, operating time and the time required for evaluating and testing the processes and controls. Hence it is difficult to determine the timing of this process. Some organisations may take longer time and some may take less time.

Further auditors are more cautious about the material aspect as any misstatement will increase the liability. This in turn increases the report issuance time. Therefore IS auditors should deliver the timely information by minimising the audit risk.

Adoption of a continuous auditing methodology is a complex process but not an impossible job. The demand for continuous auditing is increasing with the requirement for provision of real-time information that enables organisations to take timely decisions.

Answer: [b] Evaluate the effectiveness of controls

Module:1

Reference No:M1075

Question: Which of the following is not true of snapshots?

- [a] Snapshots are digital pictures of in-the-process transactions
- [b] Snapshots are either manual or scheduled
- [c] Snapshots store digital pictures of system data
- [d] Snapshots are used for tracking down any disruption in the functioning of system software

Module1 – Snapshots

Definition

Most applications follow a standard procedure whereby, after taking in the user input they process it to generate the corresponding output. Snapshots are digital pictures of procedures of the console that are saved and stored in the memory. These procedures serve as references for subsequent output generations in the future. Typically, snapshots are implemented for tracing application software and mapping it. The user provides inputs through the console (consisting of keyboard mouse and the like) for processing the data. Snapshots are a means through which each step of data processing is stored and recalled.

Working

Specifically designed snapshot software applications or audit tools (incorporating snapshot software) are used for tracking every step involved in the output generation process. It takes the "digital picture" of the user input and the corresponding output. Subsequently, digital pictures or snapshots taken by the snapshot software are stored in the computer memory to be retrieved later. The digital pictures (stored in the memory) are distributed to selected servers and clients. This implies that these are selectively accessible and cannot be retrieved by every user in the organisation. These are stored once in a day on a regular basis and available in read-only mode so as to keep track of changes in application programs.

One more important point to remember about snapshots is that, they do not take pictures of the system data. In fact they store the digital pictures of the running transactions (or current input/output operations).

An illustration of how a snapshot is implemented

Let us consider for example bank transactions. Numerous transactions are made in a day, and output is generated for all of them. Thus, in order to keep track of withdrawals, money transfer, deposits and the like, snapshots are taken. In event of a system crash or software failure, the auditing trail can fall back on snapshots.

The retrieval of snapshots is of two types:

- *Manual:* Manual as the name suggests are snapshots taken on demand by the user when there is any change in the system configuration or input/output change. Taking snapshots manually is totally dependant on user's discretion. This means, whether a particular transaction under process is important enough to be saved or not is decided by the user himself. Such snapshots are not automated and are time driven.
- *Time coded:* In time coded snapshots, the software is instructed to take snapshots at regular intervals of time. Such time-driven snapshots do not have to be revoked manually by the user. Hence, these snapshots are also referred to as scheduled snapshot.

Uses of snapshots

Snapshots are employed in the following:

- They are used for analysing and tracking down the flow of data in an application program, so as to know the underlying logic of the data-processing software.
- It is responsible for documenting the logic, input / output controls (or conditions) of the application program and the sequence of processing.

- Snapshots are taken for tracking down any disruption in the functioning of system software like operating system or database system.

Answer: [c] Snapshots store digital pictures of system data

Module:1

Reference No:M1076

Question: In a standard operating environment, PCs are not expected to have

- [a] Standard applications
- [b] Installed applications
- [c] Unauthorised applications
- [d] Licensed applications

Module1 – PC Desktop Audit - 1

In a Standard operating environment, PCs are expected to have only the standard applications, which are installed, like Windows NT, McAfee that are commonly found on all PCs. There may be some other additional software like AUTOCAD and accounting tools to deal with specific areas.

But in reality the standard operating environment doesn't continue for a long time because local users may install other applications, which could include unauthorised versions too. If these are recognised by an auditor during a snapshot audit, he must check the following aspects.

Checks related to executable files and applications at server and desktop level:

- Type of the applications and their legality
- Authorisation for their installation and the responsible person to authorise and install
- Place and time of purchase
- Availability of disks
- Licences possessed and its usage in the business
- Authorisation for shareware installation and respective person to authorise
- Software demonstration versions and their expiry date
- Previous audit conducted
- Corrective actions taken and benefits derived

Reasons for snapshot audit

It is necessary to conduct a snapshot audit for:

1. Determining the quantity of the installed software, shareware, demonstration and sound files, games and images quantity.
2. Identifying the unlicensed and illegal software copies.
3. Identifying the unauthorised shareware, freeware, games, image and sound files.
4. Supervising the installation and usage of software and minimising the cost of help disk.

Benefits of snapshot audit

Snapshot audit is an aggressive approach to audit. It helps to improve the desktop asset management and makes employees responsible for software compliance. It prevents installation of unauthorised software and thereby reduces the chances of being trapped for using unauthorised software.

There are audit tools available to track the types of files or software installed in PCs in the entire organisation. Such tools are capable of generating pie chart with a specific colour code to represent software used by each department or office location. However, before using such tools, the auditor should know of different types of files that could be installed in PC environment and the risk of installing unauthorised files of such types. In addition, an auditor should also be aware of the pattern expected in the pie chart by running such audit tools so that any deviation from the expected pattern can be analysed and reported with implications.

The next article discusses various areas of files that are subject to PC desktop audit.

Answer: [c] Unauthorised applications

Module:1

Reference No:M1077

Question: Who should be interviewed to get the right information on external audit?

- [a] Chief Information Officer
- [b] Project owners
- [c] Security management team
- [d] All of the above

Module 1- Audit working guideline

External audit

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
External audit	1. Audit charter 2. Independence 3. Ethical standards 4. Qualification 5. Periodical review 6. Conduct of audit 7. Reports 8. Follow-up	Not applicable for this activity

Audit Process

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. CEO 2. CIO 3. Internal audit department 4. Quality control department 5. External auditors 6. Audit committee	1. Organisation structure, manuals related to policies and procedures 2. Code of conduct 3. Policies and procedures for external audit 4. Audit charter 5. Audit standards 6. Audit risk analysis 7. Audit plans 8. Previous year reports 9. Experience and knowledge of internal audit staff

Preliminary analysis

The next step is to analyse the effectiveness of the control measures adopted, and their reliability. This can be done by ensuring that:

1. The audit committee has been set up and meets at frequent intervals
2. The internal audit department has been set up
3. External audits help in achieving the audit plans
4. The audit is conducted by adhering to acceptable standards and code of conduct
5. The Auditor is independent of the organisation
6. Audits are well planned and based on the results of risk assessment
7. Audit findings and conclusions are arrived on the basis of evidence
8. Auditors hone their technical skills by attending education programmes
9. Audit reports are submitted to the management
10. Follow up is done on audit findings
11. All IT activities are covered by the audit process

Tests of controls

A clear picture of the functioning of controls can be gained by:

- Obtaining evidence
- Reviewing the deliverables

Tests: Before the auditor takes a stand on the functioning of IT tasks in the organisation, he should check whether

- Management approves the conduct of the external audit.
- Outlook of the management towards external audit is consistent with the audit charter.
- Benchmarks of internal audit are based on auditing standards.
- Audit function is independent of the organisation.
- Audit staff keeps themselves posted on the latest developments.
- Recommendations of the audit report are relevant.
- Timely follow up on the audit report is done.

Tests should be performed to ensure that the control measures identified in the preliminary analysis section are in place.

Substantive testing

This step is undertaken to substantiate the auditor's viewpoint that control objectives are either not being met, or do not exist. The shortcomings in controls and its consequences also should be documented. He can also:

1. Compare with benchmarks from similar organisations/ industries
2. Review
 - Audit plans
 - Value addition of the audit plans to the organisation and IT plans
 - Conclusions and recommendations specified based on audit evidence
 - Implementation of recommendations, if beneficial

Identifying shortcomings

The auditor should identify:

- Cost/ benefit analysis of audit recommendations
- Variances between audit plans , budget and actual performance
- Integration of external and internal audit

Answer: [a] Chief Information Officer

Module:1

Reference No:M1078

Question: Which of the following documents are significant with regard to external assurance?

- [a] Service level agreements and any other contracts with service providers
- [b] Legal and contractual requirements
- [c] Organisation structure
- [d] All of the above

Module 1- Audit working guideline

External assurance Part 1

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
External assurance	1. Security and control 2. Effectiveness of IT function 3. Legal and contractual compliance 4. Competency of external party 5. Prior audit involvement	Not applicable for this activi

Audit Process

The audit process has been covered in two parts. This article is the first part, and deals with a preliminary understanding and analysis of the process.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and documents are given below:

Personnel	Document
1. CIO 2. CEO 3. Internal audit department 4. External auditors 5. External assurance in-charge	1. Policies and procedures with regard to external assurance 2. Organisation structure 3. Manuals of organisation policies and procedures 4. Service level agreements and any other contracts with service providers 5. Legal and contractual requirements 6. Contracts with external assurance 7. Budgets, reports of previous year and past performance of external assurance 8. Knowledge and experience of external assurance staff

Preliminary analysis

The next step is to analyse the effectiveness of the control measures adopted, and their reliability. This can be done by ensuring that:

- Charter for external assurance is defined , and covers all areas that need to be reviewed
- External opinion and certification is obtained, before venturing into any new IT activity, and after implementation must be done on a regular basis
- External opinion and certification is obtained, before employing the services of IT service providers
- External opinion and certificate is obtained on the effectiveness of IT services - both for in- house and outsourced services
- The external assurance ensures compliance with the legal and contractual requirements of all IT services
- External assurance personnel have the requisite knowledge and skill
- The external assurance process is based on professional and acceptable standards
- External assurance personnel are provided continuous training to update their technical knowledge
- The management consults external assurance personnel, prior to implementing any IT service solutions

The next article focuses on the second part of the audit process - the test of controls and substantive testing.

Answer: [d] All of the above

Question: For which of the following should the management obtain certification from the external auditor?

- [a] For venturing into new IT activity
- [b] Before employing the services of IT service providers
- [c] For effectiveness of IT services of the organisation
- [d] All of the above

Module 1- Audit working guideline

External assurance Part 2

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
External assurance	1. Security and control 2. Effectiveness of IT function 3. Legal and contractual compliance 4. Competency of external party 5. Prior audit involvement	Not applicable for this activi

Audit Process

The audit process has been covered in two parts. The first part covered a preliminary understanding and analysis of the process. This article is the second part, and focuses on the test of controls and substantive testing.

Tests of controls

A clear picture of the functioning of controls can be gained by:

- Obtaining evidence
- Reviewing the deliverables

Tests: Before the auditor takes a stand on the functioning of IT tasks in the organisation, he should check whether:

- Performance of the external assurance is approved by the senior management.
- The opinion and certification of the external assurance is accurate, complete and timely, specifically :
 - o For venturing into new IT activity
 - o Before employing the services of IT service providers
 - o For checking the effectiveness of in-house and outsourced IT services
 - o For verifying compliance with the legal and contractual requirements of the organisation
 - o For compliance with the legal and contractual requirements of the service providers

Certificates and opinions in the areas mentioned above should be obtained on a routine basis. Ensure that:

- o The findings, conclusions and recommendations of the independent assurance are relevant and appropriate
- o External assurance are done by personnel who possess the required skill and knowledge
- o External assurance is obtained for resolving the problems related to IT services

Tests should be performed to ensure that control measures identified in the preliminary analysis are functioning as desired.

Substantive testing

This step is undertaken to substantiate the auditor's viewpoint that control objectives are either not being met, or do not exist. The shortcomings in controls and its consequences also should be documented. He can also:

1. Identify comparative benchmarks from similar organisation and industries.
2. Analyse the performance of external assurance with the charter.
3. Evaluate the accuracy, completeness and timeliness of
 - Opinions and certificates
 - Re-certificated
 - Evaluation of effectiveness
 - Legal and contractual requirements
4. Assess the ability of external assurance staff
5. Check prior audit involvement

Identifying shortcomings

The auditor should identify:

- Value added by the external assurance through the review of IT activities
- Variances between the plan, and budget and the actual performance
- Level of proactive audit engagement and its timeliness

Answer: [d] All of the above

Module:1

Reference No:M1080

Question: DLL comes under which of the following category of files?

- [a] Image files
- [b] Sound files
- [c] Executable files
- [d] Come along with the primary application software

Module 1- PC desktop audit - 2

The first part of this article dealt with an introduction to PC desktop audit, and the benefits and reasons for it to be conducted. The present article discusses the various types of files for which an auditor has to

conduct a PC desktop audit.

The audit tools available for tracking the types of files or software installed in PCs are capable of generating pie charts with a specific colour code to represent software used by each department or office location. However, before using such tools, the auditor should know the different types of files that could be installed in the PC environment and the risk involved in installing unauthorised files. In addition, an auditor should also be aware of the pattern expected in the pie chart when running such audit tools, so that any deviation from the expected pattern can be analysed and reported along with the implications.

1. **EXE, OCX and COM files:** - These are executable files of applications. Any unauthorised installation of these files would lead to licensing implications for the standard operating environment installed at the base level. Other EXE, OCE, COM files may include shareware, games, downloads of utilities, demo versions of software etc. Unauthorised installation of these files would lead to the risk of corruption of registry entries, virus attacks and the like. The expected pattern of the pie chart for tracing those files can be uniform or even a distribution of colours for all departments (as far as standard operating systems are concerned) and appropriate distribution for specific installations like the accounting package, designing package etc. If the pattern does not match the expected pattern, the auditor can probe further for unauthorised installation of unwanted software by the users.
2. **AVI, SCR, JPG, GIF, and MOV files:** - Such files are known as image files. These files are capable of being offensive i.e not permissible in the office environment. For example, an organisation may have to face legal problems in the court for the installation of unsavoury or pornographic types of image files. Further, these files consume large bandwidth and disk space, increase costs and slow down the network performance. The pie chart shows the level of image files installed by different departments. An auditor must ensure that the installed level of image files and the hard disk consumption of the same is acceptable to the management.
3. **DLL files:** - These files come along with the primary application software. As DLL files can be downloaded only under license along with the main application, unauthorised downloading of these files is risky. Further, they may corrupt files, crash systems or damage them. The standard pie chart pattern for these types of files is a uniform distribution among all departments in the standard operating environment of the organisation. The pie chart here should be similar to the chart that is developed for application executable files, because DLL files come along with the primary application software. Any discrepancy between two depicts unauthorised installation of DLL files. In that case an auditor is required to identify the names of the unauthorised files installed.
4. **MPG, MP3, WAV files:** - These files falls under the category of sound files. Unauthorised installation of these files may affect the productivity of the staff since they may cut into the organisational time. Further downloading such files may increase bandwidth and consumable costs. Unauthorised installation of these files may give rise to licensing implications. The standard pie chart for sound files shows the acceptable level of installation. An auditor should ensure that the installed level of sound files is acceptable to the management and check whether the consumption of time and hard disk is acceptable.

Answer: [d] Come along with the primary application software

Module:1

Reference No:M1081

Question: Integrated Audit tools can be used perform the functions of

[a] Control self assessment and direct audit report assessment

[b] Only control self assessment

- [c] Only audit report assessment
- [d] None of the above

Module 1- Audit Tools- An introduction to the types of tools available

Generally it is observed that the auditor performs two functions. One is to provide an assurance on various functional aspects of the business, like accounts, payroll inventory and the like individually. On the other hand he is also expected to provide an opinion on adequacy of control function for the entity as a whole.

Audit Tools

Wide ranges of audit software are available to assist the auditor to perform both functions. We can broadly categorise these software into **general purpose** and **specific purpose** audit tools. The tools of both these categories have been described below

General-purpose audit tools

The general-purpose audit tools have been developed keeping in mind the auditor's primary task of providing an opinion on the control structure of the organisation. These are generally compatible with any software platform and do not have any specific hardware requirements. Basically these tools only automate the audit process like sampling.

- *All-purpose audit tools:* These audit tools are used for performing the basic audit function. This includes sampling and statistical analysis of transactions and data, anomaly analysis and other related primary functions of the auditor. Leading developers of such tools are ACL, IDEA and the like.
- *Audit administration tools:* These audit tools assist the auditor in automating the preparation of audit programs, work paper management, report summarising, recommendation and the like. Leading developers of such tools are TeamMate, Auditor Assistant and the like.
- *Document manager:* These are the general tools that are widely used by the auditors such as spreadsheets and word processors. Example Word, Excel Corel WordPerfect and the like.
- *Computer projector:* Word processors based projectors are also available, wherein standard templates can be used to capture input of the audit data, for the required output.

Special-purpose audit tools

- *Security monitoring tools:* Numerous security-monitoring tools are available in the market for auditors to monitor and evaluate the security structure of the IT system. Some of the tools available are NT auditor for IDEA, Pentasafe VigilEnt Agents and the like.
- *CSA software:* Specific software tools are available for operational risk management and also for compliance with Basel Committee recommendations. These tools also assist in the Control Self assessment procedures. Some of the tools that are available are Prism, KnowRisk and the like.

Integrated Audit tools

These tools assist the auditor in his primary functions like direct report assessment and the organisation in risk and control self-assessment. These tools are designed to capture all information on risk and control being generated by auditors in addition to the risk, control and assurance status being generated by the organisation.

Quantitative Risk Analyser software

This software can be utilised to capture and store risk event information for years together. This data can

be analysed using sophisticated analytical and modelling tools. This software can also be used to compare the organisation's risk statistics with national and international standards.

Answer: [a] Control self assessment and direct audit report assessment

Module:1

Reference No:M1082

Question: Which of the following statement is "TRUE" with regard to security benchmark tools?

- [a] Recommendations of security benchmark tools should be implemented by the organisation
- [b] The benchmark tools are used to measure the organisations security against the defined benchmarks
- [c] Security benchmarks need not be based on the functional requirements of the organisation
- [d] Implementation of the security benchmark tool is independent of the security policy of the organisation

Module 1- Security Benchmark Tools

Recent developments in the IT scenario have literally coerced the auditing and security professionals to jointly work towards providing a secure IT environment for the business operations. Several security tools are now available in the market to assist both the auditors and security personnel in their common objective. We have described below some of the general characteristics and the types of security benchmarking tools that are currently available. This article contains some of the recent developments.

Types of security tools

Several security tools currently available in the market are suitable for various types of computing environment. They can be grouped based on the functional characteristics. The common types are

- *Operating system security:* Linux, HP/UX, Solaris, Windows 2000 security benchmarking tools are some of the operating system security benchmarking tools.
- *Network security:* Some of the networking security benchmark tools are Windows NT, Cisco routers security benchmarking tools and the like.

Security measurement process using the benchmark tools

The benchmark tools can be used to measure the organisation's security against the defined benchmarks. It should measure individual IT function. The measurement is on a scale of 0 to 10. The results should be compared with the organisation security standards and operational requirements. The organisation should strive to reach the scale of 10. The scale of 10 does not however assure a perfectly secure system.

Audit tools also suggest corrective measures for each security lapse or loophole or a vulnerability that has been thrown up by the evaluation process. However it is left to the individual organisations to decide on the actual implementation of the corrective measures. Some organisations also choose to modify the tools settings on the basis of their individual requirements. Once the changes have been implemented the entire evaluation process has to be repeated to check if the systems have improved.

Right usage of security benchmark tools!!!!

The organisation has to choose those security benchmarks that suit the requirements of the business. In other words, security must allow for full functional capabilities of each system that is being evaluated for

the security. It does not help, if ultimately the security functions of the system impair their actual functioning.

An effective usage of security benchmarks requires the following procedures by the organisation:

1. Assessment of current security policies, procedures with the benchmarks to ensure compatibility.
2. Plan for implementation of the corrective measures recommended by the security benchmark tools. Also the organisation should decide on the feasibility of implementing the correct measures.
3. Actual implementation of the corrective measures.
4. Re-assessment of the security.

Security assessment is not a one-time task but a continuous process.

Recent developments

The current trend is to combine the benchmark tools with the security tools. This will help the security practitioners, IT managers and the auditors to join hands in securing the information systems. Some of the products that facilitate this are NetIQ and Symntec.

Answer: [b] The benchmark tools are used to measure the organisations security against the defined benchmarks

Module:1

Reference No:M1083

Question: Which of the statements is "NOT TRUE" with regard to audit of procards?

- [a] Audit tool for procard transactions should provide for analysis of the data
- [b] Reasonable of charge can be verified by comparing transactions with amount greater than defined upper limit
- [c] Procards issued to a personnel can be used by another personnel
- [d] For use of audit the required data should be imported in the audit tool

Module 1- Audit of Procards

What are procards?

The widely used method by the employees to procure their requirements is to streamline their requirements through the purchase department in an organisation. To save the administrative time and for faster receipt of goods procurement cards (procards) are issued to the employees. The procards are corporate MasterCard, Visa or American express cards. Using these cards the employees can purchase their requirements without going through the channel purchase department.

Audit

The steps involved in the audit of procards are summarised under:

- *Obtaining the relevant data:* Data file containing the record of procard transactions should be imported into the auditor's tools.
- *Review of data:* The next step is to review the data. This will help in identifying unusual transactions. The data should be classified for each cardholder, expense type, purchase date, charges per statement end date, charges per vendor or any other relevant fields. This analysis will project items with unusual trend. For example classifying the data on type of purchases will facilitate the review of purchases that are ordinarily not allowed as per the company's policy. Besides the above it is also

required to ensure that the purchases made by the employees have not exceeded their card limits. This can be verified by determining the highest, lowest and average purchase amounts.

- *Reasonableness of charges:* The following have to be taken into account for assessing charges:
 - o Comparison of the vendor name and the expense
 - o Transactions with amount greater than predefined upper limit
 - o Transactions with amount less than the fee charged per transaction
 - o Charges per person per end date
 - o Charges per person per day
 - o Charges per person per card
 - o Excessive usage by any person
 - o Purchases that are prohibited and the like.

Besides the above, all data fields pertaining to amount, amount per procard holder, date, vendor and the like should be compared for duplicate transactions.

- *Use of procards by only authorised personnel:* As the employees can make purchases without the approval from the organisation it is necessary to track all the usage of the cards and that the purchases are by the employees of the company. For this the auditor should obtain list of personnel entitled to procards, compare it with the list of personnel using, verifying the procards held by few of the employees. Besides that all the expenses associated with the card should be determined and analysed if the expenditure can be reduced by drawing back the unused cards.

Audit tools

Audit tool for procard transactions should provide for analysing the data file by sorting, grouping, stratifying, classification and comparison for duplicate payments. Many products are available in the market such as ACL, IDEA and the like. The data can also be analysed using the Microsoft Access and Excel. To verify the excessive purchases made by the personnel the audit tools can analyse the transaction per person per item and can give details about the items that should be in inventory. The personnel need not purchase them, as such an inventory exists already.

Answer: [c] Procards issued to a personnel can be used by another personnel benchmarks

Module:1

Reference No:M1084

Question: Which of the following statement is "NOT TRUE" with regard to integration of traditional audit and the IT environment?

- [a] In IT environment the auditors are required to perform different roles from what he originally used to perform
- [b] Organisations at present are dependent 100% on computers for their information processing
- [c] To integrate it is better to define the expectations of IT audit department
- [d] IT environment requires that technical people acquire knowledge of audit and not vice versa

Module 1- Traditional Audit and the IT environment

The role of a traditional auditor is changing with the advancement in technology. Thus, he is required to be a computer savvy and extend his traditional role to the IT environment as well.

Paradigm shift

In the early days when EDP audit concept was introduced, the technology that was used in organisations was very simple. At that time the question was whether to train the auditors in IT or to train an IT specialist in

audit. Usually it was a computer specialist who was hired and trained in audit. But this led to the formation of separate groups within the internal audit department.

In today's environment, organisations have started depending nearly 100% on computers. But still in internal audit departments majority are financial auditors with not enough knowledge about IT.

Integration of the functions

In order to integrate the traditional and IT functions it is better to define the expectations of the integrated IT audit and the expectations of the internal audit.

Expectations of internal audit

The following are the three general models of internal audit expectations:

- Due diligence model: Internal audit is performed to ensure that legal obligations have been fulfilled and that the internal controls are functioning effectively.
- Development and improvements model: Internal audit evaluates the internal controls, improvements in the performance and development of staff.
- Professional model: Internal audit emphasis on risk management, implemented controls, improvements and internal assurance.

The organisation can also develop their own specific models as per their business and IT audit needs.

Expectations of IT audit

It is difficult to understand the expectations of IT audit in the IT environment that is changing rapidly. IT audit can be either general or application (technical) based. But the areas that can be included in IT audit are very wide. Another difficulty is that the IT audit has become so specialised that it requires in-depth knowledge and experience in that activity. Briefly the models of IT audit expectations are

- Due diligence model: The fundamental principle is to limit the liability. This can be achieved by any of the three choices. The first is to outsource to a company with expertise and experience in the IT environment similar to the organisation. The second, to co-source i.e. to establish a general internal IT audit and to outsource the specific technical IT audit. The third choice will be to establish a general and technical IT audit.
- Development and improvements model: The prime need will be to recruit and develop staff with both general and technical audit skills. Unlike general skills technical skills are difficult to develop and hence it is advisable to outsource them.
- Professional model: Internal audit should bring about improvements in operations. The staff should be able to balance both the management and technical angles of the operations. Dynamic audit methods, cross functional team based approach and proactive computer based auditing methods should be adopted.

Defining the expectations of the internal audit and the IT audit helps in achieving the organisational expectations.

Answer: [d] IT environment requires that technical people acquire knowledge of audit and not vice versa

Module:1

Reference No:M1085

Question: Which of the following forms part of building intelligence in an accounts audit software?

- [a] Review the entire account process
- [b] Analysing the exposures and performing a cost benefit analysis
- [c] Defining the exception reports that should be generated
- [d] All of the above

Module 1- Audit software for accounts payable

Auditor is required to audit the accounts of the auditee before giving an opinion. One of the financial areas that the auditor will verify is account payable. In this area the auditor needs to ensure that all the payments are actually due, authorised and that there are no duplicate payments. This article focuses on this aspect of computerised financial accounts and building intelligence into audit interrogation software.

Controls that should exist in audit software

Given below are the errors that can exist in accounts payable record for which controls should be built in the audit software.

- *Duplicate payments:* The most common error is the payment to the same vendor when the invoice number is also the same. Relevant controls should be built to avoid this.
- *Void payments:* Payments made to the vendor with the same invoice number does not necessarily mean duplicate payments. It is also possible that the original payment was void and hence the second payment. The audit software should take into account such entries before a report is generated on duplicate payments.
- *Keystroke errors:* Keystroke errors are those that are duplicate, but do not appear so in the given fields, due to the wrong keying. The audit software should be able to detect such errors. The keystroke errors that can exist are
 - o Keystroke errors in keying the duplicate entry. For example invoice number for the second entry may have been keyed with a wrong number say from 5472 to 5742.
 - o Invoice number is entered with an extra character say with 5472 and then with 5472A.
 - o Invoice number is left blank.
 The most probable field susceptible to duplicate invoice is the invoice number.
- *Duplicate record in the address book:* When there is a change in the address of the vendor the accounts department instead of updating the record may create a new record. Even if the payment were made twice it would be difficult to detect even though the invoice number and invoice amount is the same as the vendor address would be different.

Building intelligence in audit software

Steps involved in building intelligence in audit software are as under:

- *Review:* Review the entire process from entry screens, system controls, data processing and the final output to discover the weaknesses that exist in the system. The review process should include both junior and senior auditors, as brainstorming is successful only when people with different experiences are included. The review process would detect all the areas that are prone to exposures or errors.
- *Cost benefit analysis:* This will include prioritising the exposures. With the finite time and limited resources it may not be possible to review all the exceptions. Probability theory would help prioritise and verify the reported exception.. For example there are better chances of identifying duplicate payments if the amounts are similar with sorted vendor name and invoice number than just the amount. Based on the assigned probabilities estimate of the average amount of time to be spent on each type of exception can be arrived. Another way would be to divide the total available time with the estimated cost to review each exception. This would also help to understand the level of coverage the audit will accomplish.

- *Exception reports:* After selecting the exception reports the next step is to generate the exception reports. Any additional data be required should be called from the IS department. On receiving the data, exception reports can be generated. This would also help in estimating the probabilities that were assigned earlier to uncover the true findings.

Audit software can thus be tailored according to your needs based on cost benefits.

Answer: [d] All of the above

Module:1

Reference No:M1086

Question: The purpose of using automated software testing tool is

- [a] Reduction of testing time of the software
- [b] Testing of the software after it is developed
- [c] Determining the quality of the software
- [d] All of the above

Module 1- Selection of automated software testing tools

The deployment of automated software tools reduces the testing time of the software being developed. Before using any automated software it should be properly evaluated. This will immensely help in meeting the deadlines as well as assuring the quality. In this article we deal with the purpose of using these tools and its evaluation before deployment .

Purpose of using automated software testing tools

The main purposes of using automated software testing tools are

- Development of software that is error free
- Maintaining the quality of software
- Interactive development of software at every stage
- Reduction of testing time of the software
- Test of software from various dimensions i.e. its reliability, functional performance, system performance and the like

Evaluation of software testing tool

Before using any software-testing tool the software should be thoroughly evaluated. The absence of evaluation can lead to use of wrong testing tool and incorrect decisions. The evaluation process comprises four steps that are as under:

1. **Functional specifications:** The first step is to decide the functional requirements of the testing tool. The list should be a generic one and prepared after evaluating the deficiencies in the existing system. The list should be evaluated based on the overall objectives of the tools before a final decision is made.
2. **Evaluation of alternatives:** Different alternatives should be evaluated before a final selection is made. Though it is a time consuming process the benefits of it are long term as it has a bearing on the productivity. The aspects that require evaluation are

- Functional specifications: The tools should be evaluated based on the functional specifications defined above. The main areas where the tools should be evaluated are performance, reliability, ease of use and the like.
 - Vendor support: Vendor support can be analysed by interviewing the vendors on the various aspects. The interview process should be questioning and analyse
 - o The time required to respond to queries
 - o Reasonableness of the time specified
 - o Competency of the technical team
 - o Proximity
 - Reputation of the vendor: Vendor's reputation can be judged based on the list of his clientele. This will reveal the commitment and dedication of the vendor towards his product. The commitment of the vendor can also be analysed based on the upgrades and release dates of the software so as to avoid purchasing an outdated product.
3. Cost/ benefit analysis: This would include identification and computation of cost and benefits of various alternatives. The components of cost would include
- Software costs
 - Hardware costs
 - Cost of implementation
 - Training the staff
 - Any other relevant costs

The benefits will include

- Time reduction in testing
 - Reduced costs
 - Improvements
 - Accuracy
 - Morale of the staff
 - Increased productivity
 - Meeting the deadlines on time and the like
4. Selecting the alternative: The final step will be to select the testing tool based on the above steps. Where the alternatives are on the same scale, they must be evaluated on subjective factors.

Answer: [a] Reduction of testing time of the software

Module:1

Reference No:M1087

Question: Network management tools help the auditor to

- [a] Analyse the failure of network components
- [b] Analyse the intrusions made
- [c] Develop standard benchmarks
- [d] None of the above

Module 1- Security and risk management tools

Audit tools help the auditor to understand and analyse a situation. One such situation where the auditor needs to use the audit tools is security and risk assessment. These tools can help the auditor scan the network for weakness as well as to monitor the traffic on the network.

The tools that are used for network and risk assessment are similar to those that are used by the hackers for analysing the vulnerabilities that exist in the network. Therefore the auditor should ensure that he has considerable knowledge and experience to use such tools. The use of such tools without proper experience could harm the organisation. Moreover, it is always better if the management is informed about the use of such tools. This would help them in taking immediate action in event of emergencies.

Security and risk management tools can be broadly categorised as under:

- Network management tools: The auditor can use network monitors that are embedded with artificial intelligence to analyse the failure of network components, to estimate the damage and for ensuing corrective action.
- Intrusion detection systems: Intrusion detection systems can also be used as audit tools like network monitors but they are still in their early stages.
- Knowledge based systems: Use of knowledge-based systems is also on the rise for the purpose of network management.
- Risk management tools: Auditors are required to provide an assurance to the management that the organisations are protected from all the known threats. To quantify the risk and provide the necessary assurance the auditors use risk management tools. There is wide range of tools available in the market according to the requirements of the industry.

These tools are also undergoing change in accordance with the requirements of the industry and auditors.

Developments

Wide use of security and risk management tools has facilitated establishment of benchmarks for operating system environments. The standards will become mandatory and the auditor would be required to provide an assurance that the organisation systems are in conformity with the standards. This would also considerably bring down the insurance litigations regarding the claimant of insurance in case of incidents. All the organisations are required to comply with the standards and non-compliance will lead to non-claimant of the insurance amount.

Future

The management tools are bound to increase in their functionality and capability in the near future as the public and private sectors are becoming responsive to the risks that arise due to lapse of information security. Even regulatory, governance and other corporate bodies like SANS Institute, Centre for Internet Security and the like are contributing towards this development.

Answer: [a] Analyse the failure of network components

Module:1

Reference No:M1088

Question: Which of the following does not ensure effective governance process with the internal audit team?

- [a] Strategic orientation of audit team
- [b] High quality internal audit staff

- [c] Maintaining gap between internal audit team and top management
- [d] Increasing the responsibility of internal audit team

Module 1- Internal Audit and organisational value

Corporate governance and controls are being perceived differently after the Enron debacle. Investors, lawmakers, investment community and regulators are stressing the need for Directors for effective governance processes.

External auditors being mostly affected with accounting scandals; corporate governance, internal auditing practices are no exemption. With the evolution of new governing practices the senior management and audit committee are taking steps to ensure proper control over audit processes. Essentially it is the responsibility of Directors and top executives to secure the internal accuracy of controls against outsiders. The following are four steps aimed at strengthening the internal audit functions:

1. Enhance the responsibility of internal audit team: The responsibility of internal audit team can be enhanced by elevating them to the board or senior management level. It enables effective utilisation of internal audit resources. Further the role of internal audit team in creating value for the company must be properly communicated to the top executive. Measures must be taken to minimise the reporting gap between top management and internal audit team. They must strive to improve the performance of internal audit function.

2. Strategic orientation: Internal audit function must be aligned with corporate strategy to deal with control issues at corporate level. Strategic orientation of audit committee provides better governance.

Senior management and audit committee need to direct audit groups in achieving objectives. A strategic framework needs to be established for internal audit. Audit mission has to be clearly defined by the chief audit executive along with audit committee and senior management. Roles and responsibilities of audit staff need to be clearly defined.

The organisational structure must facilitate the internal audit department to focus on strategic areas. Unnecessary influence of operational management on audit function needs to be avoided. The scope of audit function will determine the level of interdependence required.

3. Corporate governance process: The reporting structure of audit function may result in conflicts. This is because, internal audit function has to report to top management on administrative grounds and it has to report to audit committee on functional grounds. Hence the reporting line is not significant. But good governance depends on the ability to comment on various levels of controls. Internal audit function must be independent so as to address the shareholders expectations.

4. High quality internal audit staff: Qualified and talented audit staff will have wider perspective of the audit function and ensures better governance. External resources must be pooled in, if necessary.

Internal audit staff should have the specialised skill in various areas like financial instruments, offshore transactions, and information technology in order to address them properly. Further sufficient amount of resources must be allocated to examine the controls.

Strategic orientation and effective utilisation of internal audit resources ensures better corporate governance and control.

Answer: [c] Maintaining gap between internal audit team and top management

Question: Which of the following is the reason for under-utilising software packages?

- [a] Centralised filing system
- [b] Centralisation of audit personnel location
- [c] Decentralised filing system
- [d] Availability of benchmarks

Module 1- Audit software for risk management

Audit software is useful to the auditor in audit. But this technology can be leveraged in data analysis, risk management and continuous monitoring. This improves the effectiveness and efficiency of audit.

The commonly used software packages include spreadsheet, database, word processing and other powerful tools. All these helps in presenting data flow diagrams, reports in standardised formats and risk modelling. But these tools have not been utilised effectively by the auditors. Take the case of spreadsheets for instance. Spreadsheet packages help in carrying out statistical sampling that in turn enables the auditor to ensure the correctness of conclusions drawn. This is not possible with traditional judgemental sampling techniques.

The following are the common deficiencies in utilising software packages and tools:

1. Centralised filing system: Reference to previous audit files is quite common in regular audit. Inability to centralise such filing system duplicates audit effort.
2. Centralisation of audit personnel: Inability to centralise the audit personnel location causes another deficiency in utilising software.
3. Absence of benchmarks: Benchmarks for evaluating the performance of audit are not available.
4. Quantitative analysis: Software tools are used only for simple recording rather than for quantitative analysis. Such simple analysis helps an auditor to undertake tests as complex as digital analysis.

Simple software packages like MS office may be helpful but not sufficient for optimal auditing.

Data mining tools

Auditor can find several data mining tools that minimises the audit risk by eliminating the sampling risk. For example, data can be selected and sorted from the data warehouse making the sample selection easy. Availability of critical data helps in easy analysis and investigative audits.

However, there is a possibility for data alteration by auditee. Therefore an auditor should verify that the data is not tainted and it is raw. Further, an auditor should take care about the reliability of the data extracted.

Risk assessment tools

Several tools are available to automate the audit process. For example, Lotus Notes, audit software helps in consolidating the administration, planning, budgeting and risk assessment work. Audtoaudit2000, another tool helps in better management of audit process. Work paper review is made easy.

TeamMate2000 allows real-time access even from remote areas. Work paper review is made electronic.

Planning and risk assessment

Planning and risk assessment can be made easy by implementing high-level audit software. Several software tools like Visual Assurance (Delloite & Touche), Price Waterhouse Controls and Comet by PriceWaterHouse are available. These tools enable an auditor to examine the computer processing function, identifying the frauds and high-risks transactions. Thus planning and implementation of audit becomes effective. Further such tools also provide a risk assessment method.

Software requirements must be determined on the basis of organisational needs. The following are some of the additional steps for optimum software utilisation:

1. Proper training on software must be provided to the selected people.
2. Select a responsible person for the project.
3. Audit clerks performance in using the techniques must be evaluated
4. Maintain close contacts with technical people to avoid difficulties in implementation

Further, establishing benchmarks to evaluate the performance also improves the effectiveness of audit.

Answer: [c] Decentralised filing system

Module:1

Reference No:M1090

Question: ----- is a type of error that can be observed during an audit of transactions.

- [a] Only mathematical error
- [b] Only relationship error
- [c] Both mathematical and relationship error
- [d] None of the above

Module 1- Auditing the data relationships - Part 1

Normally transaction analysis forms the basis for any audit, whether in internal audit or external audit. But internal auditors are now increasingly focusing on the transaction analysis.

The audit process

Usually the auditors, using some standard audit tools extract a file from the database. Then the auditors begin to look for anomalies in that file. And more often than not, the file is a conglomerate derived from two or more files. There has been no effective method to examine in detail the relationships between these two files.

Audit objective

It might be argued that such unusual relationships are taken care of by the database itself. But the database is governed by certain predefined rules set by the programmers. The programmers are sometimes ignorant of handling certain unusual relationships. Therefore it is necessary to have an effective control procedure in place, in order to at least prevent these unusual relationships. In this context, the role of the auditor assumes significance in ensuring that such controls exist in the first place.

Method of examining such relationships

In this article we have explained in detail a method of examining relationships. This consists of using forms that help in both documenting the relationships and in understanding them. And then by using the combined

facilities of certain standard audit tools we can obtain the results of our examination. There are three stages. They are

- Identifying data elements
- Determining relationship
- Actual audit of data

In order to explain this we have used a case study of purchase invoices and cheques drawn. But in reality the situations are much more complicated where the auditor is required to take into account complex relationships.

Consider a normal purchase process in an organisation. Each invoice received is processed by the accounts payable system and cheques are prepared for the invoices. In this regard we have to make the following assumptions

- Only one cheque is prepared for each invoice.
- We can obtain the files of invoices and cheque payments.
- The invoice number is available on the cheque payment records.

This is the end of first step where all the data elements involved in our examinations have been identified.

The next step is to determine the relationships that are possible between these two files.

- One to one: For each invoice there exists one cheque, and hence payment made
- One-to-none- For this invoice no cheque exists, that is no payment has been made for such invoices.
- One-to-many: In this case there exists more than one cheque. However as per our rule, such a relationship should not exist. This is an erroneous relationship.

Part two of the article consists of rest of the stage two and the actual audit.

Answer: [c] Both mathematical and relationship error

Module:1

Reference No:M1091

Question: ----- can be used as a sorting key while examining purchase files and cheque files

- [a] Purchase order number
- [b] Invoice number
- [c] Cheque number
- [d] All of the above

Module 1- Auditing the data relationships – Part 2

This is the second and concluding part of the series on auditing data relationships. In the first part we stressed the importance of auditing the relationships between two data files. We also dealt with auditing the relationships using the facilities provided by certain audit tools as also defining the data elements. In this article we will go on to describe the use of data elements in the forms provided by the audit tools and obtain the results.

For a better understanding of the relationships we can use the form provided by the audit tools. Some of the forms may look like this:

Basically, it is possible to have three relationships and hence this form consists of a 3 by 3 grid. In all, the grid consists of nine cells. The left column indicates the secondary records and the head or the right hand side of the grid consists of primary records or the invoices.

Primary file- Invoice records,			
Sorting key- Invoice number,			
Secondary file- Cheque payment details,			
Sorting key-Invoice number,			
Primary records,			
Secondary records	None	One	Many
None	Not possible 0 records	One-to none This indicates unpaid invoices-determine why any invoice is unpaid over 120 days Xxxx no of records.	Many to one This could indicate identical invoices-determine why subsequent invoices were not rejected Yyyy no of record.
One	None- to- one This indicates the existence of only a cheque but not an invoice-to be investigated further	One-to-one., This is a correct relationship. But we just have to ensure that cheque amount and invoice amount match.	Many-to-one., This could indicate identical invoices for which one payment is made. We need to determine whether the payment is valid and why subsequent invoices were not rejected.
Many	None-to-many. This is a serious situation. This indicates many cheques payment for which no invoice has been raised- will have to be thoroughly examined.,	One-to-many., This indicates that a single invoice was paid through more than one cheque. This is against the policies of the companies.,	Many-to-many. Identical invoices with many cheques-to be checked for duplication

Each of the cells indicates the relationships that are possible between these two files. As indicated earlier basically three relationships can be considered as usual. They are

- One invoice with one cheque
- One Invoice with no cheque
- One invoice with more than one cheque

This is only a simple example. But there may be cases wherein we might have to consider one-to two, one-to-four etc. Usually two or more represented by many is adequate. If required we may extend the many columns.

Apart from the above three basic relationships, it may so happen that we might find more than one identical invoices and more than one identical cheques. Ideally it should not happen, but these errors may occur and these types of errors are thrown by the other relationship cells indicated above.

And finally there is one cell viz. none-to-none. This cell only completes the grid and does not have any relevance.

The auditor based on his requirements and risk assessments might decide to fill out the relationships cells, which are most needed. It is not necessary to fill the entire form.

Answer: [b] Invoice number

Module:1

Reference No:M1092

Question: ----- is one of advantages of implementing a continuous monitoring system in audit

- [a] Audit coverage can be increased
- [b] Exception reports can be easily generated
- [c] High-level data analyticals can be used to detect organisation wide relationships
- [d] All of the above

Module 1- Automating the audit process-part 1

The objective of this article is to explain the process involved in automating the audit process. This has been done through taking the example of accounts payable audit. The various parameters and settings involved in the implementation of a continuous monitoring system have been explained in detail. This is the first of a three part series on implementation of a continuous monitoring system.

Before embarking on the various implementations the advantages of implementing such a system have been given below. They are:

- Changes in the system can be quickly adapted to
- Errors, irregularities and mistakes can be highlighted easily
- Audit coverage can be increased
- It becomes easier to understand the clients business
- Exception reports can be easily generated
- High level data analyticals can be used to detect organisation wide relationships
- Thousands of records can be utilised to base our audit reports

Step by step approach of implementing a continuous monitoring

To understand this step-by-step approach let us consider a fictitious company with a turnover of Rs. 300 crore. It has a central processing system at the head office wherein all the payments to vendors are routed through.

The implementation process will have the following stages

- Stage1: Conduct a risk analysis to select an area to automate the process

- Stage2: Estimate all the types of exceptions that can occur
- Stage 3: Plan the frequency of audit
- Stage 4: Implementation, maintenance and if required re-designing the system.

Stage1: Conduct a risk analysis to select an area to automate the process

In the said company, since the purchases consisted of a major portion of the total expenses this year. And also new computer system had been installed in the department. We had selected this area. Its record of last two years even showed a fraud in the purchase department. All these factors were considered to select the purchase area as best suited to implement the continuous monitoring system.

Stage2: Estimate all the types of exceptions that can occur

After the selection of the purchase area, the next step is to select all the exceptions and critical reports. To identify this a process needs to be established to identify all the sources of inputs from various departments. And also the best practices of the industry can be taken into account for this purpose. The various activities involved in this process are as follows:

1. Conduct a walk through for the process flow and review past audit: When a review of the process flow and past audit files, was conducted the following observations were made
 - A clerk perpetuated a fraud by paying numerous cheques of Rs 5000 to a non-existing vendor
 - Managers were requesting that vendors make bills below their approval limits
 - Payments were made prior to finalising the terms with the vendor
 - Duplicate payments
 - Inefficiency in the purchase order system

The next steps involved in the implementation of the CMS has been continued in part two of this article

Answer: [d] All of the above

Module:1

Reference No:M1093

Question: ----- is a risk associated with the accounts payable area

- [a] Unauthorised payments
- [b] Duplicate payments
- [c] Inefficiency in the payments systems
- [d] All of the above

Module 1- Automating the audit process-part 2

This is the second of a three part series on implementation of a continuous monitoring system. The implementation process will have the following stages

- Stage1: Conduct a risk analysis to select an area to automate the process
- Stage2: Estimate all the types of exceptions that can occur
- Stage 3: Plan the frequency of audit
- Stage 4: Implementation, maintenance and if required re-designing the system.

The first part of the article dealt with stage 1 of the implementation process and part of stage 2 of the process. In this part we continue with stage 2 of the process.

2. Review best practices and external observations

After selection of around 25 reports during review of process flow and past audits, the next step is to review the best practices in the industry. This could be done by going through various re-engineering and enhancement industry books and magazines. There could also be participation in the various mailing lists devoted to auditing. These mailing lists can be used to interact with other auditors.

3. Interaction with the operations personnel

After all these stages, the next step is to interact with the various important personnel in the operations department. During this stage it is necessary to interview the accounts payable manager, purchasing manager and the controller. The various personnel could be interviewed in the following aspects:

- **Identification of risks:** There should be interaction with the personnel to identify the various risks involved in the purchase/accounts payable process. The risk areas could be unauthorised payments/purchases, inefficiency, duplicate payments etc.
- **Factors impacting the risks:** Various documents, flow charts, input screens, security of the database, controls of the system etc. should be reviewed to assess the factors that could increase the above-identified risks.
- **Identification of risk monitoring tools:** The tools that are currently being used for risk monitoring will also have to be identified. These tools could be budgetary comparisons, ratio analysis, generation of exception reports, planning documents etc.

It is also important to note that everyone needs to be involved in the entire review and interview process. All levels of employee's junior, senior level should also be involved in the discussion personnel. Apart from them, the managers of other departments can also be interviewed, as these people might be willing to share mistakes and weaknesses in the system.

At the end of these discussions, steps should be initiated to compile a report that covers all the aspects of monitoring. All the relevant personnel should be involved in this initiative. This report should contain all possible scenarios wherein things could go wrong. The requirements of these reports should be able to detect and highlight all these possible errors situations. In order to create this report a time frame and project plan should be designed. This will ensure that the report will be created in defined time. And it can also be ensured that adequate approvals can also be obtained to verify the validity of the reports. In the final meeting the report can be discussed and finalised and the frequencies of the report generation can be finalised.

In the third and concluding part the last two stages with examples have been discussed in detail.

Answer: [d] All of the above

Module: 1

Reference No: M1094

Question: ----- report would highlight ineffective approval process

[a] Invoices with dates prior to purchase order dates

- [b] Payments to vendors that do not exist in vendor master file
- [c] Multiple payments to vendor under approval limits
- [d] All of the above

Module 1- Automating the audit process-part 3

This is the third and the concluding part of the series on implementation of a continuous monitoring system. The previous two parts dealt with stage 1 and stage 2 of the implementation process and part of stage 2 of the process. In this part we have discussed stage 3 of the implementation process.

Stage 3 -Plan the frequency of audit

Once the continuous monitoring report has been framed the concerned authorities must approve it. The next step thereafter is to decide on the frequency of the reports. The report can be generated either on a weekly, fortnightly monthly or a quarterly basis. The ideal frequency would be monthly. But again this would depend on the gravity of the subject matter. After finalising the periodicity of the report , the next step is to decide on the number of exception reports that needs to be reviewed. Although it would be ideal to review all the exception reports, the time and the cost factor might not permit it. In order to make an efficient use of the resources of the organisation, it is best to define a cut off limit for the exception reports to be reviewed. Even the time required to review each report can also be set up for a detail plan of the audit. Since there is very little human intervention, the time and cost factor for computer processing can be more or less accurately estimated. In most of the studies conducted it is found that total cost factor involved is more than compensated by the revenue leakage this system prevents.

Stage 4- Implementation, maintenance and if required re-designing the system.

The last stage is to actually implement the continuous monitoring system. Actual implementation involves determination of the data files that the reports and analysis should be based on. In our case study of accounts payable area, normally three data files can be used to generate reports. These are the files containing the details of each payments made to vendor and which is linked to the vendors invoice, the master file of the vendors which gives the details about each vendor and product he handles and the ledger containing the details about the purchase orders. This purchase order register should contain details about open purchase orders, approved orders and payments made against them.

As indicated above this system needs to be reviewed for any changes that need to be made and constantly re-designed as per changing circumstances.

Sample reports that are generated by the continuous monitoring system

Analytical reports

1. Total payments towards purchase order as against not towards any purchase orders.
2. Stratification of vendor checks over the past twelve months
3. Stratification of average days payable outstanding

Exception reports

1. Invoice dates prior to purchase order dates
2. Payments to vendor that do not exist in the master file etc.

Answer: [a] Invoices with dates prior to purchase order dates

Module:1

Reference No:M1095

Question: Which of the following questions statements is true with regard to using the usage of SQL based query tools in auditing?

- [a] They can be used in all computing environments.
- [b] They can be used only when data is stored in relational data bases.
- [c] It performs the functions of the a generalised audit software also.
- [d] All of the above

Module 1- SQL based data analysis

SQL is an internationally acknowledged language for manipulation of data that is contained in the relational databases. This query language can be used by the auditors for accessing the data from any type of relational database that is maintained by the company. In view of this standardisation, almost any SQL based query tool can be used for any relational data base management systems.

An example

When Giga bytes of data tables are maintained with certain clients, a general ledger that can have millions of transactions each year it would will become difficult for auditors to download all that data into a general audit software. As this would involve an extensive reformatting by the general audit software exercise to make the data readable by the general

audit software. This would invariably slows down the entire audit process and. will This also took require additional human resources and personnel deployment.

All these problems issues prompted the auditors to use SQL in addition to the other audit software tools. Now, the agency data was could be directly accessed using SQL and its powerful query tool was used to get customised reports required for the audit .

Benefits of SQL based query tools

The benefits of using SQL tools are many. The major one being a direct access to the data. Other benefits are as follows:

1. **Greater flexibility-** Even if the auditors can now access the necessary information don't know what specific data they want just before the start of an audit, they by can have a look at the logging into the relevant database available easily and then use the relevant info for the audit.
2. **Greater accessibility-** With a more convenient downloading process, The auditors need not confine themselves to a particular data set. set they extracted, because the downloading process now is very convenient. They can go back to the re-check the data set how as many ever times as they want.
3. **Simplified process-** Since the access is available to the whole system as such, even if the an auditors can write a query and get the correct information, if he finds that he has extracted the wrong data. find out they have extracted the wrong data, now all they need to do is write a new query.

Disadvantages of SQL based query tools

SQL based query tools cannot be used in those cases wherein the when the organisation's data is not stored in a relational database environment. And moreover the SQL tools do not come with the normal audit and financial routines. Hence, most of the time SQL tools are often used in combination to with the general audit software tools. In such cases, SQL

is used to extract data, and the general audit software, to perform the analysis.

The approach

The best approach for the auditors would be to use a combination of tools available in the market. Although it is convenient to use one audit tool for the entire audit, it is practically impossible as to sift through the deluge of today the information is available in various forms and shapes available today. Hence, the auditors need to be flexible and go ahead with the use tools that is best suited for the situation on hand.

Answer: [b] They can be used only when data is stored in relational data bases.

Module:1

Reference No:M1096

Question: Which of the following audit objective complies with the functionality criteria of ISO in an ISO standards audit?

- [a] Utility of the software under development
- [b] Technical functionality of the software.
- [c] It performs the functions of the a generalised audit software also.
- [d] All of the above

Module 1- ISO standards based IT audit

ISO standards constitute an important baseline for auditors to verify and validate the efficiency and utility of the software. Although traditional IT audits also assist in bringing the right technology to users, there are many attributes of the software development that cannot be verified without the help of the ISO standards. These standards provide a guideline for the auditors to verify certain aspects of the software development project, which will ultimately result in a more appropriate technology for the final end users.

ISO audit objective

The main objective is to establish that the technology, service or process being developed conforms to specified characteristics. The team developing the product defines these characteristics. The actual attributes of the project are measured against the above-defined characteristics by the team.

Also using the ISO standards based approach the auditors can validate that the ultimate product confirms to the initial specifications.

The approach

In this approach the certification given by the independent and third party provides an assurance that the technology, process or service confirms to the pre-defined characteristics. The standards, which is used here, is the ISO standards 9126 which is applicable for software development products and the related documentation. ISO standards were developed by nearly 140-nation alliance, which consisted of representatives from all strata of the society like public and private organisations, consumers, industry, government and international organisation.

Sample audit template

We have given below sample ISO criteria that can be utilised for auditing certain aspects of software development

ISO	Criteria Documents prescribed by ISO	Related audit objective that can be fulfilled
Functionality	Original Test matrix	Is the technology really functional?
Reliability	Requirements analysis	Does the application perform as required under defined conditions for a defined period of time?
Usability	Marketing requirements software requirements specifications	Is the application useful to customers as described by marketing?
Efficiency	Product requirements documents	Is the application convenient to maintain?
Maintainability	Onsite interviews	What is the degree of convenience to the development team to make the required modifications to the application?
Portability	System design requirements	Is the software transferable from one environment to another?

Common features observed in such audits

It is generally observed that in many organisations a formal requirements analysis document is not prepared. Such requirements take various forms and shapes like informal specifications; information flow oriented specifications structure oriented or object oriented specifications. Sometimes the chief technologist may just jot down the specifications on white board. But whatever be the specification type, it is important for the auditor to obtain and maintain them, to facilitate formalisation.

Auditors would generally know the contents of specific documents. If these requirements are not available in writing, it should be formalised and the information confirmed by the specific person.

Answer: [b] Technical functionality of the software.

Module:1

Reference No:M1098

Question: The use of CAAT in inventory audit helps the auditor to

- [a] Identify slow moving inventory
- [b] Analyse the inventory requirements
- [c] Classify the controls for implementing appropriate controls
- [d] Monitor the inventory transaction

Module 1- Audit of Inventory control through CAAT - Case Study

Inventory cost is one of the major components of the cost structure in an organisation. Management constantly strives to reduce these costs by trying to reduce storage and transportation cost. In this article we will deal with audit of inventory control and explain the same with a real case study.

Importance of inventory control to management

Inventory control helps the management to

- Monitor inventory transactions
- Analyse the requirements
- Classify the stock for implementing appropriate controls
- Enables future planning

Due to its importance, inventory becomes one of the critical areas of the audit.

Audit of inventory controls and use of CAAT (Computer Assisted Audit Techniques)

The audit of inventory is a cumbersome process. The auditors should physically verify the correctness on inventory and analyse large volume of records. Also he must ensure that the management has correctly identified slow-moving, obsolete, scrapped and damaged items.

CAAT can help the auditors in performing a detailed analysis covering larger volume of transactions, combine multiple files and records into one database and maintain the integrity of data. CAAT also provides for comparison of inventory and sales, master file and transaction file data, age analysis and the like.

Case study

This case study highlights the advantages of using CAAT in audit.

Let us understand this in the context of a company called BMV that is involved in exploring oil. The entire IT system is computerised including the inventory. The inventory department consists of three sections - material planning and control, receipt and custody.

Material receipt section checks the materials that are received against the purchase orders and creates an inventory-delivery receipt and goods received notes (GRN) for the custody section.

At the custody section the GRN is received and after verification is sent to accounts department. It also issues the materials for various jobs based on issue vouchers generated by it. The system also provides for return of all unused, used and serviceable goods and the like through material return vouchers.

Audit

During the course of audit it was discovered that the company was making profits even though other companies had a decline in their profits. This led to the verification of inventories. The auditors with the help of CAT analysed the inventory database. This consisted of goods received, goods issued - their data, value, return data and value of returned goods.

With the help of CAAT, the auditors were able to find out that out of 150 records of returned goods only 4 records had a significant value and other records had zero value. This difference in value raised suspicion, which made the auditors delve further. The enquiry revealed that it was management's practice to assign zero value to materials that were returned after use, as it was difficult to evaluate their value. But the returned goods were new and not used.

The management was able to manipulate the accounts to show higher profits to shareholders about the inventory and better position of the company. This practice of inventory management helped to hide indiscriminate purchases, those that were not required for production. They would buy the materials required by them, 'issue' to a production and return it. When received by the stores they would be assigned zero value. Thus the number and value of inventory was reduced wherein the company was able to depict a rosy picture about inventory management.

Thus without the employment of CAAT tools, it would have been difficult to reveal this fraud.

Answer: [b] Identify slow moving inventory

Module:1

Reference No:M1099

Question: Which of the following ratios will indicate an unusual payment to a vendor?

- [a] Highest to lowest
- [b] Highest to next highest
- [c] Comparison between two numeric fields
- [d] All of the above

Module 1- Ratio analysis -A data analysis technique

One of the most under-estimated digital analysis techniques is the ratio analysis. Ratio analysis is a much more powerful analysis technique than the oft-used Benford's Law. Benford's law only highlights the set transactions for instance begins with a certain amount and exists more than the pre-defined number of times. For instance the number 250 occurred 100 times more than set limit of 50 times. But the problem lies further; it becomes very difficult to identify which of 50 excess transactions are fraudulent or problematic. In this matter ratio analysis comes to [our help in the sense that it helps us exactly pin point the fraudulent transactions.

Commonly Employed Ratios

- Highest to the lowest. Maximum/minimum
- Highest to the next highest i.e. maximum/second highest
- One numeric field to another. For instance, figures of one particular year are compared to the previous year's figures. (field 2002/field 2001)

Examples

1. Highest to the lowest

If the auditors want to identify whether the prices charged for customers are reasonable, the best ratio would be the highest to the lowest. The ratio to be calculated would be the maximum sales price to minimum sales price for each type of product. If the ratio is close to 1 then the auditor can safely presume that there is no great variance between the sales prices charged for different customers.

On the other hand if the ratio is greater than 1 it becomes a matter of concern to the auditor and would be an indication that either a customer is being highly charged or some customer is being undercharged. Auditors can then examine only those transactions that show a variance of more than 1.

2. Highest to the next highest

This ratio can also be used to identify possible fraudulent transactions. For instance this ratio can be utilised in the review of payable accounts. This analysis can be used to compare the vendor payments.

Sample result of a ratio analysis

Supplier	Highest payment	Second highest Payment	Highest/2nd highest ratio	Minimum payment	No of payments between min and 2nd highest
ABC Ltd	Rs 242538	50542	4.80	12368	133

In this case it is clearly evident that there is large difference between the highest and second highest payment. This can be especially problematic when it is observed that 133 number of transactions between min and the second highest transaction. This can indicate an unusual transaction, which the auditor can pick for further verification.

3. One numeric field to another

Another and most often used ratio analysis is comparison of data between two entities. For instances between two years, between two organisations, two locations two departments etc. When the variance is very large for instance if the purchases from certain supplier for two years and there is a significant decrease or increase this can be further investigated.

Conclusions

Ratio analysis can be a very useful digital analysis technique in current business scenario. When there are millions of transactions conducted per day, auditing a selected few transactions may not be very effective and may not fully indicate the problematic transactions. In such matters ratio analysis can be of immense help and mitigate the risks of the auditors to a great extent.

Answer: [b] Highest to next highest

Module:1

Reference No:M1100

Question: Vulnerability assessment is difficult as threat occurrence is unpredictable. Which of the following is an alternative to minimise the security risk?

- [a] Protection of sensitive data
- [b] Improving the efficiency of operations
- [c] Insurance options
- [d] None of the above

Module 1- Return on Security Investment and Insurance options

Measuring return on security investment (ROSI) is not an easy task due to the complications involved in measuring benefits of security. Some argue that there exists no return on security investment. Security investment, however, does not contribute revenues to the business directly. It can of course minimise the damages that may occur due to corruption of sensitive data, which will in turn protect the earnings. It contributes through improving the effectiveness and efficiency of operations.

Any security attack will have a subsequent affect on the company's market value or brand value. But it is difficult to determine the financial loss of such attacks. Professionals and researchers have perceived ROSI as "investment versus chance of something occurring multiplied by the severity of the problem".

However, it is not clear because of the uncertainty factor. Therefore, the security related activities have to be identified. And the impact of security solution on such activities has to be determined. For example, reduction in the manual inspection costs is the return on investment in intrusion detection measures.

Cost-effective analysis

Sometimes decisions involve taking into account the intangible factors. In such cases, risks cannot be quantified. Then a cost-effective analysis is the best-suited method. This approach helps in selecting the highest benefit providing opportunity in comparison to its investment. However, the quantum of investment or the return on investment cannot be determined using this approach.

Insurance options - an effective alternative

Insurance options can be cost-effective alternative for minimising the security risk. Risk management has been the main function of insurance and the objective of security is also risk management. Therefore, management of information security risk is providing a new market for insurance. Coverage provided by the insurance companies must be properly evaluated, as there have been constant changes to the products. Cost of insurance must also be considered. At the same time, the magnitude of risk and the ability of the insurer to pay the policy amount in case of attack are important considerations.

Insurance companies involvement in security risk management does not mean that they will provide security products. But they assume the company's risk. It minimises the burden of insured parties.

But one difficulty associated with insurance options for security risk is the premium calculation. However, this is not a major issue because insurance companies are capable of determining appropriate premiums. In future network security insurance will be as common as fire or theft insurance. Companies are ready to take security insurance as it brings cost savings to them in the long run.

Evaluation

Finally it is essential to evaluate all the options available so as to build a cost-effective security strategy.

Answer: [c] Insurance options

Module:1

Reference No:M1101

Question: Which of the following is/are involved in effective risk assessment process?

- [a] Setting an objective
- [b] Identifying areas prone to risks
- [c] Assigning values to risks
- [d] All the above

Module 1- Risk Management - Benefits

IT managers can not avoid protecting networks from threats and dangers. The older methods of common sense, intuition and good luck are being replaced with structured and scientific methods commonly termed as risk management.

Risk Management in IT

IT companies have become more prone to network-related threats due to the increase in virtual private networks, e-commerce and mobile workers. Threats ranging from hackers to viruses, systems overload to insider misuse can destroy the network of an organisation. Network security risk management enables IT managers to measure the assets and vulnerabilities of the network in a systematic manner while constantly monitoring the security baseline.

Network security risk management can help IT managers recognise the risk which will affect a company's business most, and the security expenditures which yield the best return on investment.

Assessment

Assessment is the first step in risk management. The basic objective of assessment is to identify network security vulnerabilities. Although there are no specific risk assessment tools, a few companies employ methodologies and calculations. Others use a qualitative question-and-answer method. Every method involves varying degrees of uncertainty.

The procedure for sound assessment involves:

1. **Setting an objective:** CIOs and IT managers should spell out their reasons for implementing risk management. The underlying reason behind risk management is to manage and improve the company's revenues.
2. **Including inventory critical systems/assets:** IT managers should include everything they consider worth protecting as inventory. The inventory should spread across all systems, services and components and include proprietary data, content, passwords, services etc.
3. **Identify threats:** Every person or thing, who is considered a threat to the network should be identified. These threats could be hackers, viruses, human error, system failure and the like.
4. **Identify areas prone to risks:** Identify areas which provide entry to threats, these could include points of network entry, available applications, servers etc.
5. **Assign values to risks:** Since a company cannot provide 100% protection from all risks, it needs to prioritise its expenditure and efforts based on the momentum of the threat. The momentum can be calculated by assigning values and employing a basic equation $\text{Risk} = \text{Assets} \times \text{Threats} \times \text{Vulnerabilities}$.
6. **Planning:** Clarity in communication across all departments and senior-level buy-in, are two factors which contribute towards the success of risk management planning.

Activities in planning include-

- **Developing policies:** It is essential to develop policies as they define the Hows, Whys, When, and By Whoms of security procedures.
- **Setting up a security audit process:** Constant reviews help IT managers measure the effectiveness of their security strategy. Some questions which need to be addressed before audits are conducted include; Who will conduct the review? Will the process be kept in-house? Or given to a third party? What methods will be used to analyse security data? What parties will review the data? Who will determine whether security system reforms are necessary?
- **Establishing technical procedures:** When a potentially risky technology is being employed, "What if" situations should be anticipated and dealt with.
- **In case of security breaches:** Set procedures for IT and users to follow when there is a hack attack, virus, or other kind of security breach. Whom to notify if a virus is discovered? The situations in which IT should shut down the corporate e-mail server or network? How will IT communicate emergency messages to users.
- **In case of changes to network configuration:** Allocate a person for making changes to network configuration, and also define why and when he should make changes to the network.
- **In case of new applications:** Determine a procedure for testing new applications before roll-out. Determine who is charge for data conversion. Determine steps for integrating new applications with users.
- **Form an incident response team to make contingency plans:** Incident response team members have pre-assigned responsibilities for emergency situations. Select an incident response team leader to set team operation policies. Network-wide contingency plans take care of back-up server provisions, additional manpower, expert consultant resources, vendor services and relations.

Answer: [d] All the above

Module:1

Reference No:M1102

Question: IT framework to be developed by the management need not focus on

- [a] Alignment of IT with business
- [b] Value derived from IT
- [c] Management of risks that arise from IT
- [d] Checking for technological obsolescence

Module 1- Managing IT

Technological advancements have made any time anywhere commerce a reality. Companies big or small spend millions in infrastructure and technology to cope with the developments and thereby sustaining its market, customers and superiority over its competitors. This raises a question to what extent management is responsible for the IT governance, because they are ultimately answerable to stakeholders.

Managing IT is a tough task, as poorly managed IT shall lead to business losses, damage reputation and reduce competitiveness. Hence there is a need for IT framework to be developed by the management. Management must concentrate on:

- Aligning IT with business
- Ensuring that value is delivered from IT
- Management of risks arising out of IT

There has to be a measure to check results of IT engagement.

The failure of IT is largely due to inadequate attention paid by the management. These include

- Failure to check technology for inadequacies and obsolescence
- Poor support from the top management
- Missed deadlines
- Expected results overridden by increased costs

A well managed IT will add value to business and help for faster operation with appropriate quality and security. The gains would not stop at improved efficiency and productivity but in value creation.

What should the management do to govern IT?

1. Align IT strategy with business strategy
2. Develop appropriate organisational structure to give importance to IT throughout the organisation
3. Percolate IT and business strategy down the organisation
4. Develop and adopt appropriate control and security framework to help IT governance
5. Provide the required IT facilities and infrastructures
6. Train and encourage sharing of information
7. Give responsibilities for risk management spread through the organisation and not make it only the responsibility of top management
8. Focus on IT processes and develop core competencies in IT
9. Develop performance measurement metrics

A general approach

A general approach for good IT governance would be

1. Identifying performance measurement elements consisting of performance drivers and measurement of outcome for all IT process
2. List out critical success factors for all IT process
3. Compare results with the set goals
4. Align where the results show poor comparison

Like any other management IT governance also requires the general management activities involving planning, organising, directing and controlling.

Planning:

- What is the IT investment required?
- What are the capabilities required?
- How would the IT impact the enterprise?
- Fixing roles and responsibilities

Organising

- How to acquire and mobilise resources?
- Sustain current operations
- Improve and increase operations
- Directing
- Set policies and guidelines
- Get expected return
- Assign responsibilities
- Constantly train, inform and make transformation happen
- Keep the personnel informed on the constraints within which to operate

Controlling

- Measure performance
- Manage risk
- Get audited and obtain assurance

At the operational level, the company can follow an approach derived from Maturity Model followed by Software Engineering. This would help in knowing

- The current IT status of the organisation
- The current IT status of best in the industry
- The current IT internal standards
- The strategy to be adopted for improvement

In addition to the Maturity Models, Critical Success Factors (CSF), Key Goal Indicators (KGI) and Key Performance Indicators (KPI) would be useful.

CSF: It defines the important issues that include strategic, operational, organisation and procedural so that the IT process in these areas are under control.

KGI: These indicators help management whether the business objectives are achieved say for example availability of information, efficiency of processes and the like.

KPI: These are measurement of performance against the respective goals.

Answer: [d] Checking for technological obsolescence

Module:1

Reference No:M1031

Question: Penetration testing helps in identifying the vulnerabilities in a network security. Which of the following is not a reason for conducting the test?

- [a] Make the management aware of the security issues
- [b] Test intrusion detection and response capabilities
- [c] Help in decision making process
- [d] Identifying the systems to be tested

Module 1- Penetration Testing - Part 1

Penetration testing helps in identifying the vulnerabilities in the system or the network in which security measures exist. It employs the same method used by hackers or hostile intruders. Trusted individuals conduct the test. Penetration test may vary from a simple scan of the IP addresses to identify machines that offer services or may extend to exploiting known vulnerabilities that exist in an unpatched operating system.

Purpose of test:

1. Makes the management aware of the security issues.
2. Tests intrusion detection and response capabilities.
3. Helps in decision-making processes.

Pre-test phase:

Scope and objective: The scope and objective of the penetration test should be well defined. The objective of the management will be to detect the vulnerabilities existing within the company's network infrastructure. The test will have under its scope the identification of machines, systems and network, operational requirements and the staff to be involved.

Timing and duration: Timing and duration of the test should be decided before the test is conducted so that everyday operations of the company will not be disrupted. It may be decided to run the test at particular times of day.

Identification of the system to be tested: Decision should be made as to which systems should be tested. Not all the systems can be tested, since this may lead to loading of the network in event of heavy and critical use. This will ultimately cause the network to crash. If the management cannot take this risk then some systems or network should be excluded from the test.

Informing the staff: The management must decide whether the staff should be informed about the tests or not. If the staff is informed beforehand about the test it may change their behaviour. This will affect the result of the penetration test. If the management decides not to inform the staff then it may result in them taking actions that may unnecessarily affect the organisations operation. For example, if the management wants to assess the response of the security team to the attack it may not inform the staff about the conduct of the test. Otherwise it will be appropriate to inform them so that the security staff in response to the penetration test takes no action at the decided time and duration.

Preparation of legal documents: Penetration testing strictly speaking, an illegal activity, irrespective of whether it is carried on the external or internal network of the company. It is breaking of law by the penetration testers. Hence the management must prepare legal documents to protect the penetration testers before the test is conducted. Even if the test is conducted by the company's own staff, the legal documents must be prepared as anything can go wrong during the test. The management must also make sure that any information or data that has been obtained during the test should be treated as confidential and should be returned or destroyed after the test.

Before commencing the test, the management and penetration testers should discuss the above matters. Penetration testers should discuss with the management about the conduct of the test, so as to ensure that the test is not affecting the operations of the company. There should be a clear understanding about the time of the conduct of the test.

Answer: [d] Identifying the systems to be tested.

Module:1

Reference No:M1032

Question: Penetration testers in an attempt to penetrate into the system or the network use different techniques to break in. Which of the following techniques do they employ to obtain critical information for the company's employees?

- [a] Password cracking
- [b] Social engineering
- [c] Physical security
- [d] Logical security

Module 1- Penetration Testing - Part 2

The purpose of penetration testing is to identify vulnerabilities in the system or network in which security measures exist. It is a testing which employs method similar to that used by hackers or hostile intruders. Trusted individuals conduct the test.

This is the second of a three part series on penetration testing. In this article we discuss the test phase of penetration testing.

Test phase:

Gathering information: The first step is to carry out a network survey and gather information about the network. This is followed by a port scan and obtaining information about the closed and open ports running on the system or the network. Where they are restricted IP addresses, the penetration test should not be conducted on them. The port scan identifies the list of open ports on a particular IP addresses. Compare the domain registry information to ensure that IP addresses belong to the organisation. The result of this step will be a list of systems and IP address with information about the operating system, running services and open ports. There a number of tools that helps in this process of information gathering and analysis.

Vulnerability Detection: The next step after gathering the above information is determining the vulnerability of each system. Penetration test should obtain the knowledge of all exploits and vulnerabilities. An analysis should be done on all the information obtained to detect for any possible vulnerability. The result of this step will be the list of targets that should be investigated in depth.

Penetration attempt: In this step, targets for penetration attempts should be identified. An estimate should be made of how long the test would take on a particular system. The system that is selected for the test should be of some relevance. For example if the company has a network of 200 systems and on the basis of information gathered it is found that they have 7 servers then it will make more sense if the test is limited to these servers instead of testing all the systems. After choosing the target the penetration test should be performed. Penetration into the system can be through password cracking, social engineering and testing the company's physical security.

Password cracking: In password cracking, the penetration tester uses tools for making a combination of all possible words e.g. Hybrid crack that tests for passwords that are variation of the words in a dictionary file.

Social engineering: The penetration tester obtains critical information from the company's employees using the art of social engineering. For example,

Attacker: "Hi Surekha this is Mahitha from the IS department. There is a virus in your mailbox. Can I have your password so that I can remove the virus?"

Surekha: "Oh! Please remove the virus, my password is Deepa"

Physical security: The penetration tester tries to gain access to the company's physical security. Social engineering can also be used in this method.

Reporting: The report should contain

- An overview of the tests done
- Analysis and commentary on critical vulnerabilities
- Vital vulnerabilities
- Less vital vulnerabilities

Vital and not so vital vulnerabilities should be shown separately, as the management may be ready to accept the risk in case of less vital vulnerabilities. The classification helps the management in decision-making. Besides these, the report should outline the result of the successful penetration with the details of all the information that was gathered during the test. The report should give suggestions to resolve the vulnerabilities found, by explaining the list of all the vulnerabilities that were found, giving a description of the same and the techniques to resolve them.

Answer: [b] Social engineering.

Module:1

Reference No:M1033

Question: Which activity is taken up during post-test phase of penetration testing?

- [a] Cleaning up
- [b] Vulnerability detection
- [c] Preparation of legal documents
- [d] Penetration attempt

Module 1- Penetration Testing - Part 3

Penetration testing helps in identifying vulnerabilities which exist in the system or network in which security measures exist. It is testing which employs method used by hackers or hostile intruders. The test is conducted by trusted individuals.

This is the concluding article of a three part series. This article deals with post-test phase and the limitations of penetration testing.

Post-test phase:

Cleaning up: The changes that had been made during the penetration testing to the system or network must be cleaned. This is done during the cleaning up process. A detailed list of all actions performed during the penetration test must be kept. Compromised hosts must be cleaned carefully so as not to affect the company's normal operations. The company's staff must verify that the clean up has been done. One of the ways to do is to remove the user account created by the penetration tester. The responsibility of cleaning lies with the penetration testers. They should also inform the company of the changes that have been made to the system consequent to the test.

Limitations of Penetration Testing: Penetration testing is not the best way to find the vulnerabilities. Not

finding any vulnerabilities does not necessarily make the systems secure from the hackers or intruders. The following are the limitations of penetration testing:

- Penetration tests are conducted for a limited time period only. It is just a snapshot of system or network security. It gives the status of a particular time.
- Penetration tests are usually carried out as black box exercises where the tester does not have complete information of the system being tested.
- The test may not identify a vulnerability that is obvious to anyone with access to internal information about the machine.
- The test can identify only those vulnerabilities that it is designed to look for.
- If any service is not tested, then there will be no information about its security or insecurity.
- The test will not provide information about new vulnerabilities that are discovered after the test is carried out.

Conclusion: Penetration testing emulates the real world attack to some extent. Penetration testing should not be confused with network security assessment. The network security or vulnerability assessment does not give the accurate picture. . But in penetration testing the testers in order to determine the vulnerability that exists in the system try to penetrate in the system as a hacker would.

Penetration testing does not guarantee that the intruder will not find any vulnerability. If the penetration tester finding 4 holes in a system is no guarantee to the fact that the hacker will not find more holes. Hackers and intruders have to find only one hole to exploit, whereas the penetration testers task to find as many as possible holes that exist. Moreover they have to complete the task within the set time frame. Penetration test by itself does not improve the security of the system or the network. The management should take action to address the vulnerabilities that are found as a result of conducting the penetration test.

Answer: [a] Cleaning up.

Module:2

Reference No: M2001

Question: In a network security policy, a statement on methods of data communication will be listed under

- [a] Identification and authentication
- [b] Accountability and audit
- [c] Data exchange
- [d] Access control

Module 2 - Detailed Network Security Policy

A detailed policy on security issues should cover the following aspects:

- (i) Documentation
- (ii) Identification and authentication
- (iii) Accountability and audit
- (iv) Access control
- (v) Accuracy
- (vi) Data exchange
- (vii) Reliability of service/availability

Documentation

Objective - To document all assets. Consider :

- What are the assets/ devices to be documented along with their location?
- Who and how will assets be identified?
- Who will be in charge of these documents?
- Who can authorise changes-/add/ modify to documents?
- Who can have access to documents?
- What are the reports and periodicity of reports required?

Identification and Authentication

Objective - To identify and authenticate all subjects on the network. Consider:

- Who should authorise permission to the user for system/ devices and applications?
- Who is responsible to maintain a log of users, preferably through a single mechanism across multiple applications and systems?

Accountability and Audit

Objective - To make users adhere to network policy. Consider: · How often should logs be reviewed?

- Who is in charge of reviewing them?
- What type of exceptional report should be prepared?
- Which method to adopt for identifying unauthorised users?
- What action should be taken against unauthorised users?
- What measures should be adopted to prevent unauthorised usage?
- What is the periodicity of audit?

Access control

Objective - To provide access to users on a need basis. Consider:· What is the method of identifying network services and disabling them?

- How should devices and data be labeled-as open access, restricted access or highly restricted access?
- What types of tools should be used for access control?
- What is the physical arrangement of devices in case of restricted access?

Accuracy:

Objective - To maintain the integrity of information. Consider: Who are the owners? What type of data do they own?

- What are the tools employed to check integrity of data?
- What are the mechanisms to identify and check the functionality of such tools at regular intervals?

Data Exchange:

Objective - Monitor information when they are transmitted to different devices in the network. Consider:

- What are the guidelines to communicate different types of information?
- Which type of information should be encrypted?
- Who will assess the confidentiality level of information and authorise the same to be sent in encrypted form?
- Who will classify the data?

- Who will receive what type of information and in what form?
- What type of identification will be used while sending and receiving the message?

Reliability of service

Objective - To make the services and resources available to users. Consider:

- Which services will be available round the clock /for a limited period?
- What is the periodicity of regular maintenance?
- What is the alternative arrangement of resources and services during maintenance period?
- Who will monitor regular functioning of the network?
- What is the immediate action to be taken in case serious problems are encountered?
- Who is authorised to take immediate action?
- Who is authorised to change configuration?
- Who is authorised to prepare periodical reports?

Answer: [c] Data exchange.

Module: 2

Reference: M2002

Question: A network security policy need not include

- [a] A security matrix table
- [b] Penetration testing
- [c] Risk analysis
- [d] Network assets

Module 2 - Network policy I

While framing a network policy, matters related to usage, risk, monitoring, review etc. should also be considered in addition to the general guidelines for framing a policy (covered in a separate article).

Based on these guidelines you can determine specific assets related to the network and user group. Some of the specific network assets are-

- Core network devices eg. ATM switches
- Distributed network devices eg. Network routers
- Access network devices eg. Closet switches, ISDN or dial up servers, firewalls
- Network monitoring devices
- Network security devices
- E-mail systems
- Network file servers
- Network print servers
- Network application servers
- Data Application servers eg. Oracle and other stand-alone applications
- Desk computers
- Other devices like standalone print servers, network fax machines etc.

Network devices like switches, routers etc. should also be identified.

The user group may consist of -

- Administrators who are responsible for the network
- Users who need greater access
- Users within the organization
- Users outside the organization with access to some resources
- Customers or other users

After identifying the assets and the users, perform a risk analysis by categorising the risk into low risk, medium risk and high risk.

Low risk - The risk does not disrupt the business or cause any legal or financial implication. The business can be easily restored and further damage to any other data or system can be easily prevented.

Medium risk - The business may not be seriously effected and normalcy can be restored easily. Further damage to any other data or system is not possible.

High risk - The business can be disrupted causing major financial or legal implications. Rebuilding the business requires significant effort.

The security matrix table should be framed for each network resource and for its corresponding risk and user group. Following is a model of the security matrix. The risk level may change depending on the structure of the organisation.

Assets	Asset classification	Risk Level	Type of users
ATM switches	Core network devices	High	Administrators (for configuration) Others (for transmitting)
Network routers	Distribution network device	High	Administrators (for configuration) Others (for transmitting)
Closet switches	Access network device	Medium	Administrators (for configuration) Others (for transmitting)
Firewall	Access network device	High	Administrators (for configuration) Others (for transmitting)
DNS or DHCP servers	Network application	Medium	Administrators (for configuration) Other users (usage)
External e-mail	Network application	Low	Administrators (for configuration) Server Others (for transmitting mails between the Internet and the server)
Internal e-mail	Network application	Medium	Administrators (for configuration) Server Other internal users (for transmitting mails)
Oracle	Network application	Medium	Administrators (for administration) Database or High Other users

			(for data updates or access)

Managing risk requires balancing usability and business requirements against the risks. After framing the network policy the organisation has to implement the policy with the help of the security team, alter the policy when required, review it etc. This is covered in a different article.

Answer: [b] Penetration testing.

Explanation - Penetration Testing is done to determine the effectiveness of security measures.

Module: 2

Reference: M2003

Question: A general guideline of a security policy does not

- [a] Identify and determine what is to be protected
- [b] Identify acceptable activities
- [c] Update the policy
- [d] Keep the policy a secret

Module 2 - Security Policy

A security policy is a statement that provides a framework to achieve goals related to confidentiality. It is also a statement of information values, protection responsibilities and the company's commitment to security.

The security policy should

- Be concise
- Be based on business objectives
- Easy to understand
- Backed by appropriate security tools
- Balance productivity and security
- Not require frequent changes, but should be flexible enough to continuously keep pace with changes in technology and employee requirements
- Specify disciplinary measures that will be adopted, if security is breached
- Identify persons responsible for the implementation of the policy. Describe methods to educate and train employees
- Explain procedures to evaluate effectiveness

A separate security policy should be framed for information security, personnel security, physical and environmental security, network security, application development and business continuity. These policies should not be in conflict with each other or with the general security policy.

The following steps are useful for developing a policy:

1. Identify: Identify data, people, environment network and the like that has to be protected. Take an inventory of all systems.
2. Prioritise: Allocate priority based on vulnerabilities in the systems.

3. **Assign:** Determine the acceptable level of risk and assign the risk factor. However, eliminating all losses is either impossible or too expensive.
4. **List:** Identify acceptable activities. For example, an activity within an acceptable limit can be the installation of antivirus software, and an activity outside the acceptable limit can be opening an attachment from an unknown source.
5. **Communicate:** Keep employees posted of the dos and don'ts. Also, provide training.
6. **Update:** Revised the policy periodically. Identify a person who can don the role of an administrator, and enforce the policy.

Individuals who need to be involved while framing a security policy:

1. Security administrator
2. IT staff
3. A representative from each corporate function
4. Security response team
5. A representative of the management
6. Legal counsel

Key success factors: Implementation

- Support and commitment of the management
- Evaluation of security risks
- Communication
- Evaluation of the policy by a third party

Answer: [d] Keep the policy a secret

The policy should be communicated to all employees of the company, and should not be kept a secret.

Module: 2

Reference: M2004

Question: Which of the following is not true (with regard passwords)?

- [a] It should be communicated to the management.
- [b] It should not be written anywhere.
- [c] It should not be written in plain text.
- [d] Users should not be allowed to use the previous password.

Module 2- Password Policy

A password is a series of characters, which ensures that only a valid user can access the system. Each user has a unique username and password, which defines his identity and allows access to the system.

A password policy defines rules that need to be followed and helps to create effective passwords. It should clearly state that:

- Passwords cannot be shared.
- They should not be written anywhere. Passwords should not be transmitted over e-mails or other electronic media.
- They should not be very simple.

- Passwords are valid only for a stipulated period. At the system level (eg. application administration accounts) they must be changed on a quarterly basis; user level passwords (eg. Email, web, desk computer) must be changed at least every six months.
- User passwords should be synchronised across platforms.
- They should be stored in encrypted form.
- The use of previous three passwords should be disallowed.

The "Remember password" feature of applications should not be used, as far as possible. Accounts should be locked after a specified number of incorrect login attempts.

Choose a password

- Which has at least two alphabetic character (a-z, A-Z) and at least one numeric (0-9), or special (punctuation) character
- Which is six to eight characters long

Don't choose a password With more than eight characters

- With login name in any form (eg. reversed, capitalised and the like)
- With your first or last name in any form
- With spouse's or child's name With any other information that can be easily obtained eg. Licence plate number, telephone numbers, birth date and the like
- With all digits or the same letter.
- Which is a word found in dictionary
- Which was used earlier
- Which is similar to the previous one

Passwords should not be displayed when being entered, neither should an "*" be shown for each character. Use a password that can be typed quickly, and is hard for someone to hack.

Methods to create a password Choose a password based on a song title, or poem or phrase and use the first letter of each word. For example "This May Be One Way To Remember" and the password could be "TmB1w2R" Use one consonant and one or two vowels. This creates nonsensical words that can be pronounced and are easy to remember. Example "routboo", "quadpop" Use two short words and concatenate them with a punctuation character. For example "donkey+load"

Answer: [a] It should be communicated to the management.

odule: 2

Reference: M2005

Question: _____ is not a component of the network security policy.

- [a] Encryption policy
- [b] HR policy
- [c] Authentication policy
- [d] Access control policy

Module 2 - Components of Network Security Policy

A network security policy outlines effective usage of system resources, mechanisms to prevent security incidents, assets to be protected and the level of protection required. The document must set a standard for employees.

A security policy should be feasible, practical and enforceable. The policy differs depending on the operations of the company. However, generally the components of a security policy are:

Physical security

Confidentiality, availability and integrity of data will be compromised, if the network is not physically secure. Sometimes the corporate network is not limited to a room, but may spread across the globe. The physical security should state ways and means to protect facilities and hardware. It should also define areas that are protected, for which access is only through permission.

Network security

Security regarding access controls, firewalls, network auditing, remote access, directory services, Internet services should be specified.

Access control

Access control table that specifies access rights of every user should include even remote access users. Access control should be simple.

Authentication

Authentication is a process of verifying the user, through the user id and passwords. This system has a drawback, as passwords can be stolen or forgotten. Hence, digital certificates are better to perform authentication.

Encryption

Encryption protects vital data during transmission. It is especially necessary in case of wireless communications, which can be easily tapped. It would also be useful for sensitive transaction such as online purchases through credit cards.

Key management

Keys are required to encrypt and decrypt the data. A proper policy outlining the management of keys should be formulated.

Compliance

Procedures ought to be in place to determine whether the policy is being implemented as desired. It should also include action to be taken in case of violations, and the penalties thereof.

Auditing and review

After implementation of the policy, an audit must be conducted to ensure that the corporate functions are in compliance. It helps to identify areas that are not functioning in accordance with the policy, and areas of improvement. The policy must also be regularly reviewed to be in accordance with business operations.

Security awareness

Employees must be educated about the need to prioritise security. Otherwise, they may make compromises.

Incident response and disaster contingency

The disaster contingency plan helps the management to cope with any type of natural disaster, or attack from hackers, or employees. It must include the procedure for back up of servers, the frequency at which it should be done, and the procedure to store it off site. The plan should also contain a list of members to be

informed in case of a disaster or an attack. It should also include the conduct of drills to familiarise employees, with measures during an attack or disaster.

Acceptable use

It should state the purpose of the network, personal facilities employees can avail of, the type of information that can be sent via mail, messages that should be encrypted and the like.

Software security

It should state the persons authorised to purchase software, and describe the software to be used by the company on networks and the like. It should also indicate security measures to be taken while downloading free software.

Answer: [b] HR policy

Module: 2

Reference: M2006

Question: A firewall ruleset should not block

- [a] Inbound traffic without Internet Control Message Protocol.
- [b] Inbound traffic from a non-authenticated source.
- [c] Inbound traffic without the source address of the local host.
- [d] Inbound traffic from an authenticated source having Simple Network Management Protocol (SNMP).

Module 2- Firewall Policy I

A firewall policy states how a firewall will protect the network from users and other networks. It should specify the services that are permitted through the firewall. The policy should be approved and signed by the management.

Steps involved in creating a firewall policy

- Identify network applications
- Identify threats and vulnerabilities
- Develop a strategy to counter threats
- Create an application traffic matrix
- Create a firewall ruleset based on the application traffic matrix.

A list of applications that require security must be drawn up by performing a risk analysis. The risk analysis should take into consideration risks and vulnerabilities to which the applications may be exposed.

For implementation of security controls a firewall ruleset is prepared to determine the actual functionality of a firewall. A ruleset should contain the following-

- Source address of the packet (eg. IP address such as 142.613.4.2) This is the layer 3 address of the computer system from which the network packet originated.
- Destination address of the packet (eg. 165.457.4.1) This is the layer 3 address of the computer system that the network packet is trying to reach.
- Type of traffic The network protocol being used to communicate between the source and destination systems eg. Ethernet at layer 2 or IP at layer 3

- Characteristics of layer 4 communication sessions (eg. TCP 45 for destination port belonging to a web server, TCP 452 for the source port of a computer accessing the server). The protocol (such as TCP) and the source and destination ports of the session.
- Information regarding the interface of the router from which the packet originated, and the interface of the destination router of the packet.
- An action (like Deny or Permit the packet, or Drop the packet), which does not return a response to the packet's sender.

A firewall ruleset should be simple and specific to the network traffic it controls.

The default policy for firewalls should block all packets and connections that are not specifically permitted. The firewall ruleset should always block the following types of traffic-

- Inbound traffic from a non-authenticated source system with a destination address of the firewall system itself, such a packet will normally attack the firewall.
- Inbound traffic with a source address indicating that the packet originated on a network behind the firewall, such a packet indicates a spoofing attempt.
- Inbound traffic containing the Internet Control Message Protocol traffic coming from the Internet or an unauthorised network.
- Inbound traffic from a non-authenticated source system containing SNMP (Simple Network Management Protocol) traffic.
- Inbound traffic containing IP source Routing information. Sometimes a network packet can be constructed using source routing and can bypass a firewall.
- Inbound or outbound network traffic containing a source or destination address of 0.0.0.0. This traffic can sometimes be read as address of a local host or broadcast and can be used for attacking the firewall.
- Inbound or outbound traffic containing the source or destination address of a local host.
- Inbound or outbound traffic containing directed broadcast addresses. Sometimes this is used to send messages with a spoofed address.

After the creation of a ruleset, the policy should be tested, implemented, maintained etc. These aspects are covered in a different article.

Answer: [d] Inbound traffic from an authenticated source having Simple Network Management Protocol (SNMP).

Explanation: Inbound traffic from non-authenticated source containing Simple Network Management Protocol should be blocked as these packets indicate that an intruder might be probing the network.

Module: 2

Reference: M2007

Question: A detailed policy on firewalls should not

- [a] Include log reports
- [b] Include guidelines for assessment of logs
- [c] Ensure that it is physically secured
- [d] Ensure that it is logically secured

Module 2- Firewall Policy II

The first step in formulating a firewall policy is to develop a ruleset. Then guidelines should be outlined with regard to implementation, maintenance, periodic reviews, and action to be taken in case of breach or failure. The following points should be kept in mind while formulating the policy.

1. Verification of implementation: There are two ways of verifying implementation:

- (a) By obtaining a hard copy of the firewall configuration and comparing it with the policy
- (b) By performing tasks that a firewall should prohibit.

The policy should include

- (i) Persons responsible for implementation and verification, preferably independent parties
- (ii) Periodicity of verification
- (iii) Reports to be generated
- (iv) Action to be taken

2. Back up: The policy must define the back up process, its frequency, the personnel who can have access to the archives and the like. The policy should provide for another firewall configured on the same lines as the existing one, which can be used in the case of failure.

3. Integrity assurance: The policy should also provide a procedure to prevent unauthorised modifications to the configuration, by employing integrity assurance processes, such as checksums, cyclic redundancy checks or cryptographic hashes. The person authorised to do so, should also be mentioned.

4. Documentation: The policy should state that all configuration and operational procedures of the firewall should be documented. In case the authorised person leaves the organisation, or is not available, business functions can continue.

5. Physical security: The firewall should be physically secure. The policy should specify that the firewall should be located in a separate room, which is equipped with air conditioning, fire extinguisher and smoke alarms. It should also indicate the persons authorised for the task.

6. Log book: The firewall must be configured to generate logs of all activities on a daily, weekly or monthly basis. The policy should specify persons, who can access the logs, types of reports required, analysis and the like.

7. Restoration: The procedure for restoring the firewall when a break-in occurs, and the response team to be contacted should be mentioned. It should be specified that Internet services should be disabled, a second firewall should be made operational, and systems should be disconnected from the Internet.

8. Upgradation: Firewall software and hardware components need to be upgraded for optimum performance. The policy should state that the person, who is responsible, must know about hardware and software bugs, and firewall upgrades provided by the vendor. The policy should also state that all vendor recommendations should be adhered to.

9. Review: Last but not the least, the policy must be reviewed and upgraded to ensure accuracy and timeliness. When there is a change in network requirements, the policy should be reviewed. The configuration control board should evaluate a new service, before authorised persons are notified to implement the change. Similarly, when an application is phased out or upgraded, the firewall ruleset should be changed. Firewall installations and other systems must be audited on a regular basis.

Answer: [d] Ensure that it is logically secured

Question: Insecure information, which could threaten the existence of an organisation is classified under:

- [a] Low sensitivity
- [b] Average sensitivity
- [c] Medium sensitivity
- [d] High sensitivity

Module 2- Information Security Policy

Information is a key resource in an organisation, and helps the management in planning and decision-making. In consequence, it is essential to formulate and maintain an information policy. The policy must include general guidelines for information classification, labelling and handling, access, copy, transmission, retention and destruction of information.

Classification

In an organisation, information has to be classified based on the level of sensitivity and criticality. Sharing/restriction of information should be on 'need' basis. Guidelines should also be flexible enough to accommodate changes, over a period . The owner of the information should be responsible for its classification and review. Based on its sensitivity, information can be classified as

Classification	Sensitivity
High	If not protected, could threaten the existence of the organisation
Medium	If not protected, could harm the interests of the organisation
Low	All other information

The label should figure in the header and footer of all documents. The classification of information should be displayed on paper documents, electronic documents and sub-displays of such documents. The policy should define the procedure for labelling and handling information. These procedures should be communicated to concerned employees.

Access

The management must provide access to information, depending on the relevance and value-addition it provides. In some cases, the information may be of low value, but when coupled with other information it may assume significance .The policy should include controls over:

- The creator of data or information
- The management of the process.
- The location where information is created
- Sensitive and critical information

Personal computers and computer terminals should not be left unattended, and should be protected by passwords or other controls when not in use; sensitive information when printed should be cleared from printers immediately.

Copy

The policy should clearly mark the confidential status of information including e-mails and computer files. Access to these files requires permission of the sender/ recipient of a message or the owner of the account, in which the material resides. The policy should reserve the right to lock or copy the information to prevent destruction or loss.

Transmission

Information during transmission is vulnerable to unauthorised access, misuse or corruption. The policy should provide guidelines to control the flow of information. The agreement may include management responsibilities for controlling and notifying transmission, dispatch and receipt, procedure for notifying sender, responsibilities and liabilities in the event of lost data, information ownership, data protection, technical standards for recording and reading information and the like.

- The policy should lay down the procedure for information that can be publicly available. It should comply with laws, rules and regulations of the jurisdiction in which the organisation is located, or where it trades. It should also ensure that information requiring high level of integrity has checks in place like digital signature.

Retention

The policy should also provide guidelines for retention of information. The retention schedule should include details of records, and the time duration (minimum and maximum) for which they are to be retained. The policy should also provide for the exception to the maximum retention period rule in the case of records pertaining to litigation, criminal or civil investigation, audit and the like.

Destruction

The policy should provide clear guidelines for the disposal of information. This can be done either in-house or outsourced. When it is outsourced, the agreement should lay down the procedure for handling the material, the destruction process, the confirmatory evidence, and the authorised person to be present during destruction.

Answer: [d] High sensitivity

Module:2

Reference:M2009

Question: Corporate guidelines to download anti-virus software from the official site help to

- [a] Detect virus
- [b] Prevent virus
- [c] Correct virus
- [d] Contain virus

Module 2- Anti Virus Policy

Computer viruses are programs that replicate, attach themselves to other programs and perform unsolicited and sometimes malicious actions. Any computer whether at work, at a service provider or at home is susceptible to virus infection. The management must frame an anti-virus policy taking into consideration the factors given below, since even the best anti-virus software can be rendered ineffective.

1. Virus education: A good anti-virus policy depends on the knowledge and cooperation of users. The management should educate users, and make employees aware of dangers that virus present, and the person to contact in case of a virus attack.

2. Preparation: The policy should provide steps to be followed by the management to prevent virus attacks, such as :

- a. Preparation of regular and sound backups of data in case of data loss, corruption or damage. The frequency of backups depend on how often data is changed. A sound backup ensures data integrity.
- b. Creation of a write-protected system disk containing all system files. This disk should be used for booting, when the operating system has a virus.
- c. An alternative plan of action with a mention of person/s to be contacted.

3. Prevention: Steps can be taken to minimise the risk of virus infection, if the policy provides guidelines:

- a. To make available current and fully updated version of corporate anti-virus software onsite.
- b. To download and run the current version of corporate anti-virus software from corporate site only and not from other sites
- c. To prevent automatic opening of email attachments.
- d. To apply software security to client and server applications.
- e. To always scan floppy disks, CDs and any other removable applications, before using them on their computers
- f. To scan all files as opposed to programs or selected file only
- g. To prevent sharing diskettes for installing software or worse still, copies of software
- h. To prohibit download of software from non-trusted sources
- i. To configure all computers to boot from drive C first, then drive A.
- j. To prohibit installing any unapproved software on computers
- k. To delete spam, chain and other junk email without forwarding it
- l. To ensure that the machine is clean when lab tests conflict with anti-virus software. Run the anti-virus utility, disable the software and then run the lab test. After the lab test is done, enable the anti-virus software. When the anti-virus software is disabled, other applications that could transfer a virus should not be allowed to run.

4. Detection: The policy should seek to educate users to apprehend a virus attack. Some of the symptoms of virus infected computers are

- a. Programs take longer to load
- b. The size of the program changes
- c. The disk runs out of free space even when it seems to have plenty
- d. Bit errors occur frequently while running windows
- e. The disk drive is active when it should not be
- f. File names change
- g. New files appear
- h. The screen board becomes distorted
- i. Text on screen behaves in an unusual manner

- j. The keyboard makes a clicking noise.
- k. Personal observation is an important part of detection.

5. **Recovery:** An amateur should not attempt the restoration process. The policy should provide clear procedures for restoration. Check systems for infection, identify systems that have been infected, track the source of infection, isolate systems that have been infected, and check back ups to make sure that they are clean.

Answer: [b] Prevent Virus

Module:2

Reference:M2010

Question: A good email policy should state that:

- [a] All mails sent and received should be monitored
- [b] All messages should be encrypted
- [c] Emails should be used only for official purpose
- [d] All personal mail should be labelled

Module 2- Email Policy I

The email policy of an organisation should clearly state the dos and don'ts. While formulating a policy, the issue of privacy (of the employees) should be given due consideration. Representatives of employees, technical experts, lawyers and the management should be involved in the process. The involvement of employees will help in framing a policy that will be easily accepted.

Factors to be considered

- Purpose for which email may be used: The policy should make clear whether the facility can be used for professional and personal purposes. If so to what extent can it be used for personal purpose?
- Encryption and Labeling:
 1. The policy should state the type of information to be encrypted before being sent, the level of protection required, the encryption software to be used, and the authorised person for encryption keys.
 2. The policy should also include labelling of personal email.
 3. The policy must clearly lay down the requirements and limitations of employee's authority to use signature files or message text. (Refer our article on digital signature)
- Systematic Monitoring: The policy on systematic monitoring should include:
 1. Extent of monitoring of professional mail
 2. Amount of personal mail that can be received and sent
 3. Knowledge dissemination to all employees on monitoring
 4. Procedures of monitoring
 5. Persons responsible for periodic monitoring and report
 6. Actions ensuing the violation of email policy
- Access and Disclosure without consent in specific cases: The policy should state:
 1. Whether employee emails or files can be accessed without their explicit consent, if so under what circumstances?
 2. The persons authorised to access such information and make disclosures.
The access and disclosure policy of the company must be made known to employees.
- Substantive rules: The policy should clearly state that emails should not be used, if it infringes the copyright or other intellectual property rights, to distribute defamatory, to send fraudulent

messages, and no software should be downloaded without checking for virus. The policy should prohibit snooping, and state that disciplinary action following the violation of rules could even mean termination of service.

The email policy framed should be consistent with other company policies.

Answer: [d] Should include a procedure for labelling personal email.

Module:2

Reference No :M2011

Question: To enforce the email policy, the management in order need not:

- [a] Educate employees
- [b] Educate third parties
- [c] Take prompt action in case of misuse or complaints
- [d] Prohibit subscription to e-newspapers and e-groups

Module 2- Email Policy II

Email is an easy and cheap mode of communication. Now, almost every company uses email for its business, as it is flexible, automatic and fast. But, some of the threats to the company posed by emails are:

1. Legal liability: The company is responsible and liable for outgoing mail sent by its employees. Thus an email meant to a joke, if found offensive by the receiver, may result in a lawsuit.
2. Confidentiality: Accidental or intentional breach of confidentiality may cost the company dearly. Especially when addressed to the wrong person or intentionally sent to competitors.
3. Damage to reputation: Poor language may damage the reputation of the company.
4. Loss of productivity: Without a proper email policy, employees may spend most of their time reading and replying to personal mail.
5. Network congestion and downtime: Spam and personal mail will use bandwidth and cause network congestion.

In order to protect itself, the company must create an email policy. Creation of an email policy will not suffice; the company should ensure implementation also.

An email policy may include the following:

- Email risks: Users should be made aware of risks by listing them.
 - Best practices: To uphold the reputation of the company and to deliver quality customer service include email etiquette and writing rules.
 - Prohibited content: It should not be used for sending offensive or disruptive messages with comments about race, gender, age, sexual orientation, pornography, religious or political beliefs, national origin, to discuss competitors, potential acquisitions or mergers. Stringent action that will be taken against employees who indulge in such activities should be specified.
 - Wastage of resources: It should be made clear that the company's resources should not be used for other activities. Permission must be obtained from authorised persons, before subscribing to e-newsletters or e-news groups.
- Document retention policy: If the company is required by law or if it requires to archive email messages, it should state where e-mails should be saved and stored, how long they should be retained and the like.

- Email disclaimer: It should state where the disclaimer text would be appended, and employees should be aware of it.
The company should make the email policy available to its employees. A short statement may be included in the employment contract to make sure that the employees are aware that such a policy exists. Whenever the policy is updated, it should be circulated to them and their signature obtained. The formulation of the policy does not lead to its implementation. Providing training to users, taking prompt action in case of complaints and misuse, and monitoring email help in enforcing the policy.

Answer: [b] Educate third parties

Module: 2

Reference No: M2012

Question: Information that must be provided in the register is part of the _____ guideline of the server security policy

- [a] Ownership and responsibility
- [b] Monitoring
- [c] General configuration
- [d] Compliance

Module 2- Server Security Policy

Information is a major asset of a company. The information we enter, store and transmit via our computers is critical not merely for ensuring efficiency and profits, but also for the very existence of the company. In consequence, information must be accessible yet protected.

Policies have to be in place to ensure that appropriate security procedures are designed and installed. A server security policy must be framed to minimise unauthorised access to information and equipment on the internal network. It must include guidelines on the following:

- Ownership and responsibility: This issue has to be considered from two angles - with regard to internal servers deployed for the use of specific groups; and the main server used by many groups. Internal servers must be under the control of an authorised person in the group. They must have approved security configuration guides on "need basis". The policy should provide:
 1. The procedure for monitoring configuration compliance
 2. The procedure for implementation
 3. Follow up of exceptional reports
 4. Periodical updates and communication of the same.
- The corporate enterprise management system should register all servers used by individual groups, as well as, the main server. The following information must be provided in the register:
 - o Server contact and location, and a backup contact
 - o Hardware and Operating System/ Version
 - o Main functions and applications, if applicable
 - o The enterprise management system should be updated on a regular basis.
- General guidelines:
 1. There should not be any conflict between the server security policy and other policies viz. physical security, software security, logging rules, configuration of operating systems etc.
 2. Services and applications must be disabled when not in use.
 3. The access control table must be provided for access to services, and all activities must be logged.

4. Security patches must be installed on the system, unless its immediate application interferes with business requirements.
 5. The root directory should not be used if a non-privileged account will serve the purpose.
 6. Servers should be specifically prohibited from operating in uncontrolled cubicle areas.
- **Monitoring:** Activities on critical or sensitive systems must be logged, and audit trails should be saved. The policy should also state the duration for which security related logs and daily incremental tape backups should be kept online. The policy should also mention the person to be contacted in case of security breaches. It should also mention clearly the person who would review logs, and the person who would prescribe corrective actions.
 - **Compliance -** The policy should ensure that audits are conducted on a periodic basis. Details regarding the authorised person to conduct an audit, and the person to whom the findings must be reported, the follow up of the recommendations etc should also be clearly mentioned. The conduct of the audit should not cause operational failures or disruptions.
 - **Enforcement:** Employees must be educated and trained to follow the policy. They should be informed that disciplinary action would follow, if the policy is violated.

Answer: [a] Ownership and responsibility

Module: 2

Reference No: M2013

Question: Shareware software acquired by a company can be used

- [a] Only by the company
- [b] By its employees for their personal purpose also
- [c] By all third parties associated with the company
- [d] By Everyone with whom the company chooses to share it

Module 2- Software Policy

Software runs specific programs or operates related devices. The company cannot make a copy of this software except for backup or archiving purpose, unless it is authorised to do so by the developer.

Every company should have a software policy. The purpose of having such a policy is to prevent infringement, and protect the integrity of its computer environment from viruses. The policy should ensure that the all employees and others working on behalf of the company should adhere to the terms of software licenses to which it is a party. The software or related documentation should not be duplicated, unless the company is authorised to do so, under the agreement with the licensor, and only after obtaining written permission from the concerned authority. The software should be used only on machines and LANs for which the license has been obtained. It should not be authorised to third parties including clients, contractors, customers and others.

The software policy may include guidelines on the following:

User education: All employees must be educated on software agreements and licenses. They should be made to sign the anti-piracy statement.

Budgeting for software: When a proposal is made for acquisition of the software all costs related to its acquisition, hardware requirements and training should be taken into consideration.

Approval for purchase of software: The approval of the concerned department head and the Information Technology team must be obtained for the purchase of software. The procedure must be in line with that followed for the purchase of other assets.

Acquisition of software: Only authorised persons should acquire software for the company. It must have a complete record of software that has been purchased on its behalf and must register, support and upgrade them.

Registration of software: The software when delivered must be handed to the authorised person to complete the registration and inventory requirements. The software should be registered in the name of the company. The authorised person must maintain a register and a library of licenses. The register should contain

1. Title and publisher of the software
2. Date and source of software acquisition
3. Location of each installation, as well as, the serial number of the hardware on which each copy of the software is installed
4. Name of the authorised user
5. Location of backup copies
6. Software product's serial number.

Installation of software: The software should be installed either by an authorised person, or by the user of the software. Manuals, tutorials other user material, and a copy of the license agreement should be provided to the user. After installation, the original software should be kept in a safe storage area.

Home computers: The software owned by the company should not be loaded on a computer owned by the employee, without the permission of the authorised person, unless the license agreement provides for it. Similarly the software acquired by the employee should not be loaded onto that owned by the company. This is to ensure that the computers are loaded with only legal software, and are virus free.

Shareware: Shareware software is copyrighted software that is distributed freely through bulletin boards and online services. Registration of shareware software should be on the same basis as other commercial software, and the company should pay the authors to use their products.

Periodic audits: The authorised person should conduct regular audits, as well as, surprise checks. The audit may be conducted using an audit software product or through manual inspection. This ensures that only licensed software is used, and computers are free of virus.

Penalties and reprimands: The policy should state that any employee who makes, acquires or uses unauthorised software will be prosecuted, and his employment may even be terminated.

Answer: [a] Only by the company

Question: One of the following statements is true in relation to network policy change

- [a] It should be changed only by the management
- [b] It should have flexibility for change by authorised people
- [c] It should implement changes to prevent violation.
- [d] It gives a blanket permit to incorporate changes without specifying a limit.

Module 2 -Network Policy 2

After creating a security matrix table, the management should ensure that the policy is implemented. The security team along with representatives from all user departments will be in charge of policy implementation. This team will also be responsible for policy development, changes of policy and response to violations.

Policy development involves framing and reviewing the policy. The policy should specify the configuration of network assets in plain language. For example, instead of stating "No outside FTP connections will be permitted through the firewall" it should be worded as " Outside connections should not be allowed to retrieve files from inside the network". The policy should be reviewed periodically so that it does not become obsolete and corresponds to the changes in the organisation. Any changes in the policy should be based on a risk analysis. The security team should review changes to the following-

- Firewall configuration
- Access control list
- Simple Network Management Protocol
- Updates to the software

Changes to the policy should not be allowed unless the security team approves them. The policy should also specify the procedure for notification of security violations and should monitor low risk areas weekly, medium risk areas daily and high risk areas hourly or as frequently as required.

The policy should define the procedure to be followed in the case of a security violation. It should specify the names of people to be informed, the levels of responsibility and to what extent and areas they are authorised to change policy. However any serious change should be taken up by the management. The change can include guidelines on the following:

Implementing changes to prevent further violation

- Isolating the violated system
- Contacting the carrier or ISP in an attempt to trace the source of the attack
- Using recording devices to gather evidence
- Disconnecting violated systems or sources
- Contacting the police, or other government agencies
- Shutting down violated systems
- Restoring systems according to a priority list
- Notifying internal managerial and legal personnel.

The security policy should also specify the procedure for back up and the process of obtaining approval from the concerned persons for utilisation of the back up for restoration purpose.

Finally the policy should be reviewed at periodical intervals. It should change with changes in the organisational environment. Regular reviewing helps in filling the gaps existing in the policy.

Answer: [b] It should have flexibility for change by authorised people

Module: 2 Reference No: M2016

Question: While evaluating the IT control environment for obtaining an understanding of the management's control over IT activities, the auditor should consider

- [a] The functions of the IT steering committee
- [b] The Security policy
- [c] The IT strategy of the management
- [d] The user's perception of IT

Module 2- Evaluation of IT environment

The control environment in an organisation is made up of

- The system of internal controls
- The managements' responsibilities regarding controls
- Key elements of the system of internal controls as related to a computerised system
- The different types of controls related to Information System
- The general control environment of IT

It is important for an IT auditor to formulate a strategy before beginning the audit. Each client/ customer/ company he audits will have a different environment, platform, policies and procedures. It is important to keep a complete documentation of the control environment of each client. This will help the auditor formulate his audit strategy not only for the first time but also for subsequent years. From this, he can easily track the changes that have taken place in the subsequent years of the audit. The study will also give the auditor an in-depth view of the clients' facilities, commitment etc. The study should cover the following areas:

1. Understand how the IT function is organised: The auditor should obtain an understanding of

- The structure of IT
- Roles and responsibilities of each individual in the IT department
- Significant changes that have happened during the year by way of recruitment, resignation, retirement etc.
- A representative from the top management who is responsible for IT.
- The IT steering committee, its functions and priorities
- Key audit contacts within the IT function
- Other significant IT activities outside the IT function

2. Understand the management's control over IT activities: The auditor should consider

- How the management measures the performance of the IT staff?
- What is the Systems Development methodology?
- How is routine system maintenance managed?
- What are the security policies they have to be prepared and communicated?
- Do they have business continuity and a disaster recovery plan in place?
- Do they have computer controls to limit access to information

3. Understand IT support for a business: He should obtain this understanding by considering
 - The management's view of IT roles in meeting business objectives
 - The IT strategy of the management -the roles and to what extent IT will help in fulfilling business objectives
 - Key business activities identified by the management as having IT components. For instance, do they use IT excessively in Finance, Marketing, Customer Care etc.
 - Users' perception of IT
 - The IT needs of the senior management. Are their needs being met by the current systems - what type of information is required to make a decision
 - Technologies being used by the IT department
4. Understand the characteristics of systems and environments: The auditor should obtain an understanding of
 - Systems that the client considers important for use
 - Development of the system- in-house or packaged
 - If the system is being developed in house, do they have the expertise to develop it
 - The extent of customisation of the packages and their success
 - Main computer processing locations
 - Main hardware environments
 - The network
 - Key external network connections
5. A Document containing significant changes to systems and environments:
 - New systems that have been implemented
 - Outcome of the implementation
 - Significant changes in the routine maintenance of existing systems (both hardware and software)
 - Migrations to new environments
 - Significant upgrades to system software
 - Significant changes in the network
 - Major IT initiatives planned - long term and short term
6. Understand problems in the client's systems:
 - Significant problems or faults in the exiting systems
 - Significant operational failures or data corruption probl

Answer: [b] Security policy

Module:2 Reference No:M2083

Question: Chief Information Officer is responsible for which of the following function in Information Management?

- [a] Managing the information resources in line with the strategic plan
- [b] Library and record management
- [c] Establishing the activity responsibilities
- [d] All the above

Module 2 – Information Management

Meaning

Knowledge pertaining to events, processes, facts and things, ideas and opinions is described as information. Information can take various forms like graphics, text or numerical figures. But effective dissemination is possible through information management. This refers to the process of managing the activities in the information life cycle like collection, storage, access, usage and disposal of information.

Organisational responsibilities

A clear understanding of Information management and its practice in the organisation is essential.

1. **Chief Information Officer** plays an important role in this. Managing the information resources in line with the strategic plan is the main responsibility of CIO. Policies, development of standards, design of activities and performance evaluation are the main functions of CIO.
2. **Senior managers** are accountable for library services, record management and data administration.
3. **Chief Executive Officer** establishes the activity responsibilities and monitors the performance.

Information management requirements

The information requirements helps to identify the gap between the information required and that, which is actually available if they are recognised as an element of information inventory. Information audit evaluates the effectiveness of organisational information performance. This requires a through understanding of information life cycle.

Information lifecycle

The information lifecycle consists of collection, storage, access, usage and disposal stages. All these stages are equally important in managing the information. Considerations like information levels, responsible persons, sensitivity and quality are also addressed in the lifecycle. It has to be managed properly by considering the cost element.

- **Collection:** Information can be collected through different sources. Records, databases, publications and the like. Necessary changes must be incorporated in the information over a period of time.
- **Storage:** The collected information must be classified, appraised, coded and listed so as to facilitate the business processes. Electronic information must be designed according to the storage medium and non-electronic information must also be stored properly.
- **Access:** It involves identifying, recovering and delivering information to user. Communication networks or physical electronic media can be used to transmit the electronic information.
- **Use:** Information must be readily available for its usage in several purposes. Electronic medium adds value to the information.
- **Disposal:** Unwanted information must be suitably disposed of by taking in to account the storage medium, user demand, value and business requirements.

Information Management Framework

Features

Effective information management is based on the effective management of its features like definition, ownership, sensitivity, accessibility and quality.

1. **Definition:** It deals with identifying, classifying and explaining the information held by the organisation. Inventory and classification measures provide guidelines to recognise the information inventory required by the present and potential users thereby classify it according to the needs.
2. **Ownership:** Specific persons must be made responsible for the ownership of information. They are answerable for any loss or damage.
3. **Sensitivity:** It deals with privacy and confidentiality of sensitive information. Placing access controls, identifying the intended use of information protects the privacy and confidentiality.
4. **Accessibility:** Information indexing helps to supply appropriate information to the users. Further rights and responsibilities must be defined before allowing access to the external users.
5. **Quality:** Information quality is measured in terms of its accuracy, completeness and consistency aspects. Quality assurance measures and security controls ensures integrity of information.

Answer: [a] Managing the information resources in line with the strategic plan

Module:3 Reference No:M3100

Question: The primary objective of a data classification scheme is to

- [a] To meet the business requirements
- [b] To increase the integrity value of the data
- [c] To assign different security levels
- [d] To ensure optimal utilisation of resources

Module 3- Control objectives for planning block

Building the information architecture framework

Introduction

Once the long term and the short-term plans are formulated, the next logical step is to frame an information architecture model. This information architecture should define appropriate systems that are required to generate accurate information.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
An optimal information system organisation	To ensure effectiveness, efficiency, confidentiality and integrity of the information that is fed into, processed, generated by the information system	1. Data dictionary 2. Data repositories 3. An information architecture which represents the needs of the organisation 4. Data syntax rules 5. Information architecture standards.	• Data • Application technology

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **The information architecture framework:** The information that is generated by the system should be the basis for the decision support system of the management. Accordingly, an optimal information structure has to be built to serve the needs of the organisation. This information model should provide a process or methodology for regular collection and communication of data that is generated and required by the organisation. It should have a timeframe to ensure that people carry out their responsibilities in an effective manner. The information architecture should be consistent with the long-range IT plans. It should be regularly updated and changed as per the changing environment of the business.
- **Data dictionary and syntax rules:** All information architecture models should consist of a data dictionary, which incorporates the organisation's data structure. It must also be ensured that the data dictionary is regularly updated for any changes in the business environment. The data dictionary should also define the data syntax rules.
- **Classification of data:** The information model framework should consist of a data classification scheme for the corporate data. Data is classified to assign different security levels to each category. This also facilitates in managing the access rights that are to be given to each category of users.
- **Assignment of security levels:** The information model adopted by the organisation should constitute a mechanism for definition, assignment and maintenance of security levels for each category of data. A minimum set of security measures should be adopted for each security level defined. The assignment of different security levels to different categories of users should be based on some pre-established criteria. Such a criteria and the security levels defined should regularly be evaluated and modified if the need arises.

II. Operational Controls

Not applicable for this activity.

Answer: [c] To assign different security levels

Module:3 Reference No:M3106

Question: Which of the following is not the preventive system internal control?

- [a] Automatic logoff
- [b] Account balances
- [c] Auto encryption
- [d] File deletion

Module 3 - Preventive Controls - Printing operations

Businesses have to take reasonable care while printing important documents for use by others. For example, some companies print payment cheques to pay the suppliers. Such a task, which is a part of payment management, requires a very high level security. The risk of counterfeit cheques looms large, in event of

which the management will have to bear heavy expenses in the form of bank fees. A new technology, Laser Cheque printing has been introduced to counter this problem to a great extent. The main functions of Laser cheque printing software packages are cheque printing and payment management operations. It ensures proper control over fraud and hence reduces operating costs.

The organisation should also realise that any change in the technology would certainly warrant a change in the existent internal controls of the organisation. It is necessary to understand the types of internal controls for evaluating their effectiveness before implementing them. The cost effectiveness of the controls need to be appraised in relation to the benefits (like reduction in operating expenditure) accrued from the controls.

Internal controls are segregated into preventive and detective controls. **Preventive controls** are those, which prevent the occurrence of any error or irregularity. On the other hand **detective controls** aim to identify the error after its occurrence. Both the controls can be again divided into system controls and manual controls. Preventive controls are being discussed in the present article, while detective controls and the audit of printing operations will be discussed in the second part of the article.

I. Preventive Controls: -

A. Preventive system controls: The following are the preventive system controls

- 1. Auto encryption:* When cheques have to be printed, the system first receives input from accounting data authorising the payment. This file is then formatted to cheque image file, and encrypted. In addition, the digital signatures data and bank account details of receiver (if any) are also encrypted. Logs for system activity, cheque prints and the like are kept.
- 2. Automatic deletion of a file:* After cheque printing, the data file should be automatically deleted by the system.
- 3. Automatic logoff:* If the system is used for a specific time limit, it must be controlled by automatic log-off.
- 4. Login controls:* Laser printing system should provide adequate login controls. Users must be allowed to login through a set of procedures, different from general procedures. Some systems may have separate passwords for different processing operations to ensure security.
- 5. Pause with warning:* The system should warn the user in case of any interruption caused to the process to avoid reprinting that give scope for frauds.
- 6. Positive pay system:* Under a positive pay approach, bank verifies each cheque with the details sent by the customer through MICR. It rejects and informs the customer of those that do not match. Banks may provide this service free of cost or charge a fee.
- 7. File deletion:* Cheque image files must be deleted after processing. If they are retained for the purpose of reprinting, it must be ensured that they are deleted after particular time limit.
- 8. Reprint authorisation:* Only an authorised supervisor with a different user ID must perform the cheque reprinting operations.
- 9. Printer related security features:* Background images on the cheque can be done using security features like void pantographs or wicker. Void pantographs are small dots, which cannot be captured while scanning or copying. Wicker features are lines with different lengths printed at different angles that are not compatible

with scanner or copier protocol. An attempt to scan or copy these lines leaves a garbled image.

10. Two dimensional barcodes and data glyphs: Data glyphs and two-dimensional barcodes are printed on the cheque by a laser printer. A small picture of the complete cheque is contained in these features. It makes fraudulent printing difficult.

B. Preventive manual controls: The following are the preventive manual controls

1.Account balances: The cash balances to be maintained in the checking account must match the predetermined levels arrived through cash budgets. It avoids fraudulent overdrawing of funds.

2. Isolated PC: Cheque printing systems must be separated from other software to avoid interruption in the cheque printing operation. It also reduces the possibility of fraudulent cheque printing.

3. Control on cheques after printing: The printed cheques and the print log should not be made available to the accounts payable staff.

4. Supply control: Cheque supplies such as MICR toner, stock of blank cheques must be controlled properly. It can be ensured by physical isolation.

Answer: **[b] Account balances**

Module:3 Reference No:M3107

Question: **Which of the following is an effective control over paper stock?**

- [a] Activity logs
- [b] Printer related security features
- [c] Paper count
- [d] Number log

Module 3 – Detective controls – Printing operations

Businesses have to take reasonable care while printing the important documents for use by others, which otherwise may result in heavy expenses. Laser Cheque printing has been introduced to detect malpractices to a great extent. The main functions of Laser cheque printing software packages are cheque printing and payment management operations. It also ensures proper control over fraud and hence reduces operating costs.

Preventive system and manual controls are covered in another article. This article dwells on the detective controls and the audit aspects of printing operations.

II. Detective controls:

Detective controls, created by the system are referred to as detective system controls. Those requiring human intervention are referred to as defective manual controls.

A. Detective System controls: The following are the detective system controls

1. Logs: System logs, cheque printing system logs and image files must be compared with the independent records to find out the fraudulent runs made if any. Operations staff must maintain the print logs, which shows the details of cheque runs. It helps in reconciling the bank balances and also enables internal auditors

to review the process.

2. Limiting messages: Limited encashment through cheques and validity of date could be incorporated.

3. Manual and duplicate signatures: Manual signatures serve as a good control to detect and avoid forgeries. Whenever manual signatures are used, the system should be programmed in such a way that digital signatures are deactivated automatically.

4. Control over paper stock: Using coloured paper for cheques is an effective control feature to differentiate cheques printed by different departments. However, because of existence of colour copiers forgeries may not be easily detectable. But pastel-coloured papers ensure some level of security. In addition, different colours may be used for background and foreground printing.

5. Printer related security features: Non-repetitive printing, secure font printing and warning band controls are some of the detective controls.

7. Signature plates: Signature plates serve as effective control to identify forged cheques. Proper measures should be taken to protect digital signature plates. It should be encrypted and kept in removable disks when printing is not being done.

9. Ultraviolet imaging of cheque snippets: Banks generally use these cheque snippets to record the information on paid cheques. Cheque makers can also use snippets to stop the encashment of modified cheques.

10. Special ink security features: The special inks that were used in preparing cheques traditionally served as a control to differentiate between the original and duplicate. But with the advent of laser printers this became difficult. However, if two printers were operated in series using special inks, in such a way that the printing is completed only when it is processed through both printers, it would be more secure.

12. Paper related security features: Certain paper related security is available to identify tampering of cheques. They use certain chemicals and toner adhesion coating. In some cases the security feature detects when the cheques are scanned or photo copied.

B. Detective Manual controls: The following are the detective manual controls.

1. Account reconciliation: Lack of accurate reconciliation schedule, delay in reconciling the balances and inefficient staff are some of the reasons for frauds. A good pay system should ensure a precise reconciliation.

2. MICR testing: Appropriate machinery must be selected to process the cheque through MICR.

3. Number log: Operations staff is required to maintain a number log showing the details of cheques printed on each day. It enables to identify the unauthorised printing if any, by comparing the previous day closing numbers and the next day opening numbers.

4. Paper count: Paper count control is an effective control over paper stock.

Audit of printing operations

1. **Preliminary evaluation:** Under preliminary evaluation, an auditor should check the back up, retention and purge policies that are framed in the committee meetings. Ensure that these policies are not

changed without prior approval. The committee should consider all the rules and regulations relating to banking contracts and clearing houses before framing the policies.

2. **Personal visit to the location:** Auditor must visit the processing locations. He should examine the documentation of each and every process. He should ensure that the processes are run according to the set procedures.
3. **Evaluation of controls:** Auditor should examine the controls established over processes to evaluate its effectiveness.
4. **Change management process:** Auditor should ensure that adequate controls exist over change process. All new features added to the system should interface accurately with the existing security features.
5. **Restrictions on vendors:** Whenever vendors support the system for its functioning and maintenance, they should not be allowed to access the sensitive information. Updation of software at a remote location may give rise to unauthorised changes.
6. **Audit report:** Audit report should not contain a detailed description of the internal control in place. As the audit report is accessible to many, one can easily beat the controls if they are discussed clearly.

Answer: [c] Paper count

Module: 2

Reference No: M2017

Question: Project management is considered a separate division on the basis of:

- [a] Interdependencies among departments
- [b] Sharing of resources
- [c] Size of the project
- [d] All the above

Module 2 – Project Management

Before we delve deep into the hows and whys of project management, let us first understand what a project is. There are few activities that are associated with a project, such as:

- They are a well-defined set of activities with a clear-cut beginning and an end.
- They have a desired outcome.
- They are undertaken frequently.
- They consume organisational resources.

On this basis, a project can be defined as, 'Any undertaking that has definite objectives, and uses specific resources to attain these objectives.'

Project Management

While managing a project, many factors come into play. Hence, project management is defined as planning, organising, staffing, directing, and controlling specific parts of an organisation for a relatively short period of time.

But, why should project management be considered as a separate function within an organisation? A few factors that are responsible for this decision are:

Interdependencies: There might be different departments that are involved with the same project. This provides a platform for linkage.

Sharing of Resources: Organisations may always find themselves with scarcity of resources, in terms of expertise, cost or the like. It is hence better to adopt unified project management practices to ensure that resources are optimally used.

Size of the project: If any department within an organisation is thinking of venturing into new areas, it should first assess the size of the venture. If it is large enough to involve more than one department, then it should be taken up as a separate project.

Who becomes the PM

No, it's not a soap opera on TV. Rather, the sub-title seeks to focus on attributes that a Project Manager (PM) should possess. Although, people with a lot of knowledge and experience put forth ideas, a project manager has to make the best use of people and resources to ensure that the ideas are translated into reality, and the project is completed on time. His main duty is to co-ordinate and integrate diverse activities that are carried out, across different departments. He should possess:

- Good communication skills to clearly convey his ideas to all members
- Effective interpersonal skills to motivate his team members
- A fair idea of the prevailing technologies s:

Answer: [d] All of the above.

Module: 2

Reference No: M2018

Question: The LAN policy describes the job of persons who work on the network. The duties of a network administrator are

- [a] Monitoring security violations
- [b] Password administration
- [c] Configuring and optimising storage systems
- [d] Monitoring network environmental conditions

Module 2 – LAN Policy Part 1

Every company should have a policy that defines LAN procedures related to usage, operation, maintenance etc. The policy helps users to know the purpose for which LAN is to be used, the activities that are supported by LAN, its operations, functions etc. The LAN policy is framed by the IT steering committee and approved by the management. The policy must be reviewed and updated annually so that it stays current. Any changes to the policy must have the consent of the IT steering committee and the management.

A LAN policy should address the following issues:

- LAN hardware
- Network applications and system software
- Data confidentiality, integrity and availability
- Network backup
- Use of network resources

- Software license agreements
- Hardware maintenance
- Problem logging/ reporting and monitoring
- Users responsibility
- Detection and prevention of computer viruses

This article is first in the four part series on LAN policy. In this article we deal with the set up of the organisation and job descriptions in a LAN policy.

1. Organisational setup: The policy should define the organisational set-up for the implementation of LAN. The policy should identify one person who will be responsible for the overall administration of the LAN. Each branch of the organisation that has a network should be under the control of an assistant network administrator.

2. Job description: The policy should describe the job of various persons who are connected to the network. The following are a few important job descriptions.

2.1. Network Administrator: Duties include

- Monitoring network efficiency (response time, utilisation of disk space etc.)
- Troubleshooting network problems
- Monitoring environment conditions
- Taking regular back-ups of the system, shared data files, and application programs on the file server
- Detecting and preventing computer viruses
- Ensuring that network security features in the Network Operating System are implemented
- Recommending hardware and software acquisitions
- Resolving technical problems by contacting the network maintenance persons
- Deleting and adding users
- Coordinating installation of new network hardware and software
- Maintaining an inventory of network hardware and software
- Reporting suspected security problems to the security officer
- Any other duty assigned by the management

The network administrator should not perform any duties that are in direct conflict with the principles of internal control.

2.2. Assistant Network Administrator: An Assistant Network Administrator does the job of a Network Administrator at the branch he is in charge of. Additional duties that he may perform are

- To ensure that back-ups of individual PCs are performed
- Contingency/ recovery operations of the branch are performed
- Reporting network problems to the network administrator

2.3. Network Security Officer: Duties of a network security officer include

- Monitoring security violations on the network
- Password administration
- Any other duties assigned by the management

The manager of every department/ section should ensure that employees comply with the policy. All support needs must be addresses to the network administrator and all security aspects to the security officer. The

policy should also state clearly if network resources can be used for personal purposes or not. If they can be used, it should specify the extent and the time for which the facilities can be used.

Answer: [d] Monitoring network environment conditions.

Explanation: Monitoring security violations and password administration are important duties of a network security officer. Configuring and optimising storage systems is the duty of the system administrator.

Module: 2

Reference No: M2019

Question: The LAN policy is framed by

- [a] The IT steering committee
- [b] The management
- [c] A business analyst
- [d] A project manager

Module 2 - LAN Policy Part 2

Every company should have a policy that defines LAN procedures related to usage, operation, maintenance etc. The LAN policy helps users to know the purpose for which LAN is to be used, the activities that are supported by LAN, its operations, functions etc. The LAN policy is framed by the IT steering committee and approved by the management. The policy must be reviewed and updated annually so that it stays current. Any changes to the policy must have the consent of the IT steering committee and the management.

This is second in a four part series on LAN policy. In this article we deal with Network security and software aspects of LAN policy.

1. Network Security: Network security can be in the form of Log in/ Password (initial access)

- Trustee (directory level access)
- Directory (directory level access)
- File attributes (file level access)

1.1. Log in/ Password: The log in / password is used for initial access to the network. The user name and password should be recognised by the server for a user to log in. The user can choose his password, which is encrypted by the system. If the user forgets the password the network administrator can assign a new one.

1.2. Trustee: Each directory and file has an owner. The owner grants a directory level access to users on a "need to know" basis. The access may be assigned to individuals as well as groups. The trustee to whom access is granted should ensure that the company's confidential information to which they have access to is not written to removable media and transported from the company's premises unless they have authorisation.

1.3. Directory: The owner may grant directory level access with the following rights to the user

- Supervisor (assigns the right for the directory)
- Access control (trustee assignments)
- Modify filenames and attributes
- Create new files or subdirectories

- Erase existing files or subdirectories
- Read files
- Write files
- The owner should grant these rights to users on a "need to know" or "need to have" basis.

1.4. File attributes: The owner can assign one of the following rights to trustees or users

- Shareable read only
- Shareable read write
- Non-shareable read only
- Non-shareable read write
- Hidden file
- Delete inhibit
- Rename inhibit
- The above rights protect accidental deletions or changes to the files.

2. **Network software:** The detailed policy regarding the following should be included:

- Software licensing violations
- Authorised software
- Personal use of company software
- Ownership of software
- Support of purchased software

2.1. Purchased software: The management should evaluate the financial stability of LAN software vendors. If required, alternative vendors should be located. The company should have an agreement with LAN software vendors to provide access to software source codes and documentation if the vendor is unable or unwilling to support the software at future date. (For a detailed discussion refer to our article on software policy)

2.2. Custom software: For custom software development a cost justification should be conducted before developing or contracting is done. The project must be approved by the IT steering committee. Custom software should follow the standards for development and testing that have been set.

a) Development: Before considering the development of a project, products that can be bought off the shelf must be checked out, as a substantial amount of time may go into developing a project. Documentation and testing standards must also be developed before a project is undertaken.

b) Maintenance: Maintenance of the program should be possible even if the original programmer is not around. Detailed manuals and documents for reference must be developed.

c) Testing: Programmers should test the developed product against written standards and test data. Users should perform acceptance testing and departmental heads must approve the installation.

Answer: [a] The IT steering committee

Module: 2

Reference No: M2020

Question: In the LAN environment, _____ officer is responsible for prevention and detection of virus

- [a] Web administrator
- [b] Security officer
- [c] Network administrator
- [d] A project manager

Module 2 – LAN Policy Part 3

Every company should have a policy that defines LAN procedures related to usage, operation, maintenance etc. The LAN policy helps users to know the purpose for which LAN is to be used, the activities that are supported by LAN, its operations, functions etc. The LAN policy is framed by the IT steering committee and approved by the management. The policy must be reviewed and updated annually so that it stays current. Any changes to the policy must have the consent of the IT steering committee and the management.

This is third in a four part series on LAN policy. In this article we deal with the security aspects in a LAN policy.

Security policy: The management frames a network security policy to have adequate controls over the network. The network administrator is in charge of implementing the policy and the access control table provided by the department supervisors. (Refer network policy) Department supervisors provide rights on the basis of the job description. The rights can be extended only with the written approval of department supervisor.

1. **Access control:** Access control may consist of the following features:

- Files which can be accessed by the users
- Time period for which the user can log on to the network
- Days of the week when the user can log on to the network
- Workstations that can be accessed by the user
- Access to the network should be restricted to normal working hours. Access to the network after normal hours should be on need or shift basis.

2. **Passwords:** The network administrator initially assigns a user ID and password to users. Users can then change their passwords. For a detailed discussion refer password policy.

The network administrator should be notified when a user leaves the company so that he can delete his user ID and password.

3. **Data security:**

a) **Types of directories:** Data may be saved in the appropriate directory, which may be a group or departmental directory. Users may be allowed to save the data on local user directories also. Other users of the group can access information from the group directory. Members of the department can access departmental directories but only the user can access data from his local directory.

b) **Responsibility for Data Security:** Users should be responsible for the security of data. The responsibilities include

- Taking a backup of files on their individual PC hard drives.
- Security of their individual workstations
- Security of PC back up disks
- Access security
- Non-disclosure of passwords

- Reporting maintenance problems
- Environment conditions

c) Utilities: The policy should specify the utilities that are available to the user. Examples of utilities are Filer, Salvage, Set pass etc. File altering or other unauthorised utilities are prohibited.

4. **Monitoring:** The network administrator is responsible for monitoring the network. Data integrity and security are enhanced when the system is running smoothly and is at peak performance. The network administrator monitors the performance with the help of diagnostic tools available. The policy should specify tools that are available to the network administrator. The network administrator should review network files that are located in the root directory for ensuring file integrity and system performance. All other logs and activity reports should be reviewed on a regular basis.

5. **Prevention and Detection of virus:** The LAN security officer is responsible for the prevention and detection of virus. The network administrator is responsible for purchasing and installing virus software updates. For a detailed discussion refer to our article on Software and anti-virus policy.

Answer: [c] Network administrator

Module: 2

Reference: M2021

Question: A LAN policy should define which of the following persons should be made responsible for reporting maintenance problems or disk errors

- [a] Network administrator
- [b] Users
- [c] Security officer
- [d] Systems administrator

Module 2 – LAN Policy Part 4

Every company should have a policy that defines its LAN and procedures relating to its usage, operation, maintenance etc. The LAN policy helps users know the purpose for which the LAN is to be used, the activities that are supported by LAN, its operations, functions etc. The LAN policy is framed by the IT steering committee and approved by the management. The policy must be reviewed and updated annually so that it stays current. Any changes to the policy must have the consent of the IT steering committee and management.

This is the last of the four part series on LAN policy. In this article we deal with Network hardware, LAN backup and recovery, and purchasing policy aspects of a LAN policy.

1. Network Hardware:

1.1. Responsibility of the user: Hardware may consist of PC workstations, monitors, peripheral equipment, routers, modems etc. The user must take care of the system and report in case of any maintenance problem or disk error that might cause loss of data. The users must not do away with any data unless it is authorised by the person responsible for it. Users should handle the PC with care and follow all the environment conditions specified in the policy. Hard jerks or jolts while a PC is running can damage the hard disk drive. Users should avoid subjecting the PC to excessive vibration or bumps. Smoke, heat, magnetic fields and

excessive dust can damage other equipment. All PCs should have a surge protector. Users should not eat or drink in the vicinity of PCs and LAN equipment.

1.2. Hardware maintenance: The network administrator may purchase an annual maintenance for selected equipments. He should have emergency phone numbers and addresses to contact for replacing or repairing critical network components in case of an emergency.

1.3. Systems integration: The policy should define the systems that can be operated by the users. The systems can be used as terminals connected to a mainframe or as workstations connected to a network. Data exchange happens via the network and with the help of the TCP/ IP protocol.

1.4. Modems and routers: The policy should specify the mode of communication between the data center and the branch offices. For example the data transmission can be through a 10Base T Hub, a router or a DSU/CSU.

The policy should state that modems might be used for communication. It should also specify the vendor, client and employee names. Modems should be turned off when not in use and all its controls should be approved by the management. Modem controls that can be implemented may include:

- Use of passwords
- List of activities that can be performed
- Auto callback to identify dial-in users
- Unique operator identification
- Number of access attempts
- Automatic log-off after a predetermined number of failures to login

2. LAN Backup and recovery:

2.1. Confidential and sensitive data: The network administrator should protect and backup files containing confidential and sensitive data. The policy should specify if the operating system or a person is taking the backup. The frequency of the backup and the storage medium should be specified. Security tables should be backed up and routed to an off-site storage location as needed.

2.2. Protection of data files: The offsite data files of the backup should be placed in a secure location. After a specified period a copy of the backup must be transported and stored at an offsite location. The backups at the branches should be rotated among branch offices. The period for which the backups should be retained must be specified.

2.3. Protection of network files: Onsite backup tapes should be located at a remote place from the server. The most current tape of backup files should be kept in a fireproof cabinet in the company's office and the remaining tapes should be stored in a fireproof cabinet at the branch.

2.4. Contingency plan: Recovery of critical network applications and data files should be included in the contingency plan.

3. Purchasing policy:

3.1. The IT Steering committee: Developing long and short term plans for purchasing LAN hardware and software is the responsibility of the IT steering committee. All major requests should be initiated by the IT steering committee. The network administrator should purchase the approved equipment and software.

3.2. Other purchases: Routine purchases that are included in the annual IT budget should be made by the network administrator. Other departments may make minor purchases that are budgeted.

Answer: [b] Users

Module: 2

Reference: M2022

Question: ISO stands for -

- [a] International Statement of Organisation
- [b] International Organisation for Standardisation
- [c] International Standards Organisation
- [d] International Organisation for Stability

Module 2 - ISO

With the increase in globalisation, different standards for similar technologies used in different countries/regions were causing many technical barriers to trade. Thus, the business community came to the conclusion that a common standard should be adopted by different business communities across the world to standardise the international trading process. This led to the establishment of the "International Organisation for Standardisation (ISO)". However there is a variation between the term "International Organisation for Standardisation" and the full form of 'ISO'. The reason for this is that ISO is not an acronym; instead it is a word derived from a Greek word called "isos", which means equal, thus extending the meaning of equal to apply to standards.

ISO

ISO is a non-governmental organisation, which was established in 1947. Its mission is to assist standardisation in order to promote international trade. For instance, in the IT industry there is an immense need for quick standardisation for products and quality at a global level. Therefore it has become imperative to achieve total compatibility.

The need for standards

Industry-wide standardisation exists when the majority of products and services in that particular industry are of the same standard. Standards are established when all economic players (suppliers, users, government) in that industry reach an agreement on the specifications and criteria to be met. This should include classification of materials, manufacturing processes and rendering of services. These standards help in facilitating trade through -

- Improved product quality at reasonable prices
- Compatibility and interoperability of goods and services
- Increased usability that is ensured through simplifying the usage of products
- Ease of maintenance
- The reduction of models-to-standard product ratio resulting in reduction of costs
- Protection of health, safety and environment

There are two series of ISO standards -

- ISO 9000 - provides a framework for quality management and quality assurance

- ISO14000 - provides a framework for environment management

Complying with these standards can instil a lot of confidence in the users. Quality of products and services are confirmed by conducting a proper audit.

Members of the ISO

The ISO has three types of members -

The member body - It is the national body, which represents standardisation in its country. Only one such body from a country can become a member of the ISO. This member body is responsible for -

- Informing interested parties in the country about the various international standards
- Taking care of the interests of the country during international negotiations that lead to agreements on standards
- Payment of membership dues to the ISO on behalf of the country to provide for the financial support for its central operations

The rights of member bodies include voting in any committee related to technical and policy making in the ISO.

Correspondent member countries, which do not have full-fledged national standards activity, have correspondent members to represent them. Though they do not participate actively in technical and policy development work, they are kept informed of activities of their interest.

Subscriber members - These are members from very small economies. They pay a reduced membership fees for maintaining contact with the organisation.

Answer: [b] International Organisation for Standardisation

Module: 2

Reference: 2023

Question: Which one of the following standards is relevant for a company dealing with inspection and final testing?-

- [a] ISO 9000
- [b] ISO 9001
- [c] ISO 9002
- [d] ISO 9003

Module 2 - ISO 9000 and Management Practices

Most of the ISO standards that exist are highly specific to certain products and services. However, ISO 9000 and ISO 14000 are two standards, which are known as "Generic Management System Standards".

Generic in this context means that the same standard is applicable to any industry or any kind of organisation (whether large, small, private limited, public limited or government undertaking) irrespective of the products/services it is manufacturing/offering. Management system here refers to the management of processes and activities done by organisations. Management system standards help the organisation set up and follow the management system. These standards are usually based on the best practices of the organisation.

Both the families of the standards focus on the processes of the organisation. In simple terms, it means that they care more about how the organisation does its work rather than focussing on products. Although these ISO families do not directly affect the quality of a product, they indirectly make a lot of difference. For instance, in the case of ISO 9000, standard processes ensure that everything is done in the right way and thereby ensuring the quality of the product.

Software companies are also focusing on ISO standards to implement the rules of self-improvement. For software companies it is important to create a quality product, because customer are going global and are demanding higher quality.

ISO 9000

ISO 9004-1 and its other parts provide guidelines for establishing effective quality management and systems. This standard lists the requirements and guidelines for an effective quality management system. The standard only focuses on the requirements that the quality system should meet and not on how they should be met.

The ISO 9000 family also includes other standards that provide guidelines for auditing. This is to assure that the organisation and its clients have quality systems that are established as per standards. This is done through quality assurance models ISO 9001, ISO 9002 or ISO 9003. The differences between the three models are -

ISO 9001 - Lists guidelines for companies whose processes involve design and development, production, installation and servicing.

Effect of ISO 9001 on software development

The following figure shows the software development process.

In the above figure, ISO 9001 affects every segment excepting technology.

ISO 9002 - This is for companies whose activities are not related to design and development. This standard does not include design control requirements; but other wise its requirements are identical to ISO 9001.
ISO 9003 - is for companies that do not have design, process, purchasing or servicing activities and which are in the final inspection and testing process to ensure that products and services are as per the requirements.

ISO 9000 - 3

It has the same provisions as ISO 9001. It is an international guideline for software development, supply and maintenance environments. These guidelines have been made keeping in mind the contract driven (contractual) nature of projects in software department. However, it can be easily adapted for commercial and internal software development.

Thus, quality assurance standards are applied depending on the processes that the organisation uses. Although the above three standards are the important ones, there are more than 20 other standards in this family. Hence, it is suggested that all the standards should be used in an integrated manner to derive maximum benefits.

Answer: [d] ISO 9003

Question: The network of the company must be protected from remote access that may damage the company's reputation due to unauthorised use of information and resources. The policy should cover

- [a] All employees
- [b] Vendors
- [c] Contractors
- [d] All the above

Module 2 – Dial-in access, Remote Access, Wireless Communication Policy and its Audit

Dial-in access policy:

Dial-in access is a medium to access the Internet through a telephone connection and is intended for a limited duration of time. A modem or a similar device is used to initiate such an access. The management should define a dial-in access policy for its employees to protect the company and its resources from unauthorised use. The policy guidelines

- Necessitate authorisation of employees or third parties to access the network through dial-in facility.
- Authorise the new name that is added to the dial-in access list.
- Access to the network should be password protected.
- The employees should not disclose their passwords to any unauthorised persons.
- It is the responsibility of all the users of dial-in access facility to ensure that company's assets are protected and that it is not misused.
- Analog and non-GSM digital cellular phones should not be used to connect to the network. GSM standard digital cellular phones can be used though.
- The user's account if not used for a considerable period will automatically expire and consequently he can get a new account from the concerned official.
- The concerned official will monitor the use of facility.

Remote access policy:

Remote access is the access to the computer or the network from a distance. In a company, staff at branch offices or those travelling or who work from home may need to access to the company's network. Remote access may be through the modem over regular telephone line or may be through a dedicated line. The network of the company must be protected from remote access that may damage the company's reputation due to unauthorised use of its information and resources. The policy should bring under its purview the employees, contractors, vendors and agents of the company. The policy should

- It covers all the dial-in modems, frame relay, ISDN, DSL, BPN, SSH, cable modems and the like.
- The access to the facility will be on the basis of password authentication.
- The login and password should not be shared with others.
- The users when they are connected to the company's network should not connect with any other outside network except their personal network.
- The users should protect the access to the remote connection from unauthorised users.
- The users should ensure that their family members do not use the facility for illegal activities or for personal business interest or violate the company's policy.

Wireless Communication Policy:

In wireless communication, electromagnetic waves carry the signals over part or the entire communication path.

The policy should cover all the wireless data communication devices connected to the company's network. The policy should state that

- Wireless communication devices must maintain point-to-point hardware encryption of at least 56 bits.
- Hardware address must be maintained that can be registered and tracked i.e. MAC (Media Access Control) address.
- There should be strong support user authentication which checks against an external database.

Any employee found to waive the above policies will be subject to disciplinary action that may lead even to termination of employment.

Audit of policies:

The auditor should review the following:

- Policies to ensure that they current.
- Process used to get dial-in approval from the concerned official.
- Identify the person responsible for issuing the passwords and login.
- Ensure that the access is granted on need to know basis.
- Dial-in technical support and problem tracking.
- Process of requesting, approving, documenting the location of analog lines.
- Security and administration over the blockade application.
- Administration over the ID cards for remote/ distribution system.
- Management intention for providing internet access.

Answer: [d] All the above

Module:2

Reference No:M2025

Question: ISO 9000:2000 standards are based on eight quality management principles. One of the principles follows the systems approach to management, which has various advantages. Which of the following comes within the purview of this approach?

- [a] Defining different activities and their working within the system
- [b] Segregation of duties
- [c] Continuous monitoring
- [d] All of the above

Module 2 - Quality Management Principles

The ISO 9000:2000 series is intended to improve processes in organisations. These standards are based on eight quality management principles, which help senior managers to improve performance. International experts of the ISO Technical Committee ISO/TC have used their vast experience and knowledge to develop these principles.

Principle 1 – Customer Focus

The success of a firm depends on its customers. They should therefore understand the needs and expectations of current and future customers, and fulfil their requirements. This is possible only when organisations align their objectives with customer needs and expectations. In addition, customer needs should be properly communicated to the entire organisation, so that everybody works towards fulfilling them. Apart from this, it is also important to balance the needs of other stakeholders such as employees, creditors, shareholders and community, with those of the customers.

Principle 2- Leadership

Leadership provides unity of purpose and direction to the organisation. Leaders are responsible for creating an environment, which encourages employee participation to achieve the organisational goals. Leaders should provide challenging goals and targets, and give employees the freedom and resources to fulfil them. Responsibility and accountability go hand in hand. They should also motivate their workforce by acknowledging their contribution.

Principle 3 – Involvement of people

Employees are the intellectual assets of any organisation and their commitment to work enhances productivity. This helps in two ways – on the one hand, they understand their responsibilities and become more accountable, and on the other, it helps them realise the constraints within which they have to work. This not only encourages employees to share their knowledge and experience, but also to discuss problems and issues.

Principle 4 – Process approach

When activities, tasks and related resources are managed as a process, then the desired results are achieved more efficiently. This approach analyses the interdependencies among various functional departments. It also determines the risk, consequences and impact of each activity on different stakeholders. In addition, it helps in prioritising activities and identifying critical areas.

Principle 5 – The Systems Approach to Management

Here, interrelated processes in an organisation are identified, understood and managed as a system. This ensures that the objectives of the organisation are achieved in an effective and efficient manner. It also helps in identifying interdependencies between different processes, and seeks to develop an integrated approach. Other benefits of this approach are –

- It provides an insight into the functioning of different processes and eliminates cross-functional conflicts
- It helps in defining different activities and how they operate within the system
- It improves the system by constant monitoring, measuring and evaluation

Principle 6 – Continual Improvement

Organisations should make an effort to continuously improve their performance.

Principle 7- Decision making

Organisations should base their decisions on factual data and information. This leads to effective decision-making.

Principle 8 – Mutually beneficial supplier relationships

Suppliers also help to achieve the objectives of an organisation. A good relationship with the supplier creates value. This can be achieved by sharing expertise and resources with suppliers.

Most organisations use these principles to implement quality management systems.

Answer: [d] All of the above.

Module:2

Reference No:M2026

Question: Service level agreements ensure that effective and efficient computer services are provided to users. Which of the following is correct with respect to service level agreements:

- [a] They are limited to certain IT resources
- [b] They are static agreements
- [c] They are arrangements between users and computer operation facilities
- [d] It is the responsibility of user department to provide a framework for each service level agreement

Module 2 – Service Level Agreements

In a growing organisation, the number of users is always on the rise. This increases the IT resources and many times users do not know whom to contact in case of an urgent need. Service level agreements meet these requirements. They also ensure that effective and efficient computer services are provided to users. Service agreements are made between users and computer operation facilities.

Service level agreements can be made in the following areas-

- Number of transactions to be processed in each application system during peak hours
- System availability
- Workstation procurement
- Software procurement
- Average response time/ Turnaround time for each batch job/ application system

It is the responsibility of the management to provide a framework for each service level agreement. At the minimum the agreement should contain the following information

- Description of the service
- Particulars of users/service providers
- Responsibilities of users/service providers
- Availability and response time of service providers
- Service level in quantitative and qualitative terms
- Levels of support
- Continuity of service/contingency plans
- Reliability of services
- Restrictions, if any
- Service changes, if any

Depending on the type of service, the service level agreement should incorporate related application systems, the number of transactions that can be conducted, deadlines for services/ jobs, processing windows etc.

Proper procedures should be incorporated for performance and for specific functions. There should also be a service level manager who takes care of all service level agreements. This person will be responsible for maintaining services. He should also ensure that services comply with service level agreements and should report in case of deviations. All deviations and non-compliance should be analysed periodically and action should be taken on a timely basis so that the same problem does not recur in future service agreements.

Service level agreements are not static agreements. The management should ensure that they are reviewed and updated periodically. The management should also have periodic meetings with users and service providers to resolve issues. This will give a clear picture of the services to be provided. This also helps rectify any lacunae in the service level agreement. These service level agreements are important from the system efficiency and effectiveness point of view. They are applicable to all types of IT resources viz. people, application, technology, facilities and data.

Answer: [c] They are arrangements between users and computer operation facilities.

Module: 7

Reference No:M2027

Question: Which of the following persons is not a member of the IT steering committee?

- [a] Senior managers**
- [b] User departments**
- [c] The control group**
- [d] The information system department**

Module 2- IT Steering Committee

It is essential for every organisation to have an IT steering committee. The IT steering committee is like the watchdog of a company.

What is an IT steering committee, and why should it exist? These are the questions that we shall answer in this article.

IT Steering committee:

The IT steering committee is appointed to overlook the IT related functions of the organisation. It assumes the overall responsibility for activities related to the information system function. These functions range from investments to be made in IT equipment, projects to be undertaken, detailed planning of these projects, their implementation and the like.

The functions, roles and responsibilities of the committee must be defined in the charter. The management of a company should appoint the IT steering committee. The number of the members of the committee depends on the size and function of the organisation. It should include representatives from senior management, user management and the information system department.

IS Department:

Should the IT steering committee exist even when there already an IS department? Many companies think that there is no need for an IT steering committee if there is an IS department already existing in the company. However, if the steering committee does not exist, the management will find that a number of decisions will be taken based on technology and not on the actual implementation and usage point of view. In other words the IS department is not good decision maker from the business point of view. Decisions made by it can lead to wastage of human and financial resources and a poor return on investments made.

Functions:

Does the mere existence or the appointment of a steering committee serve the purpose? The answer is 'No'. If the functions and responsibilities of the steering committee are not well defined, the committee's functioning will be rendered ineffective. For this the following should be well defined

- Charter of the committee
- Committee structure
- Skills that members need to have
- Organisational culture
- IT processes

The functions of the IT steering committee should include:

- Ensuring that the IT plans and policies are in compliance with the overall corporate plans, and that they are current.
- Monitoring and supervising the IT investments of the company, ensuring that the risk is minimum, and it is in line with achieving the overall objectives.
- Considering requests from users and managers for the purchase or development of IT related activities.
- Considering the same in terms of cost, resources availability, benefits, and organisational impact.
- Making decisions related to outsourcing activities.
- Managing IT projects, allotting priorities for them, allocating resources and monitoring the progress.
- Direct the activities of sub-committees like the Project Steering Committee.
- Making a post implementation assessment of the projects in order to assess the benefits derived and making a comparison between the desired and actual result.
- Determining the policy related to research and development and for user charging, data custodians and the like

Answer: [c] Control group .

Module:2

Reference No:M2028

Question: Segregation of duties is the procedure of dividing the critical functions among different individuals so that no two critical aspects of a function are performed by the same individual. Which of the following is not a benefit of segregation of duties:

- [a] It reduces the possibility of frauds and misconducts
- [b] It increases the opportunity for someone to perpetuate misdeeds and conceal errors
- [c] It makes the individual accountable for any unauthorised access
- [d] It reduces the dependency on one individual

Module 2- Segregation of Duties

In general auditing, the job of the auditor is also to ensure whether there is segregation of duties. This applies to the Information System audit as well.

The Federal Bureau of Investigation reported that 71% of those questioned, reported that unauthorised access was by inside personnel. The damage caused in an IT environment is much more than that caused in the

non- IT environment. This is because in an IT organisation all the information is maintained in one place and not dispersed at different locations.

The management implements certain internal controls for the effective functioning of the company. Internal controls are designed to protect the organisation and to ensure that no one person handles all aspects of one particular activity i.e. there should be effective segregation of duties.

Segregation of duties

Segregation of duties can be defined as the process of dividing critical functions among different individuals in such a way that no two critical aspects of a function are performed by the same person. This reduces the opportunity for someone to be in a position to perpetuate misdeeds and conceal them in the normal course of their duties. The personnel should have predefined operational limitations and they should be accountable for any unauthorised access outside those boundaries. The Segregation of duties is the responsibility of the IT manager. Although segregation of duties is similar to a financial audit or other audits which involve segregation of recording, authorising, execution and custody, here it is related to designing, coding, developing, testing and implementing. The manager should grant access to information systems on a need basis.

Organisational structure

Every organisation has its own organisational structure that meets its needs and requirements. Personnel who exist in the organisation are-

- **Developers:** They are responsible for developing systems. This includes designing, writing program code, maintaining, modifying replacing testing and documenting. All these activities must be assigned to different individuals.
- **Computer operators:** Their job includes making the system available continuously, which includes backup and recovery operations. A librarian is also a part of this team. Functions would include maintaining a control over system disks, tapes and documents.
- **Database administrators:** They are responsible for administering the database for the system owner and the users. Computer operators may perform this job in a small organisation.

Guidelines:

Each organisation and department can have their own way of segregating functions. Following are certain guidelines that need to be followed while segregating duties

1. There should be a segregation between the information technology department and information user department.
2. Program developers should not be allowed to test programs. Programs should be tested using test data and original data should not be used. This ensures that the integrity of data is not lost.
3. Computer operators should never be given access to source code. This restricts the chances of computer operators introducing malicious code.
4. Program developers should not perform the role of database administrators.

In small organisations it may not be possible to implement all the above mentioned segregation of duties. In such organisations, other compensating controls should be introduced. Besides this, the HR policy should be framed giving guidelines on how an employee should be hired. It should also specify that no employee should be appointed unless his background has been verified and the references provided have been contacted. For best results

1. There should be rotation of jobs. No employee should be allowed to perform a job for a long duration. The duration should be based on the judgment of the manager.
2. Employees should be forced to take a vacation. When the employee goes on vacation his task will be performed by another. This may highlight errors and frauds that might have been committed by the employee who is on vacation.

Off-the-shelf software:

In this case, the software dictates the segregation of duties. In such cases the manager must make sure that there is rotation of jobs.

Conclusion:

If duties are properly segregated it deters errors and irregularities that may be committed by those developing, accessing or administering computer systems. Segregation of duties is not a solution for the entire security control needs of an organisation. It should be implemented along with other security controls.

Answer: [b] It increases the opportunity for someone to perpetuate misdeeds and conceal errors

Module:2

Reference No:M2029

Question: Many organisations are outsourcing specific activities to Service Providers (SPs). Which is the least probable reason for such a move?

- [a] High security
- [b] Low cost
- [c] Reduced operational risk
- [d] Better service

Service Providers

Gone are the days, when organisations used to purchase software, and hire experts to install and maintain them. Today, they prefer to outsource most activities to External Service Providers (ESPs). There are many types fops, but the most popular are -

Application Service Providers (ASPs)

They provide business applications over the Web. These applications include accounting, CRM and personnel management systems. These are delivered to end users working in non-IT departments of the organisation.

Management Service Providers (MSPs)

They deliver system applications over the Web. Examples of such applications include remote control, server mentoring and network monitoring. These applications are delivered to end users, working in the IT department of the organisation.

Two fundamental aspects that all ASPs and MSPs have in common are -

- Web- based delivery of applications, and
- Storage of user data at the Network Operating Centre (NOC) in the premises of SPs

Why do organisations prefer to outsource activities to SPs?

Organisations have started outsourcing different activities, due to various benefits that they offer -

- Low initial set up cost - The software to be used is provided by the SP, and payment is made on the basis of the usage. A huge initial outlay on purchase/development of software is saved.
- Reduced risks - By migrating to SPs organisations can transfer their operational risk that includes maintenance, staffing and upgrades, thus reducing their overall risk.
- Greater rate of return The initial outlay is low, implementation is quick, and the return on investment is also fast.
- No need to recruit experts - Since SPs staff the Network Operations Centre (NOC) with experts in different disciplines, clients are saved the effort of hiring and training them.
- Better performance - Since SPs provide applications to many organisations, they are experienced, and provide better, and more reliable processes.

Security issues

Every organisation that outsource its activities to SPs should consider the following security aspects -

1. Physical security of the user data
2. Ownership rights of the data at NOC
3. Accessibility of data at the NOC
4. Issues regarding the Internet link that connects the client and the SPs
5. Software that is installed in the network of clients

Conclusion

No doubt, there are many advantages to outsourcing activities. However, the organisation should conduct a due diligence, before giving the contract to an SP.

Answer: [a] High Security

Module:2

Reference No:M2030

Question: When an organisation outsources its activities, it also provides data to the service provider. In such cases, the ownership of data -

- [a] Is transferred to the service provider
- [b] Is with the client/organisation that outsources services
- [c] Is shared by both parties
- [d] Is not transferred

Module 2 - Security Aspects of Service Providers (SPs)

While discussing terms with SPs, the focus should be on security issues, such as -

1. Physical security of user data
2. The Internet link that connects the client and the SPs
3. Ownership rights of the data at the NOC (Network Operations Centre)

4. Accessibility of data at the NOC
5. Software that is installed in the network of clients

Physical security

Typically, client data is stored at the SP's offsite location, in most cases, at the NOC. Thus, it is imperative for the client to thoroughly analyse the physical security provided at the NOC. The following points should be considered -

- Are data access checks in place?
- Have procedures been laid down for granting access to authorised personnel?
- Have appropriate steps been taken to safeguard the NOC from fire, fog, and rain?
- What is the backup arrangement and schedule maintained by the NOC?
- Does the SP have a documented and tested disaster recovery plan?

Internet link security

When the SP provides web-based applications, then the client's and SP's servers are linked through the Internet. In case, adequate security measures are not taken to secure this link, then both the SP and the client are vulnerable to hackers. Thus the SP should provide a solution by-

- Connecting with the client, only after getting through its firewall, or
- Providing a customised VPN (Virtual Private Network) solution

Clients prefer the second option, as the SP provides a standardised solution to all. The SP is not affected by changes that are made in the client's firewall. Similarly, clients need not worry about the SP, when they make routine changes to their firewall.

Ownership of data

The data belongs to the client, and the SP should not have access to it. It is required to store, guard and provide data to the client, as and when the client makes a request for it. However, an SP may use the data for statistical purposes in accordance with its terms with the client.

Access to client data

When an organisation decides to outsource, then it has to entrust the data to the employees of the SP, as they have to maintain and upgrade the data, manage the operations, take backups and the like. Thus it is not possible to restrict employees from accessing the data of the client. However, some SPs are able to minimise the risk by providing access to data files of the client only to a very limited number of employees. The SP also has to ensure that client A cannot access the data of client B.

Access to customer networks

In most cases, SPs usually install 'agent software' at every end-user terminal at the client's premises. In some cases, this software is installed at the end-user's servers also. This software enables communication between the client and the SP, and runs applications. However, there is a threat that the SP may access individual client systems, and be privy to confidential information. This is yet another issue that organisations have to be careful about.

Answer: [b] Is with the client/organisation that outsources services

Module:2

Reference No:M2031

Question: Due diligence of third party service providers need not cover

- [a] Evaluation of testimonials
- [b] Evaluation of infrastructure
- [c] Evaluation of experience
- [d] Evaluation of ownership

Module 2 - Control Objective - Managing Third Party Services

In an IT environment, third parties are indispensable considering the amount of service they provide. When companies outsource certain processes and services, third parties are involved. Several hardware, software and communication assets supplied by different vendors need maintenance and servicing that are provided by third parties. In many cases, for contingency and disaster recovery, companies agree with third parties for a hot site or cold site. As such, there is a need to manage third party services. The roles and responsibilities of third parties should be clearly defined, followed and maintained.

IT objectives of efficiency and effectiveness are essentially aimed at managing these services. Third party services may have an impact on all IT assets viz. people, application, technology, facility and data.

Legal enforceability: All third party service agreements would fall within contractual obligations and hence legal and regulatory requirements should be incorporated. While providing services third parties have to be given access to hardware, software and other assets. They also interact with employees for confidential information. One major control objective is to incorporate properly worded non-disclosure agreements. This should conform to universal business standards and enforceable legally.

Identification and supplier interface: The objective is to ensure that all services provided by third parties are identified and documented. The document should contain details of services and service providers. It should include the technical details and service details, clearly indicating the technical and organisational interfaces.

Owner relationship: A specific person designated for the job should monitor all third party services. He should be made responsible for the services quality, timeliness, adhering to contractual terms etc.

Contract: The objective should be to cater to appropriate contractual terms depending on the type of service, periodicity of service, risk involved and the assets involved. No third party should be allowed to commit a service unless a formal contract is defined and agreed upon.

Qualification: Before third parties are appointed to provide service, due assessment should be done on the selected parties. It should include an assessment of their capabilities, their experience, their infrastructure, manpower and the utilities to be used by them. An evaluation of testimonials given by them on similar services undertaken for other customers would be helpful in finalizing the parties.

Continuity of service: The contract should include a provision for continuity of service in case the third parties cannot provide the services. Management should consider the business risk related to this and legality and liability involved. If necessary escrow agreements should be entered where appropriate.

Monitoring and maintaining: The person in charge of ensuring quality of third party agreements should monitor the continued and timely service, evaluate periodically and report to management. He is accountable for deviations, negligence and non-performance. He is responsible for initiating penalties and informing legal department in case on continued non-performance by the third parties.

Answer: [d] Evaluation of ownership

Module:2

Reference No:M2032

Question: IS activities can be outsourced to a third party. To evaluate the performance of the service provider the auditor should

- [a] Benchmark the services
- [b] Identify the risk associated with outsourced activity
- [c] Determine the duration of the contract with the service provider
- [d] Determine the frequency at which the payment will be made for services

Module 2 - Outsourcing of IS activities

A company can outsource some of its activities to a third party. The IS activities that can be usually outsourced are data centre operation, application system development, maintenance and the like. In this article we discuss how an auditor is concerned with outsourcing.

When any services are outsourced, the company should bring the same within the purview of the audit by including such services in the audit charter. The auditor should be provided access to the agreements between the company and the service provider. He should have the right to carry the audit of such outsourced service that is deemed necessary by him. The auditor should be asked to report his findings, give his conclusions and recommendations.

Now we shall discuss how the auditor goes about conducting the audit of the outsourced service.

The auditor during the course of his audit should

- Understand the nature, timing and extent of outsourced services
- Identify the risk associated with outsourced activity
- Identify the controls that have been provided by the service provider to ensure that the services are provided as entered into the agreement
- Assess whether the controls are reasonable and assure that the services will be provided as per agreement and all undesired events will be prevented or detected or corrected
- Determine whether the agreement provides for the audit of the outsourced service

Pre-audit:

The auditor before commencing the audit task should consider the previous audit reports. He should also consider the policies on service level agreements and third party service agreements. This would help him obtain a better understanding of the service provider's environment. He should ensure that the objectives of the audit have been communicated to the service provider.

Audit:

During the course of the audit he should obtain the service agreement and ensure that the same is in

agreement with the overall company policies and procedures. He should obtain a copy of the minutes of meetings as regards the outsourcing of the service. The contract should give complete account of service providers and their services. Detailed review of the contract should be conducted to determine if the qualitative and quantitative provisions confirming the obligations are defined.

The auditor should ensure that the following form a part of the service agreement:

- Service provider should comply with all legal requirements that are applicable to the outsourced service
- Activities of the service provider will be subject to controls and audits
- Auditor has the access rights to the service provider's facilities
- Performance monitoring procedures
- Contingency planning to be done by the provider to ensure continuous service
- Duration of the contract
- Non-disclosure requirements i.e. any such information about the company that cannot be divulged
- Cost of service and frequency at which the payment will be made for services
- Fidelity insurance arrangement

To evaluate the performance of the service provider

- Services should be benchmarked against competitors or industry practices
- Ensure that there is adherence to security policy specified by the company
- Ensure there is adherence to the service provider's personal policies and procedures
- Continuous monitoring by the company of the services being provided
- Evaluation of the action taken by the company where the agreement is not met

Where the service provider does not cooperate with the auditor he should report the same to the company. Before issuing the report he should discuss the same with the service provider. He is not responsible for forwarding the report to the service provider. The company will forward the final report. If any restrictions are imposed on him either by the service provider or the company the same should be mentioned in the report. An explanation should give details of the effect of the restriction with respect to the audit.

Post-audit:

The auditor should determine whether any actions have been taken on the findings and the recommendations specified in his audit report.

Answer: [a] Benchmark the services.

Module:2

Reference No:M2035

Question: The purpose of establishing Information System Security Evaluation Team is to

- [a] Guide the management and help them in protecting information assets
- [b] Help in recruitment of the staff
- [c] Assist in appointing auditors
- [d] Frame the security and other policies of the company

Module 2- Information System Security Evaluation Team - Security Insurance

Information systems that were once confined to large companies can now be found even in small companies. The management must establish Information Systems Security Evaluation Team (ISSET) for maintaining the

security and reducing the risk of disruption of business operations.

Purpose: The purpose of establishing ISSET is to

- Guide the management and help them in protecting information assets
- Assure that the company's security policy are appropriate and they are in accordance with law
- Providing the system administrator with a team of security specialist when required
- Audit the systems of the company to ensure that the company has implemented the security measures and security policy.

Structure: The structure of the team will depend on the size and business of the company as well the level of information operations. The size of the team could also depend on the areas of expertise. For example if the company is using different operating systems, then the members with specific experience in the given operating system would be included in the team.

The team should have permanent members though they need not be full time members. The minimum number of members should be three. Two members can conduct on-site audits and the other member for any matters that come up in the absence of other two members. The membership to the team could be an additional duty along with their other responsibilities in the company. But sufficient time should be allowed to the members for training and study so that they can update themselves in information security theory and practice.

Management support: For the success and effective function of the team, management support is necessary.

Supervision: For the team to carry on the work smoothly and effectively there should not be any conflict of interest. Political conflicts arise especially when the members are required to perform the team function as an additional duty. For this purpose it should be seen that the team reports to Chief Information Officer or Director or President or Vice President of the company.

Operations: The team in order to ensure that the information assets are protected should conduct audits and on-site inspection of the information networks, applications and services. The team will prepare an audit plan schedule. The audit plan will be published so that the various departments can know when they will be subjected to audit. The team to test the security of servers, firewalls and routers will be aided by automated tools. Where the team consists of temporary members an audit checklist should be prepared to ensure that all areas are covered in the audit.

While conducting the audit the following should be ensured

- The team members are introduced to key managers and IT staff.
- Key managers and IT staff are explained the purpose of the audit, how it will be conducted and how it will be useful.
- The team when conducting audit should not disrupt the normal activities except when it is necessary
- An exit briefing should take place.
- The result of the audit should be presented along with the detail about who should receive the final report.
- While preparing the report, the draft report should be presented to the department for review. The comments of the department should be included in the final report.

Other functions: Besides auditing and insuring that the assets are secured, the security team can serve as a

- Focal point to get expertise in risk analysis. Risk analysis helps in setting of a good security plan. The security provided should be based on the risk assessment and the magnitude of the damage that could result from loss, misuse or unauthorised access to or modification of information.
- Education and training resource. Good information security ensures the confidentiality, availability and integrity of systems and applications. Therefore the team who are to ensure information security

should be knowledgeable and best trained employees. Usually the company has several offices at different locations or may employ a single person to look after security matters. ISSET can help in developing handbooks, manuals, and checklist to provide the technicians with the knowledge and tools to implement the company's information security program.

Conclusion: There are some who believe that ISSET exists to find problems and punish the irresponsible employees and managers. Others believe that they are a form of insurance to ensure that security of the assets is being provided for. If the latter is accepted then the team identifies the risk, takes actions to mitigate them and educate the managers and IT staff.

Answer: [a] Guide the management and help them in protecting information assets

Module:2

Reference No:M2036

Question: IT operational efficiency is measured in terms of:

- [a] Technological value added to the organisation.
- [b] Its impact on other business processes and business units.
- [c] Decreased costs and increased revenue.
- [d] All the above

Module 2 - IT Efficiency and Business Value

Measuring, delivering, enhancing, and communicating IT value has emerged as perhaps a major challenge facing today's Chief Information Officers. A recent survey found that CEOs believe that 55 percent of IT spending is "strategic" in nature. However, the same senior executives believe that only a third of IT spending results in a measurable impact on profitability. The challenge is clearly formidable. For one thing, objective and meaningful criteria for measuring IT value are still in their earliest stages. At a more basic level, there's no consensus on what role IT and IT management-should play within an organization.

How does IT fit in?

IT adds value to a business when it either *decreases costs or increases revenues*. Clearly, IT can do both. As IT spending increases, and as IT becomes recognized as an increasingly important strategic tool, IT managers are clearly eager to take on the challenge of using IT to help a business run successfully. But they are mistaken if they think that IT provides value only through leading-edge initiatives and those who think that they can focus on business strategies and neglect IT efficiency are in for a ride.

Efficiency v/s Value

Efficiency is doing things right while effectiveness is doing the right things. But the question that comes to mind is how does a manager think about this? Is it doing things right-focusing on the mundane but essential day-to-day operations? Or doing the right things-identifying and implementing the latest tools and systems that will deliver a competitive advantage, and thereby helping to take business in a strategic direction?

An efficient IT operation adds value and enhances the strategic role of IT in a variety of ways. First of all, efficiency is needed to gain credibility and respect within the organisation. Senior executives will be more inclined to listen to strategic ideas from a manager who delivers services efficiently and who runs his show successfully. Second, an efficient IT operation makes available the money and time needed to undertake

strategic IT initiatives that enhance the business. To fund strategic IT initiatives, managers have to manage efficiently and squeeze capital out of existing IT infrastructure budgets which can then be invested in e-commerce, data warehousing, and other advanced applications that address issues of effectiveness. Finally, any IT project, no matter how innovative, will at some point be judged on its efficiency. A manager may boast off by implementing an application that runs successfully but if it turns out that a competitor has implemented a similar program for half the cost, the credibility gained by the manager will be short-lived.

Conclusion

IT operational efficiency enhances business value in a variety of ways but IT value cannot be measured all alone. Its impact on other business processes and business units must be measured. Also, other business unit managers must be involved in defining and measuring the role and value of IT within a business.

Answer: [d] All the above.

Module:2

Reference No:M2037

Question: Which of the following criteria is essential to evaluate information processing service providers?

- [a] Input-output controls.
- [b] Job scheduling
- [c] Storage media.
- [d] Contract agreement

Module 2 – IS Service-Providers

Information processing service providers cater to the needs of financial institutions and other businesses. Processing centres have multiple clients and services. These services have to be recognised and evaluated to ensure that the existing controls are adequate. The following guidelines would help Auditors of service providers to examine the control process:

1. **Customer details:** The client list and data related to each client should be documented, including their names and addresses, types of services provided and the like. Evaluate the number of customers for each type of service.
2. **Legal rules:** Examine whether the services provided to the financial institutions are in accordance with the rules and regulations in force.
3. **Contract agreement:** Examine the contract agreements between service providers and customers.
4. **Quality:** Scrutinise management reports like quality indicator reports, customer complaint file, and payment records to evaluate the quality level of service provided to each client.
5. **Service function:** The efficiency of the customer service function can be evaluated through specific management reports. Ensure categorisation and summarisation of the information. Determine the effectiveness of the customer service department in providing feedback.

Auditors must enquire the management on the deficiencies found during the evaluation process. Corrective actions must be recommended to counter the same. A summary statement showing the details of strengths, weaknesses and deficiencies of control procedures has to be made. It should contain detailed information about the process to assist in future inspections.

The auditors should specifically look into:

I. Contracts

Verify the contract agreement and determine whether the following are mentioned in it:

- The type of the service to be provided
- The charges for the services mentioning separately for each type of function like development, conversion, processing and the like.
- The time frame to deliver the work
- The service provider or the client company's responsibility for protecting the communications network.
- Provisions for safeguarding records and their backups, which are useful during emergencies
- The provision for sharing the disaster recovery plan (maintained by the service provider) with the clients to evaluate efficiency of the system.
- Responsibility for the source documents when they are in transit, rest with the service provider or with the client.
- Provision for maintenance of insurance
- The method in which the confidential records are stored
- Ownership of programmes and documents
- Provisions for returning data files at the end of the contract period
- Mention of a sudden termination of the contract due to price changes, the time limit and the method of cancellation.
- Order of processing activities
- Periodicity of reports and the content or details of report to be submitted by the service provider
- Provisions for penalties to avoid unreasonable termination of the contract or unfair practices.

Examine the terms provided in the contract.

II. Service quality:

The quality of the services provided has to be evaluated by considering the following:

- Compliance of the services provided with the terms agreed in the contract
- Customer complaint file and the approach to solve them
- Training on specific applications offered to the respective users.
- The user manual, containing guidelines for control over source and output documents supplied to the customers.

After an evaluation, management should be probed regarding the inconsistencies after which corrective measures should be suggested.

Answer: [d] Contract agreement

Module:2

Reference No:M2038

Question: Which one of the following is not a function of Operations department?

- [a] Performance monitoring
- [b] Library and data file protection
- [c] Equipment control
- [d] Software documentation

Module 2 – Operations department functions

The main function of computer operations department is to maintain a proper control over equipment, operations, data preparation, library and data file protection. It is responsible for performance monitoring and disaster contingency planning.

Operator's Run Manual should contain all the information like instructions for processing, re-run, special applications, file rotation procedures, recovery and emergency procedures. The manual should be made accessible to operations personnel to perform their functions. In addition, the overall procedure manual covers maintenance and operation of equipment, staff policies and coordination aspects.

Operations management must have proper control over operators. Techniques like separation and rotation of duties are used to achieve this.

Separation of duties: No individual should be made responsible to start and complete a transaction. Computer operator's duties (equipment operation) should be separated from others as a part of internal control procedure. But at the same time, operators must be trained to perform other duties in emergencies. The aim is to avoid overlapping between functions like operations and data preparation for processing. It minimises the danger that could be caused by employees to information systems.

Rotation of duties: It serves as an effective control measure for small concerns where the scope for separation of duties is little. The aim of rotating duties among operators is to identify the irregularities by the previous operator. It also acts as a cross-training tool in large concerns.

Computer operators are responsible for common preventive maintenance like cleaning tape heads, printers, which doesn't require any technical knowledge. Operations department has to

- Monitor the maintenance programme conducted at regular intervals to assess the employee performance.
- Maintain a record showing all the hardware problems faced during maintenance.
- Make sure that agreements with equipment manufacturers contain adequate provisions for repair services. Responsibilities of the vendors must be clearly stated in case of more than one manufacturer.
- Must undertake all steps to avoid unauthorised access to the programs and data files by maintenance staff.

Operations department has to prepare and update a manual for computer operation. The manual should consist of instructions for input/output forms identification and programmed halts, forms alignment, input and output disposition. It should also state the hardware requirements and the records used. The operating log has to be regularly monitored.

Scheduling the workload of computer is essential for an efficient system operation. Management has to consider the following while scheduling the production runs:

- Utilisation of computer resources
- Completion of jobs on the basis of available data
- Processing jobs on priority basis

The timing of input and output has to be mentioned in scheduling. Management has to ensure that unscheduled jobs are processed under proper authorisation. It has to compare the actual time taken to process with the scheduled time. Any discrepancies have to be properly examined.

Back up: Back ups for programs and data is essential to prevent data loss. Operations department has to ensure the adequacy of back up procedures by reviewing the programmes. Back up of Master and Transaction files has to be conducted either on daily basis or cumulative basis. Rotation of back up files is essential to minimise the institutions risk.

Answer: [d] Software documentation

Module:2

Reference No:M2039

Question: The role of _____ is to define the security policy, perform risk analysis and ensure that all the employees are aware of the security

- [a] management
- [b] System maintenance in charge
- [c] System developer
- [d] IT security manager

Module 2 - Security structure for an organisation

Every organisation has its own structure depending on its needs and activities. But there are certain fundamental activities that are to be carried out in each organisation. We shall discuss few of the roles in this article.

The roles listed here are not exhaustive. It may vary from organisation to organisation but the responsibilities must be assigned to specific person.

People: Given below is a brief description of the role of each person in the organisation

management: The management has the ultimate responsibility of ensuring the adequacy of security and its implementation thereby.

IT security manager:

- Define the security policy
- Advise the management
- Perform risk analysis
- Ensure that all employees are made aware of the importance of the security
- Update himself with the latest security equipments and software that are available

Business unit manager:

- Responsible for the security aspect of his unit
- Report to the management
- Should not be involved with audit

System maintenance in charge: Systems may be maintained either by an external entity or internally. When the services are outsourced to an external agency, the service level agreement should be entered into, which should emphasise on the security aspect to be followed by the agency.

System developer: He is in charge of ensuring that the security features are implemented in the system during the designing and the development stage.

Project Leader: He has to ensure that the security features as defined in the security policy of the company are integrated into the projects.

Users: Users should be aware of the security policy of the company and any lapse of security on his behalf will have serious consequences which may even lead to his removal from the company. They should classify the information on the basis of sensitivity so that other the users are aware of the security aspects to be implemented.

Auditor: Either an external or an internal auditor may be conducted the audit. The auditor should not be involved in security administration.

Processes

The following are few of the security processes that are carried out in organisations.

Security Help Desk: The help desk provides help to the users in event of a problem. It is usually the case when users have forgotten their passwords. Before coming to the aid of the user, the help desk should authenticate as to whether the user is what he purports to be. The security guideline should be framed for this purpose so that no outsider can gain entry into the system.

Change management: The changes must be properly planned and tested before moving them into production environment. Only authorised person should install system upgrade. When changes are made to the hardware it should be ensured that anti-static wrist straps are worn, and instructions of the manufacturer are followed.

Systems monitoring: Monitoring should be decentralised so that the appropriate action can be taken in event of a security breach at the earliest.

Audit: Audit should be conducted at periodical intervals of the various policies and procedures and check for proper follow up. Audit should include servers, IT security, management, IT administration and all other IT resources.

Disaster planning: The security aspects have to be implemented even in case of a disaster. (Our other articles deal with this issue in detail).

Answer: [d] IT security manager

Module:2

Reference No:M2041

Question: Which one of the following is a principle of successful risk management?

- [a] Risks once identified should be re-evaluated
- [b] Risks are identified only once for each operation.
- [c] Activities are scheduled, based on the criticality or the risk factor of the activities
- [d] Risks identification needs to be done in person independent of all other operations.

Module 2 – Risk Model For Operations-Introduction

This series of articles explains the basic principle of risk management and the risk based operations methodology. First an overview of the risk model is discussed .The overview describes the basic characteristics of a risk model, its principles, benefits and the process overview.

Background

The risk-based model is structured around proven risk management techniques. It involves adopting these techniques to the problems that the operations staffs in an IT department face in their day-to-day activities. It prescribes a customised five-step methodology, which can be repeated often to combat the risk inherent in IT operations. This model can be easily integrated into small to large IT operations. Since the businesses are more and more dependent on IT, IT operations have become that much more critical and IT failures will have a direct impact on the operations of a business.

Elements of a risk based model

The model identifies the following basic components. They are described below

Risk and characteristics of risks

The word "risk" indicates prospects of damage or loss. Risk has some basic characteristics. Understanding these basic characteristics will help in managing risks.

- **Risk is all-pervasive:** Every business environment has risk. Risk is the most fundamental part of any organisation. No business can be devoid of risks. Such an environment does not exist.
- **Risk per-se is not good or bad:** only the outcome of a risk is good or bad. If some loss arises due to the risk, the loss is considered bad for the business. If some gains are made out of the risks then the outcome is good.
- **Risk cannot be avoided but can only be managed:** No organisation or team can avoid risk. Only through proper risk recognition and analysis can risk be managed, but it cannot be avoided.

Risk management principles

The risk based operations model is based on three risk management principles.

Continuous Risk Assessment

This means that the team carries out the process of identification of new risks on a regular basis and the risks that are already identified are re-evaluated in the same way.

Integration of Risk into all functions

This means that all IT operations are involved in risk management. Every process owner should participate in the identification of risks and risk indicators. For instance, the manager in charge of a help desk will identify the risks associated with that function.

Risk based scheduling

Every critical activity in IT operations should be based on the relative risk element of each activity. For instance, while scheduling testing, those modules that are categorised as high risk and are critical should be tested first. This will help in saving the resources of the organisation.

Establish an acceptable level of formality

Any process should have an optimal structure. A trade off needs to be done between a very simple structure with less control and generally preferred by employees and a very strict structure with many protocols, which provides a high level of control over the activities but is frequently despised by the employees. Likewise even the risk-based model should also be structured optimally in an organisation.

Answer: [c] Activities are scheduled, based on the criticality or the risk factor of the activities

Module:2

Reference No:M2042

Question: When IS services are outsourced the controls to mitigate the risks are to be implemented by

- [a] The service receiver only
- [b] The service provider only
- [c] Service receiver and service provider
- [d] None of the above.

Module 2 – IS servicing – Controls

When the activities of a company are outsourced they are exposed to certain risks. Necessary controls have to be implemented both by the service provider and receiver. The controls to be implemented are

- User institution controls
- Operational controls
- Technology controls

User institution controls

The controls that are implemented by the service provider should be on similar lines as that of the service receiver. Controls that are implemented must secure the information and decrease the level of risks to which the information is exposed. They can basically be implemented through sound policies, procedures, separation of duties, access controls, audit and the like. The objectives that these controls should meet are

- Integrity and confidentiality of information
- Physical, logical and environmental controls
- Backup and recovery capability
- Protection of information during input and output process

The service receiver should have knowledge of security requirement and identify the security features he wants, rather than accepting the security and control available with the service provider. The requirement should be compared to available features and the gap, if any, be filled by either implementing compensating controls at receiver's end or insist on additional controls at the providers end at an extra cost.

Operational controls

In case of outsourcing, certain activities originate from receiver's end, like data origination and document preparation or transmitting input data and the like. Then the activities are continued at service providers end viz. processing, back up, report generation and the like. Then the activities are shifted back to the receiver's end viz. analysis of output, decision taking and the like. All operational controls relevant to carry on the respective activities should be in place depending on who is responsible (provider or receiver). The operational

controls can be sub-classified into separation of duties and internal quality controls.

Separation of duties: The basic internal control is segregation of duties. Segregation should be such that no single person is in charge of the execution of a single transaction. There should be rotation of jobs. In case of sensitive information dual controls should be implemented.

Internal quality controls: These controls can be further sub-divided into administrative controls, monetary value controls and other controls.

- **Administrative controls:** The management must review daily operations and all the exception reports generated by the system.
- **Monetary value controls:** All the financial transactions should be subject to dollar controls. Dollar controls are the controls over the monetary value in the transaction.
- **Other controls:** These controls are implemented when dollar item is not present. Controls should be present to ensure that no file has been altered.

Technology controls

Here again the control responsibilities lie with both service provider and service receiver.

Technology controls can be categorised into data communication controls, system features and controls and backup considerations.

Data communication controls: The service receivers should review these controls. Data communication controls can be categorised into

- **User identification controls:** The service receiver company must allow only authorised individuals to use the system. They should also apply appropriate physical and logical access controls.
- **Level of accessibility:** Accessibility to the information should be on need to know basis. There should be automatic log off, if the system is left unattended for a long time.
- **Restricted transactions:** Any adjustments to the monetary items and other sensitive information should be restricted and can be altered only by authorised personnel.
- **Exception reports:** Exceptional reports should be generated and reviewed by authorised personnel who have no conflicting responsibilities.

System features and controls: The service provider should ensure that the following communication controls are implemented

- **Inquiry-only system:** Where the user can only view the records and cannot alter them.
- **Memo-post system:** The user is allowed to create records but the service provider makes them permanent.
- **Online post system:** In this system the user can directly make alteration to the system. They require more strict controls for access to the system. The controls and exceptional reports should be reviewed periodically.

Answer: [c] Service receiver and service provider

Module:2

Reference No:M2043

Question: IS service contract need not include which of the following?

- [a] Description of the services that are outsourced
- [b] Security features that should be implemented
- [c] A clause about the termination of the contract
- [d] Internal policies and procedures at the receiver's end.

Module 2 – IS service contracts

When information system services are outsourced, its security is not just the responsibility of service provider. The security receiver is equally responsible to fulfill his roles. In this regard the contract between the service receiver and service provider should be properly drafted to minimise the problems in future. It should define both the parties' responsibilities and liabilities. It should establish a baseline performance standard for services being outsourced.

IS service contract at the minimum should include the following:

- **Description of the services:** The contract should clearly state the services that will be outsourced. This should include a detailed description of all applications to be processed by the service provider. Besides, there should be a provision for adding or deleting the services.
- **Priorities:** Processing priorities in case of normal and emergency operations should be stated.
- **Security:** The security features that will be implemented in the system should be specifically stated in the contract. The provider and receiver should agree upon the security software that would be used and the security features available in the applications. Also, it must be determined as to who and how will the requirement for special security be implemented. It should also cover periodical inspection. Audit by the receiver of security and control procedures must be available in service provider set up.
- **Audit:** The contract should state whether the service receiver could get the audit of the service provider done. If no, then will the service provider make available the auditor's report? Mention must be made of the frequency, and the type of audit coverage that will be provided.
- **Backup:** The backup arrangement by the service provider should be clearly stated. A detailed note on the backup requirement based on the type of processing, the applications used and the location where the back ups need to be stored should be covered in the contract. Besides this the service provider should also have adequate disaster/ contingency plan.
- **Report:** The time frame in which the report will be sent to the service receiver should be mentioned.
- **Changes:** Before making any changes to the procedures, reports and the like the service provider should notify the service receiver. Similarly if the receiver requires any change in the processing frequency and the like, he should give adequate notification to the service provider.
- **Insurance:** The service provider would have adequate insurance coverage for the hardware/ software and the like. But he may not take up insurance on data. The data should have adequate insurance, as there is scope for data loss when it is in transit to and from the service provider's place. The contract should also state the provider of insurance.
- **Termination:** The contract should provide for the ownership of the programs, data files and other material when the contract gets terminated. It should also state the duration of the notice to be given by both the parties to each other for terminating the contract before its expiry.
- **Assignment:** The contract should specifically state that the service provider is not to outsource the outsourced activity to any other person without the consent of the service receiver.
- **Cost/fees:** The cost should include all the related development, conversion and processing charges. Where the software is specifically developed for the service receiver the contract should state owner of the software. It should clearly define the costs for one time development, the conversion costs and the costs of periodical maintenance and service.
- **Revision of cost/fees:** A provision for increase in the fees/ cost should be provided to cover the increase in operating cost.

Answer: [d] Internal policies and procedures at the service receiver's end

Question: Which of the following is not the advantage of decentralised form of organisational structure?

- [a] Better information
- [b] Low communication cost
- [c] Consistency
- [d] High-speed

Module 2 – Organisational structure of Information Systems function

The increasing level of dependence on integrated, on-line and real time systems has complicated the organisation structure. Evaluation of the organisational structure helps an auditor to understand the adequacy of internal controls existing over the Information Systems function. Organisational structure of an Information Systems can be of two types, centralised or decentralised. Each type has its own advantages. Management has to decide based on the merits of each option.

Centralised organisational structure provides the following benefits:

1. **Control:** Centralised structure ensures better control.
2. **Consistency:** In a centralised organisation, the work is performed in a group. It ensures consistency.
3. **Recruitment and retention:** Centralised organisational structure ensures recruitment and retention of skilled IT professionals.

Decentralised organisational structure provides the following benefits:

1. **Better information:** Decentralised structure provides better information and brings end user satisfaction
2. **Cost:** Reduction in communication cost
3. **High-speed:** Enables quick system development

Role of organisation in IS functioning

Organisational structure of IS functioning should ensure the existence of proper general controls on all activities. It should ensure that adequate measures for segregation of duties exist. For example, those who are designing and developing software should not be involved with operation and library functions. The IS manager is in charge of effectiveness of IS operations like system development, data accuracy and its security and supplying the requirement of the users.

System development is a capital project involving huge capital outlay. Therefore, management is responsible for coordinating the project and aligning the project goals with the organisation goals. A team consisting of several functional heads will form an advisory board to execute the function according to the needs of the organisation. They evaluate the present cost and the future benefits involved in the proposal. They also conduct post-development evaluation to assess the system at periodic intervals.

Role in system development: A good organisation structure provides for segregation of duties between system analysis, programme development and programme maintenance. System analysis personnel do all the preliminary work in the system development process. Programme development personnel are involved in development programmes for the new system. Programme maintenance personnel have to handle the post

development maintenance.

Role in quality assurance: Developing and monitoring the quality assurance programmes is the duty of quality assurance department. Organisational structure should provide for clear definition of duties of assurance department.

Security: A separate department responsible for performing the security operations helps to evaluate the security function. Their nature of work involves evaluating the security controls.

System operations: Data base administration, computer operations, input and library functions are several sub-functions in the system operations. Organisation structure must ensure adequate supervision and internal controls over the operations.

Evaluation of organisational structure

1. All the critical **personnel functions** like programming, development, maintenance, operations are to be clearly segregated and properly controlled. To ensure, auditor should examine the organisation structure, duties of IS personnel and job descriptions.
2. Auditor must ensure the adequacy of **Quality Assurance Programme** by examining the compliance of products developed with the assurance standards. He should also enquire about the reporting system on quality assurance.
3. Auditor must examine the functioning of **security programme**. The security controls existing over data systems accessibility need to be evaluated.
4. **Physical security** of computer room and library, adequate controls over input is to be ensured. Auditor must examine that the data base administration, computer operations and library functions are segregated.

Answer: [c] Consistency

Module:2

Reference No:M2045

Question: To prevent operators from accessing program documentation production source version is the function of

- [a] Library controls
- [b] Operator controls
- [c] Equipment controls
- [d] All the above

Module 2 - Operations Management functions - Part II

The following are the guidelines for Operations Management to exercise control over equipment, operators, library, data file media, housekeeping and the like.

Equipment controls

Equipment controls include proper procedures to prevent and detect unauthorised programme execution and system usage. Console printer, internal CPU clock, and system activity logs, serves the management as effective control tools and audit trails.

The following measures should be taken to make the equipment control effective:

- An attendant must be present in the computer room during system operation.
- During a cross check on personnel, there must be at least two operators present at a time.
- There are certain routine checks like internal label checks, read and write checks, which minimises processing the wrong data. Operators should not be allowed to take any decision that would compromise such routines.
- Jobs must be processed as per schedule
- Only authorised persons should be allowed to run the equipment.

Operator controls

Suitable security and internal control rules must be established to have proper control over computer operators. The following are such rules. Computer operators must be prohibited from

- Unauthorised data execution
- Access to source programs
- Performing other function apart from run-to-run controls

Library controls

Library controls refer to a set of measures that protect the data files and programs against unauthorised access. Operators can access data and program files of the object version but are prohibited from accessing programme documentation, test and production source version. In the absence of precise instructions about restrictions, operators can manipulate the programmes. Library software packages like Librarian, Secure, Panvalet, Racf, Panexec, enables the management to prohibit such actions. The time and date of access is recorded and reported.

The following measures should be taken to control the library access:

- Assign responsibilities
 - i. To maintain production library
 - ii. To ensure different versions are not kept in source and object library
 - iii. Remove or clean obsolete version
 - iv. To carry out changes to production libraries
- Operators should not be allowed to access the magnetic media unless it is essential to process the application.
- During production runs, operators should not be permitted to execute the programmes in test libraries.

Control over data file media

Operations management has to exercise proper control over data file media, which is very essential for enterprise. It should ensure the existence of proper physical conditions like temperature and humidity levels, off-site backup and security measures. Physical security measures are sufficient protection against natural disasters. Authorised persons are to be allowed to access the library where tapes and disks are stored. A record of unauthorised access during emergencies and in the absence of librarian has to be maintained and reviewed regularly.

File protect ring could be an effective method to protect the data contained in magnetic tapes. This prohibits overwriting. File protect feature, a software control can serve as an effective control to protect disk files.

Housekeeping

Operations staff is responsible for maintaining a clean working environment. They should take necessary

steps for disposing waste material and trash. The stock of stationery and cleaning material should be maintained in limited quantities.

Emergency procedures

Management should circulate in advance, the instructions for handling emergencies throughout the enterprise. The instructions must contain the precautions for protecting personnel and property. The measures include operating fire extinguishing systems, saving data and switching off systems, protecting expensive assets and personnel evacuation.

Answer: [a] Library controls

Module:2

Reference No:M2046

Question: A key clause in any outsourcing contract is

- [a] Data protection
- [b] Expected improvement in performance
- [c] Deciding on the process to be outsourced
- [d] To understand the reasons for outsourcing

Module 2 – Audit of "Outsourcing"

Introduction

The process of entrusting the functions of an Information Systems department to a third party on a contractual basis is referred to as outsourcing. Outsourcing brings many advantages to the organisation like reduction of in-house operations and sharing the expertise of the third party. When a third party is engaged to perform the internal functions, it results in assets and information sharing. Hence the contract agreement forms a basis to evaluate the outsourced operation. In order to ensure the success of an outsourcing venture, contract clauses have to be examined before the commencement of the deal.

Any structural deficiencies in the outsourcing contract may severely affect the competitive advantage of an organisation. Therefore, auditor should involve himself in the pre-outsourcing discussion rather than reviewing the document later. The discussion includes:

1. Deciding on the processes to be outsourced
2. Evaluations of alternatives
3. Understanding the reasons for outsourcing
4. Discussion on key aspects and components of the project
5. Determining the clauses included in the contract
6. Issues regarding agreement cancellation
7. Expected improvements in performance

Audit objectives

An auditor has to ensure that the third party services are managed properly with clearly defined roles and responsibilities. This is possible by evaluating the control measures over existing contracts and its compliance with the overall organisational policy. Key factors in any outsourcing are

- Data protection
- Asset protection

- Service level agreement
- Cost/benefits

Auditor should ensure that the management has detailed policy on data integrity, availability and confidentiality as per its needs. He must also ensure that the terms mentioned in the contract support this. Similarly the measures to be taken for asset protection must be clearly defined and included in the contract.

Audit Program: The following are the steps involved in the audit program

Examine previous audit report: Auditor should examine the previous years audit report and check whether the recommendations were considered and corrections made wherever needed. If any deficiencies still exist, auditor should make a note of it.

Preliminary audit process: Auditor should examine the outsourcing policies and contract requirements. He can select a few third party contracts and review for compliance with policies. Auditor should evaluate the organisations procedures for purchased services and third party vendor relationships.

Detailed audit process:

Management and planning: The clauses in the agreement are to be properly evaluated and transition plans have to be examined to ensure completeness. Auditor should ensure that the need for outsourcing, organisational and vendor constraints are evaluated before outsourcing. Evaluate the methodology adopted for risk assessment and vendor selection. The technical procedures, cost and payment processes are to be evaluated thoroughly. To ensure compliance with the project management standards, project plans have to be reviewed.

Security: Auditor should ensure the adequacy of contingency plans and back-up procedures of the outsourcer. The termination process and access controls for the outsiders are to be reviewed. The control processes in usage, to access the operating system, application system, networks and remote areas have to be evaluated. Check the controls over physical security, access, administration and maintenance at outsourcer's place.

Administrative: Ensure the accuracy of billing, payment and disbursement system. Monitor third party's performance by evaluating the internal procedures.

Answer: [a] Data protection

Module:2

Reference No:M2047

Question: Which of the following need not be included in the outsourcing contract?

- [a] Terms of the contract
- [b] Procedure for reporting
- [c] R&D expenditure of vendors
- [d] Types of services to be provided

Module 2 - Internal control - Outsourcing

Auditor should evaluate the outsourcing project thoroughly in the light of its importance to the organisation. The following internal control questionnaire enables the auditor to judge the efficiency of an outsourcing programme:

Management and planning:

- Auditor should ask whether the contract clearly specifies the requirements and expectations of management. It should define clearly the responsibilities of the user and the vendor.
- Ensure the existence of policies pertaining to third party relationships.
- Enquire management about the benefits in support of outsourcing decision including the competitive advantages.
- Auditor should enquire whether proper approval process exist for vendor selection and contract review.
- Evaluate the impact of proposed contract on the existing contracts with labour, business partners and the like.
- Check whether the supplier is capable of supporting multiple (whenever needed) locations for the outsourced function.
- Outsourcing project plans should include contingency and training plans.
- It should also contain hardware and software requirements, procedures for handling errors and legal issues.
- Determine whether the outsourcer is providing warranties and whether the customer service levels are defined.
- The maintenance and technical requirements and responsibilities have to be specifically stated.

Auditor must ensure that the vendors are evaluated in the following areas:

1. R&D expenditure
2. Ability to follow the organisations needs
3. Flexibility
4. Experience in the relevant area
5. Expertise in the technological field
6. Problem handling capacity
7. Level of performance

The following details should comprise the outsourcing contract:

- Details of service providing entity
- Type of services provided
- Qualitative and quantitative service levels
- Cost and payment procedures for services
- Provisions for non-performance penalties
- Contract modification and cancellation process
- Procedure for reporting
- Principal roles and responsibilities
- Business continuity process
- Communication procedure between organisation and outsourcer and its frequency
- Term of the contract
- Vendors are supplied with predefined access levels
- Security conditions
- Access rights and audit rights

Auditor should ensure that the following are contained in the service level agreement:

1. Service definition

2. Service cost
3. Quantitative service level
4. Growth prospects
5. Provision for contingency planning
6. Requirements for security
7. Methodology in event of changes to the agreement
8. Time limit for renewal
9. Cost and payment procedures
10. Industry and best practice based realistic changes
11. Calculation for charges
12. Committed improvements in services

Security:

Auditor should enquire, whether the contract contains clear specifications for security requirements. Access elimination practices must be present to deny the access in case of occurrence of terminations and transfers. An outsourcer should possess adequate back-up procedures and logical access control for emergencies. Adequate physical access controls must exist with the third parties. The transfer of technology resources to contractors must be properly recorded in the inventory records.

Administrative:

Auditor should ask for the validity of the billings and payables. He should also ensure that vendor performance and options for technology purchases are examined.

Answer: [c] R&D expenditure of vendors

Module:2

Reference No:M2048

Question: The system administrator has to work closely with the information security officer to:

- [a] Ensure the security of system usage
- [b] Draft the incident reporting programme
- [c] Maintain control systems that have been configured
- [d] All the above

Module 2 - Functions of System Administrator

The System Administrator is responsible for a variety of duties. He needs to work in close conjunction with the Information Systems Security Officer to ensure security of system usage, drafting of the incident reporting programme and maintaining control systems that are already configured. He advises security officers about the loopholes in integrity and manages user identification when ever necessary.

The system administrator is required to perform the following functions under different areas.

1. **General:** The general functions of a system administrator include developing policies and procedures, creating awareness and training staff. Policies include LAN, WAN, Internet and information security, local e-mail privacy, ethical and accountability policies, accreditation, and multilevel security, assurance and certification policies for local requirements.

The *procedures* include, FAX usage, housekeeping, information states, the Internet, and network and operating systems related procedures to maintain security.

In addition, a system administrator is required to provide adequate awareness about security through *training and education*. He should clearly differentiate between training, education and awareness.

Risk management functions of a system administrator include recognising the types of threats that exist and developing security measures for protection for the Internet and WAN. The System administrator should explain operating system integrity and basis for zone or control ratings.

2. **Access control:** The system administrator should implement policies related to *access controls*, data access, methods of operation, ownership and custodian rights of information, etc. he should use appropriate network firewalls and security software for access control. He should also train users in such software and tools. He must develop appropriate intrusion detection and counter measures for instances of violation of internal controls and.

He should describe authentication mechanisms; discretionary and mandatory access controls, one-time passwords, and single sign-on mechanisms to ensure proper access control.

3. **Administrative:** Under administrative functions, the System administrator is required to explain the *policies and procedures* pertaining to management issues, change control, object reuse, etc. He should review the operational procedure for policy enforcement, and conduct security inspections. The *administrative safeguard functions* include describing and implementing application development control, disposing information, media and data, document labelling, appropriate usage of security safeguards and system software controls.
4. **Audit:** The system administrator is required to frame the documentation required for auditing. He should ensure the compliance of electronic records management with the policies and procedures. The mandatory areas for separation of duties must be stated. He should also establish some countermeasures and safeguards related to audit trials. Necessary audit tools need to be identified.
5. **Operations:** His operating functions comprise explaining and implementing the operating *policies and procedures* regarding documentation, separation of duties, disposition of media and data. He is also responsible for explaining change controls, configuration management, database integrity, electronic record management, information management and risk management. He should also recognise the important factors of information integrity.
6. **Contingency:** Contingency functions of the System administer include explaining about backups, continuity planning, disaster recover plan and testing. He has to identify, select and implement the corrective actions, countermeasures, safeguards and intrusion detection methods to *protect* information systems against disaster.

Answer: [d] All the above

Module:2

Reference No:M2049

Question: Which of the following IT resources is mainly relevant to ensure compliance with and effective communication of policies and strategies?

- [a] Human factor
- [b] Data
- [c] Technology
- [d] Support

Module 2 – Control objectives for planning block

Policies and strategies - Communication and management

Introduction

The policies can be effectively implemented only when they are communicated to the required personnel in the organisation. Various alternatives are available for the implementation of the policies. A standard procedure should be established based on the alternative selected for the effective implementation of the policies.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To communicate the management policies and strategies.	To ensure compliance with the policies and strategies and their effective implementation	1. Clearly defined aims 2. Technological guidance 3. Quality assurance 4. Security 5. Internal controls 6. Compliance 7. Ethical standards 8. Assistance 9. Interactive programs	• Human factor

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities, the conduct of which is the responsibility of the management. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **Management involvement:** Policies should be framed, documented and communicated. The management assumes full responsibility for this task.
- **Communication:** The management must ensure that the policy is communicated to the required personnel. It should also be ensured that the personnel are in agreement with the policy.
- **Adherence:** The policies should have an inbuilt mechanism to ensure that the personnel in the organisation are adhering to the set policies. A conducive atmosphere should be created where the personnel are free to discuss any issues relating to the policy, their implementation, the affect on their working style and the like. This ensures that the personnel adhere to ethical standards and are disciplined.
- **Allocation of resources:** The appropriate resources should be allocated for the implementation of the policies. The allocation should be on a timely basis for effective implementation of the policies.

- **Quality assurance:** Policies should adhere to the overall quality levels set by the management. The same quality level should be maintained in all the IT functions.
- **Evaluation and updation:** The policy should be evaluated regularly to take into consideration the changes in the IT functions and environment. A process should be defined for their regular evaluation and updation.
- **Security:** Policy should provide guideline for the security of IT functions. The policy should provide for
 1. Identification of risks
 2. Steps to be taken to mitigate the risks and minimising the losses
 The security level should be based on the organisation structure and the IT functions.
- **Internal Control:** The management should define the internal controls for the protection of IT resources. Framework for internal control should be based on the overall objectives of the business and security levels. It should define the roles and responsibilities for their implementation and the actions that will be taken if the controls are not implemented.
- **Ownership:** The ownership rights of the software that are developed in-house or purchased should be stated.
- **Detailed policies:** The general policy can be broken up into specific and detailed policy for each IT function.

II. Operational Controls

Not applicable for this activity.

Answer: [a] Human factor

Module:2

Reference No:M2050

Question: Which of the following statement is "FALSE" with regard to control objective related to human factor?

- [a] Training programme should be organised on regular basis for the personnel
- [b] Orientation need to be given to all the personnel
- [c] Termination procedure should be defined by the management
- [d] Personnel holding sensitive positions should be subject to security clearance

Module 2 – Control objectives for planning block

Manage the human factor

Introduction

An organisation should have a human policy for employing, training, promoting and terminating its work force. It is only through its work force that the management is able to utilise its other IT resources effectively.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources

To ensure that the organisation employs personnel who are competent.	To ensure effective and efficient management of human factor.	1. Recruitment 2. Promotion 3. Training 4. Cross training 5. Job rotation 6. Job recruitment and termination procedure 7. Job performance evaluation	• Human factor

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities, whose conduct is the responsibility of the management. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **Defining roles and responsibilities for each IT position:** The roles and responsibilities for each IT function should be specified by the management. The personnel to be hired by the organisation should be evaluated based on such defined roles and responsibilities.
- **Required qualification for each position:** The qualification required for each IT position should be defined. The personnel who are recruited should possess the required education, membership in professional bodies, experience and the like.
- **Recruitment and promotion:** The organisation should have efficient personnel to help it achieve its objectives. For this purpose the management should define a clear policy for recruitment and promotion which should include a guideline on the following
 - o Recruitment
 - o Orientation
 - o Training
 - o Promotion
 The policy should also provide for regular assessment of the roles and responsibilities required for each position.
- **Security clearance:** Every employee should be subject to security clearance when they are appointed or promoted to positions that are considered as sensitive. This ensures that the sensitive information of the organisation is protected by its human factor and there is no scope of it being transferred to outsiders.
- **Orientation:** The hired employees should undergo an orientation programme to familiarise them with the work environment in the organisation.
- **Training and cross training:** A training programme should be organised on regular basis for the personnel to upgrade their knowledge, skills and abilities. This ensures that the personnel are on par with the latest developments in their related field. The organisation can also sponsor them to attend seminars and conferences being organised by external agencies. For the key IT positions a success plan should be designed by cross training. This ensures smooth functioning of the organisation even after the key personnel leaves the organisation.

- **Job performance evaluation:** The performance of every employee should be evaluated on a regular basis against the set standards. There should be a suitable reward system.
- **Job rotations and terminations:** Management should establish a procedure for appropriate termination activities to be performed for each job rotation and termination. This is to ensure that internal control framework and security of the information assets is not affected.

II. Operational Controls

Not applicable for this activity.

Answer: [b] Orientation need to be given to all the personnel

Module:2

Reference No:M2051

Question: Segregation of duties should be maintained between which of the following functions?

- [a] Security administration and security audit
- [b] System administration and network administration
- [c] Systems development and maintenance
- [d] All of the above

Module 2 – Control objectives for planning block

Building the IT organisation structure

Introduction

A well-structured organisation is critical to better management of the IT function. A comprehensive organisation with well defined roles and responsibilities, appropriate mix of skills and numbers, facilitates the realisation of the management's objectives and also realisation of the IT strategies and goals.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
Providing right IT services to the business	To ensure effectiveness and efficiency in the performance of the IT function.	1. Position of IT services in the overall business functioning 2. Management's involvement in the IT function 3. Roles and responsibilities 4. Segregation of duties 5. Security levels, quality framework and internal	• Human factor

		control framework	

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **IT steering committee:** The management should form a steering committee for the overall supervision of the IT function. All the parties involved in IT functioning should represent it, viz., the user community, the senior management and the IT function representatives. The committee should report to the senior management.
- **Position of IT in the organisation:** The management should arm the IT wing with adequate authority and independence, and for the user department to carry out its functions effectively. All personnel in the organisation should be made aware of their roles and responsibilities with regard to the IT function.
- **Clearly defined roles and responsibilities:** All personnel involved in the IT function should have clearly defined roles and responsibilities. Job descriptions must follow the principles of segregation of duties, internal controls and security framework. These job descriptions should be reviewed periodically and updated or modified depending upon the organisational situations.
- **Security, quality and internal control framework:** The IT organisational structure should have appropriate skills and resources for performance of the quality assurance function and the management of security. The quality assurance functions should satisfy the basic requirements of the organisation. At an overall level, a security manager may be responsible for the security issues of the entire organisation. If required, system specific security responsibility can also be assigned.
- **Supervisory roles:** Management should define adequate supervisory roles to ensure the proper functioning of duties, to assess the adequacy of authority and responsibilities given to each staff member of the IT function.
- **Segregation of duties:** It should be ensured that the principles of segregation of duties are taken into consideration and is being maintained in the performance of duties. In particular, segregation should be maintained between the functions of network and system administration, systems development & maintenance, security management, audit, change management, and information system use.
- **Physical and logical ownership:** A framework should be established for assigning ownership of the data and system ownership. It should appoint owners for all data and system assets. The data owners should be ideally made responsible for the data classification schemes and managing the security and access rights for each classification made. It is the responsibility of the security administrator for maintenance of system security.
- **Contracted personnel:** Policies and procedures should be established to control the activities of temporary IT personnel including those on contract.

- **Co-ordination:** Procedures should be established to maintain a cordial and mutually beneficial relationship with in the IT organisation and outside. For instance the risk managers, security managers and the like.
- **Evaluation and review:** The IT staffing structure should carry out periodic reviews for any changes that has either occurred in the overall business environment or in the IT organisation.

II. Operational Controls

Not applicable for this activity.

Answer: [d] All of the above

Module:2

Reference No:M2052

Question: Under which category of Database Administrator tasks does ensuring the integrity of the databases fall?

- [a] Management tasks
- [b] Security tasks
- [c] Day-to-day tasks
- [d] Planning tasks

Module 2 – Functions of Database Administrator

A Database Administrator takes care of data resource management and shared database integrity. Functions of a Database Administrator:

- Assuring the optimum utilisation of database
- Developing standards and guidelines to ensure the above functions
- Describing data structures and maintaining them in the corporate database system
- Understanding data requirements and data relationship
- Designing, defining, and maintaining the corporate database
- Assuring database security
- Maintaining the database in the effective working condition

A Database administrator's management, security, day-to-day tasks and planning are as follows:

I. Management tasks: A database administrator has to work in coordination with the management and provide timely advice to users. He has to supervise the key management and the maintenance of data dictionary to provide uninterrupted sharing of data. He has also to properly acquire and maintain the database software and other documents and tools. It is crucial that he maintain proper relations with the database software vendor and database content vendor.

II. Security tasks: An important function of the database administrator is to examine and maintain the database security. He is responsible for allowing and cancelling the database access rights. Hence, he should also preserve database software licenses and content licenses

III. Day-to-day tasks: The day-to-day functions of a database administrator include: -

- Configuring databases
- Utilising the database resources optimally

- Maximising the database performance by evaluating the performance and taking follow-up actions.
- Initiating and sping as well as creating and deleting databases
- Maintaining database integrity
- Describing and monitoring the security and back-up policies
- Defining maintenance policies for databases and supervising the maintenance staff
- Recognising problems that arise in the databases and taking necessary steps to solve them
- Maintaining documentation relating to standards, procedures, guidelines, changes and the like
- Managing and executing the data migration procedures
- Estimating the potential requirements of disk, CPU, and RAM resources based on the prospective growth of the storage data
- Facilitating - developers in the design of database, system programmers and network managers to install the database, and application programmers to adjust the database related programmes.

IV. Planning tasks: A Database administrator has to plan for the database capacity, security and integrity. The processing, storage and back-up capacity have to be determined. He has to work with security experts, network managers and systems programmers for planning database security and integrity. The database administrator has to liaison with development teams for assigning and building data models.

Additional responsibilities

The database administrator many also be made responsible for additional functions based on his knowledge and experience and organisational requirements. These include controlling programmes and quality of data, data maintenance, assisting users, purchasing hardware and software and installing them.

Knowledge

To conduct his functions effectively a database administrator should have proper knowledge of databases. He should also have a clear understanding of the operating systems, tools and scripting languages, middleware, reporting tools and back-up systems. Moreover, he should maintain contacts with system analysts, developers, users, system administrators, network administrators, hardware and software vendors, IT service companies and other Database administrators. This enables him to undertake his responsibilities efficiently

Answer: [c] Day-to-day tasks

Module:2

Reference No:M2053

Question: _____ represents the minimum level of security that is required in the organisation.

- [a] Standards
- [b] Baselines
- [c] Guidelines
- [d] Procedures

Module 2 – Policies, Procedures, Guidelines and Standards

management should develop a comprehensive approach vis-à-vis the company's mission and objectives for protecting the systems, networks and information. A security program, which states the security policies, procedures, standards, guidelines, baselines training, incident handling and compliance program need to be developed.

Security policies: management prepares a statement spelling out the role of the security in the organisation. It is referred to as a Security Policy. It is of different types.

Organisational security policy: Under this policy, the program goals, responsibilities and the security program are established. It should consider all the legal regulation at the drafting stage. It acts as guidance for future security activities. The acceptable degree of risk is specified in this policy.

Issue specific policies: Detailed explanation of a particular issue is given under these policies. Employees must be made clear about the security issues specified in these kinds of policies. It provides clear indications to the staff on the restricted and permissible areas.

System specific policies: System specific policy contains instructions regarding software application list and the procedure for database protection, locking procedure for computers, and installation of firewall, intrusion detection systems and scanners.

Types of policies

Regulatory: This lays down the requirements specified by the regulatory bodies. These are specific to the type and nature of the industry in which the company is doing business.

Advisory: Advisory policies are suggestions to the employees regarding the behaviour and activities that should be followed in the organisation. These include handling financial information, processing confidential information and the like.

Informative: Informative policy provides general information about the specific issues like goals, mission, reporting structure and the like to the employees of an organisation.

Standards: Security standards provide a standard method for usage of hardware and software. It ensures the application of uniform methods throughout the organisation. The standards are obligatory rules for the staff in the company. Security policy in total is referred to as a strategic goal, which is the ultimate end point. On the other hand, standards, guidelines and procedures are referred to as tactical goals, which are the essential steps to achieve strategic goal.

Baselines: Baseline represents the minimum level of security that is required in the organisation. They must be developed prior to the development of system architecture. Baselines provides basis for the development of standards.

Guidelines: Guidelines are the general instructions to the IT and operating staff, which provide further reference to the standards and policies. In case of non-applicability of standards,

Procedures: A detailed set of actions for installation and configuration are referred to as procedures. The steps to implement policies, standards and guidelines are provided in the procedures. For example, if a policy states that authentication is required to access confidential information, procedures define the access criteria, implementation of access control mechanisms and audit of access activities.

Implementation: Implementation of security policies, standards, procedures, baselines, and guidelines is possible only when they are informed to the personnel and provide the necessary training. Employees must be made clear about the actions, behaviour and performance required for implementation.

Answer: [b] Baselines

Question: The overall control objective of training it to ensure that

- [a] Personnel are educated and trained
- [b] Personnel are using the available technology effectively
- [c] Training is provided by the vendors
- [d] Training is as per the needs of the personnel

Module 2 – Control objectives for implementation block

Training

Introduction

Training is vital for users, for effective implementation of technology. Training makes the employees aware of their roles and responsibilities and the risks that the organisation would face due to lapses in performance.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To ensure that the effect of the change management is minimal or nil.	To ensure effective and efficient Information System through proper training of the personnel.	1. Training syllabus and content 2. Inventory of the expertise of the personnel 3. Training methods 4. Training techniques 5. Knowledge base development 6. Development of personnel	• Human factor

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **Identification of needs:** The management should define and maintain the procedure for identification of the training needs of the personnel. The training needs should be defined based on the overall recommendation of the IT managers.
- **Training syllabus and contents:** The training syllabus and contents should be defined and approved by the IT managers. The training syllabus and contents should include the security aspects, incident handling, ethical practices and the like.
- **Organising training:** This would include identification of the personnel to be trained, deciding the trainees, preparing the training material and making all other arrangements. The trainees may be either from the organisation or a third party.
- **Imparting training:** The training should be provided on a regular basis. It should also be ensured that the personnel are satisfied with the training imparted. The training can also be extended to areas that are of interest to the personnel, provided the same is approved by the IT managers and is within the scope of the overall objective of the company.
- **Security knowledge:** The knowledge of the security procedures is essential as it helps in ensuring that the personnel are aware of their responsibility with regard to availability, integrity and confidentiality of the information system.

II. Operational Controls

Not applicable for this activity.

Answer: [b] Personnel are using the available technology effectively

Module:2

Reference No:M2055

Question: Which of the following legal and contractual clauses is not obligatory for an organisation?

- [a] Trading partner agreements entered by the organisation
- [b] Insurance contracts entered into by the organisation
- [c] Government regulations applicable to the organisation
- [d] Agreements entered into by its employees for their benefit

Module 2 - Control objectives for planning block

Legal and contractual framework

Introduction

As with every organisational function, the IT functions must also comply with the legal statutes that are applicable to those functions. The management must identify, analyse and comply with the applicable statutes.

Table of Applicability

Overall objective	Why	How

		Operations/documentation	Resources
To abide by legal statutes and meet contractual requirements.	To ensure effective compliance with the legal and contractual requirements.	1. Legal statutes 2. Review of the recent developments 3. Observance with statutes and contracts 4. Compliance with safety design 5. Privacy	• Data • Technology • Human factor

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **Legal and contractual requirements:** A procedure for the identification of the legal statutes, government regulations and other third party agreements that are applicable to the IT functions of organisation should be defined. The procedure must provide for regular review of the applicable statutes, regulation and the agreements. It must also provide for making corresponding changes that may be required in the IT functions including change in the other IT policies and the like.
- **Compliance with legal and contractual requirements:** It is the management's responsibility to ensure compliance with legal and contractual agreements. The procedures should ensure that the IT functions continuously comply with them. Where required, a legal opinion must be taken.
- **Compliance with safety design:** Legal statutes may provide for the safety, environment and health measures that the organisation should provide. The management should ensure that they are complied with.
- **Intellectual property rights:** It should also be ensured that the IT functions and practices comply with the privacy and intellectual rights. Where laws relating to data transmission and cryptography are applicable compliance should be ensured.
- **E-commerce:** In electronic trading, the organisation must ensure adherence to international laws. Similarly in case of EDI transactions, the organisation should abide by trading partner agreements and the procedure defined for exchanging information and transactions in the standard form.

II. Operational Controls

Not applicable for this activity.

Answer: [d] Agreements entered into by its employees for their benefit

Module:2

Question: Policies and procedures with regard to data and system ownership should contain

- [a] Identification of ownership for data and systems
- [b] Approval of owners to access the data
- [c] Approval of owners to all changes made to the system
- [d] All of the above

Module 2- Audit working guideline

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Building the IT organisation structure	1. IT steering committee 2. Position of IT in the organisation 3. Clearly defined roles and responsibilities 4. Security, quality and internal control framework 5. Supervisory roles 6. Segregation of duties 7. Physical and logical ownership 8. Contracted personnel 9. Co-ordination 10. Evaluation and review	Not applicable for this activity

Audit Process

The audit process has been covered in a two part series. The first part covers the preliminary understanding and preliminary analysis . This article focuses on the second part-the test of controls and substantive testing.

Tests of controls

A clear picture of the functioning of the controls can be gained by

- Obtaining evidences
- Reviewing the deliverables

Tests: The following tests have to be done, before an opinion is formed on the functioning of IT tasks in the organisation.

1. The efficiency of the IT steering committee
2. The effectiveness of the reporting hierarchy of the IT function
3. The appropriateness of the position of the IT function in the organisation.
4. The usage of key indicators in performance assessment
5. The undertaking of variance analysis and implementation of corrective measures

6. The involvement of management in case of significant deviations
7. The assessment of IT functions by users and owners
8. The testing and sign-off of quality assurance for all projects
9. The completion of security reviews for all systems
10. The clear definition of ownership for all data and systems (information assets)
11. The verification that authority is commensurate with responsibility
12. The detailing of job descriptions.
13. The linking of IT jobs and responsibilities with the organisation chart
14. The compliance with segregation of duties principles
15. The review of the contract agreement to ensure clauses for security and internal issues.

Substantive testing

This step is undertaken so as to substantiate the auditor's view of controls objectives either not being met or not existing. The control weaknesses observed and its impact will have to be documented. In order to further substantiate the viewpoint

1. Comparative benchmarks from similar organisation, industries can be identified.
2. A review can be undertaken of
 - The impact of ineffective planning
 - Organisation structure, roles and responsibilities and data and system ownership
 - The Quality function
 - The Security function
 - The Sample of contracts

Identification of shortfalls

The auditor should identify:

- Weaknesses of the IT function
- Organisational gaps, overlaps and the like
- Improper roles and responsibilities, missing links, lack of segregation in duties, supervisory inefficiencies, confusion and the like
- Failure to meet quality assurance standards
- Failure to meet security standards
- Contracts that do not meet organisational policies
- Lack of co-ordination and communication in the organisation

Answer: [d] All of the above

Module:2

Reference No:M2057

Question: With regard to the implementation of new IT solutions, the system development function is independent of

- [a] Quality assurance function
- [b] Maintenance
- [c] Operations
- [d] All of the above

Module 2- Audit working guideline
Building the IT organisation structure-2

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Building the IT organisation structure	1. IT steering committee 2. Position of IT in the organisation 3. Clearly defined roles and responsibilities 4. Security, quality and internal control framework 5. Supervisory roles 6. Segregation of duties 7. Physical and logical ownership 8. Contracted personnel 9. Co-ordination 10. Evaluation and review	Not applicable for this activity

Audit Process

The audit process has been covered in a two part series. The first part covers the preliminary understanding and preliminary analysis . This article focuses on the second part-the test of controls and substantive testing.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Documents
1. CEO 2. COO 3. CFO 4. CIO 5. Quality assurance department representative 6. Security management representative 7. Steering committee members 8. Human resource department representative	1. Planning & steering committee roles and responsibilities 2. Business objectives 3. IT objectives 4. Long term and short term plans 5. IT organisation policies and procedures 6. Quality assurance policies and procedures 7. Human resource policies and procedures 8. Organisation structure of IT function 9. Roles and responsibilities of IT function 10. Job responsibilities of key personnel 11. Minutes and reports of IT steering committee meeting

Preliminary analysis

The next step is analyse the effectiveness of the control measures adopted and the degree of reliability that can be placed on the control measures. This can be done by ensuring the existence of policies and procedures on the following issues.

1. Responsibility and provision of related authority for the IT function
2. Functions and responsibilities of the IT steering committee/planning committee
3. Management issues
4. Restructuring to meet changing business objectives
5. Performance indicators to ensure efficiency in IT functions
6. Roles and responsibilities of the staff in the organisation with regard to the IT function, security and internal control
7. Quality assurance function
8. Independence of quality assurance function
9. Security of data and responsibilities of the security officer
10. Data and system ownership
11. Supervisory role and responsibilities
12. Segregation of duties
13. Evaluation and review of IT job responsibilities
14. Maintenance of job competency
15. Control of other personnel in IT function
16. Co-ordination, communication and documentation

The auditor should also ensure segregation of duties exist between the functions of

- System development and
 1. Maintenance
 2. Operations
 3. Security
- Operations and
 1. Data control /operators.
 2. Users
 3. Security

Answer: [d] All of the above

Module:2

Reference No:M2058

Question: The role of database administrator is incompatible with which of the following role?

- [a] Control group
- [b] System analyst

- [c] Security administrator
- [d] Application programmer

Module 2- Segregation of duties - Diagram

The role of staff in an IT department of a company depends on its size and structure. A single individual cannot perform all the functions. Few functions are considered compatible and hence can be performed by a single individual. The others which are non-compatible cannot be performed by the same individuals. Where such segregation is not possible, compensating controls should exist to mitigate the risk that results from the lack of such segregation. The diagram given below shows the roles that are compatible

AP	Application Programmer
Sys Anl.	Systems Analyst
TL	Tape Librarian
DBA	Database Administrator
QA	Quality Assurance
Sec Adm	Security Administrator
DE	Data Entry
Sys Pro	System Programmer
Cop	Computer Operator
CGr	Control Group

Compatibility

1. AP - Sys Anl
2. Sys Pro - QA
3. Cop - TL, QA
4. Sys Anl - DBA, DE, AP
5. DE - QA, TL, Sys Anl
6. Sec Adm - DBA, QA, CG
7. CGr - TL, DBA, QA, Sec Adm
8. DBA - TL, Sys Anl, QA, Sec Adm, CG
9. TL - DBA, QA, Cop, DE, CGr
10. QA - all except AP, Sys Anl

Let us first understand briefly the duties and responsibilities for each work group.

Control group: To collect, convert the input and distribute the output to the users.

System analyst: Development of the system as per the needs of the users.

Application programmer: Development and maintenance of the programs in the production environment.

Data entry: To key in the data generated by the organisation to produce information. However, data entry operators are usually not found in many organisations as the concerned individual at his desk does the data entry work.

Computer operator: Responsible for the operation of hardware and for ensuring that the systems are working efficiently.

Database administrator: To classify and maintain the database including its security.

System administrator: Responsible for implementing the security policy of the organisation and ensuring that the company's assets are protected and accessed only by authorised users.

Tape librarian: To maintain the record of the programs and data files.

System programmer: To maintain the system software.

Quality assurance: Assuring that quality standards are being adhered to and implemented by the personnel in the organisation.

Example:

We shall now discuss why the database administrator can perform some roles and why not the others.

As per the diagram the database administrator role is compatible with

- **Control group:** If the DBA role is combined with control group there is no risk as the DBA has access to the data. In fact combining them both will lead to better control.
- **System analyst:** System analyst task is designing the system during the initial stages of the system development life cycle. Designing of the system does not conflict with the role of maintaining data. They are not connected even remotely.
- **Security administrator:** Security administrator is responsible for implementing the defined access rule to data. The same function can be performed by DBA, as it is an extension of his role viz. defining the database.
- **Tape librarian:** DBA has access to the data and other information. The custody of the data stored in the tapes and disks will not give him any additional rights.
- **Quality assurance:** Performing the role of quality assurance will be an additional role that in no way conflicts with the role of DBA.

His role is not compatible with

- **Application programmer:** The application programmers cannot access application programs in production environment. They can access programs only in the testing environment. This ensures that they cannot alter the data. If the DBA were allowed access to both data and application program it would conflict.
- **Data entry:** If the DBA is allowed to perform the data entry job, then there will be no control over the alterations made to the data as he can easily alter the data without any compensating controls existing to detect the alterations made.
- **Computer operator:** DBA cannot perform this role, as the DBA would get rights to make alteration to the hardware. With the right to make alterations to hardware as well as to the data there would be no proper compensating control to detect the changes made by him. He can easily make alterations that suit him.
- **System programmer:** The system programmer has access to the system software including the operating system. If the DBA performs both roles then he will have access to the system as well as

the database. He can easily make any alterations and the same will also not be detected. No compensating controls can mitigate this risk.

Answer: [d] Application programmer

Module:2

Reference No:M2059

Question: The audit working guideline for legal and contractual framework need not have to focus on compliance with which of the following?

- [a] Insurance contracts
- [b] E-commerce laws
- [c] Health and safety measures
- [d] None of the above

Module 2- Audit working guideline

Legal and contractual framework

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Legal and contractual framework	1. Legal and contractual requirements 2. Compliance with legal and contractual requirements 3. Compliance with safety design 4. Intellectual property rights 5. E-commerce	Not applicable for this activity

Audit Process

The Audit process has been covered in two parts. In the first part, the preliminary understanding and analysis have been covered. In the second part, the test of controls and substantive testing have been dealt with. This article is first in the two-part series.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. Legal advisor 2. Human resource department	1. Laws and regulations applicable to the organisation in general 2. Rules and regulations related to

representative 3. IT management	- o Health and safety measures - o Privacy - o Security - o Cryptography and the like 3. Accounting standards - national and international; and taxation rule: applicable to e-Commerce transactions 4. Trading partner agreements 5. Agreements with the EDI vendor 6. Insurance contracts related to IT functions 7. Legal advisor's suggestions and opinions on the insurance contract 8. Policies and procedures of the organisation related to compliance with - o Laws and regulations applicable to the organisation - o Safety and health measures - o Privacy - o Security - o E-commerce - o Insurance 9. Audit reports of external auditors, if any 10. Audit report from service providers

Preliminary analysis

The next step is analyse the effectiveness of the control measures adopted and the degree of reliability that can be placed on the control measures. This can be done through

- Policies and procedures exist for
 1. Compliance with laws and regulations, and the related corrective action to be taken in case of a breach. This is to ensure that the compliance on a continued basis
 2. Implementation of the health and safety measures
 3. Awareness of the employees about health and safety measures
 4. Compliance with privacy issues
 5. Communicating to insurers about the material changes made to the IT environment and making corresponding alterations to the contract
 6. Compliance with insurance contracts
- Security procedures are framed in accordance with the applicable laws. It should be ensured that the security procedures are in place for
 1. Protection of passwords
 2. Authorisation of the personnel
 3. Terminals
 4. Encryption of data
 5. Firewalls
 6. Protection against virus
- Procedures exist for immediate action to be taken when violations are reported.

Answer: [d] None of the above

Module:2

Reference No:M2060

Question: The auditor need not ensure the existence of which of the following management controls while auditing compliance with legal and contractual requirements?

- [a] Safety design
- [b] Intellectual property rights
- [c] E-commerce
- [d] Classification of data

Module 2- Audit working guideline

Legal and contractual framework Part 2

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Legal and contractual framework	1. Legal and contractual requirements 2. Compliance with legal and contractual requirements 3. Compliance with safety design 4. Intellectual property rights 5. E-commerce	Not applicable for this activity

Audit Process

The Audit process has been covered in two parts. In the first part, the preliminary understanding and analysis have been covered. In the second part, the test of controls and substantive testing have been dealt with. This article is second in the two-part series.

Tests of controls

A clear picture of the functioning of the controls can be gained by

- Obtaining evidences
- Reviewing the deliverables

Tests: The following tests have to be done, before an opinion is formed on the functioning of IT tasks in the organisation.

- Procedures for compliance with laws and regulations are current and are reviewed at periodical intervals
- Corrective action is taken in case of deviations
- Implementation of the health and safety measures

- Compliance of the IT functions with privacy and security policies
- Any violation of the laws when data is transmitted outside the country
- Trading partner agreements and insurance contracts are framed after considering the organisation's policies and procedures
- Encryption keys conform to the defined regulations
- Sensitive information is encrypted as per the defined regulations and organisation procedures
- Organisation policies and procedures are complied with in case of DI transactions
- Compliance with the trading partner agreements and the EDI vendor contract if any

Tests should be performed to ensure that the identified control measures in the preliminary analysis section are functioning as desired.

Substantive testing

This step is undertaken so as to substantiate the auditor's view of controls objectives either not being met or not existing. The control weaknesses observed and its impact will have to be documented. In order to further substantiate the viewpoint

1. Comparative benchmarks from similar organisation and industries can be identified.
2. Review of the external requirements file in order to ensure that there has been compliance with the laws and regulations and corrective action has been taken where required
3. Review of the security reports to determine whether sensitive and confidential information is protected.

Identification of shortfalls

The auditor should identify:

- Failure of compliance with the laws and regulations
- Failure in taking corrective action in case of non-compliance with the laws and regulations
- Failure in complying with health and safety measures
- Flaws in the privacy and security aspects related to data transmission
- Collapse/ crash in e-commerce systems
- Loopholes/ flaws in trading partner agreements and insurance contracts
- Flaws in trust relationships with trading partners
- Failure in complying with conditions of insurance contract

Answer: [d] Classification of data

Module:2

Reference No:M2062

Question: With regard to communication and management of policies and strategies the auditor should identify failure of the management

- [a] To communicate its policies on internal controls
- [b] To draft its intellectual property rights agreement
- [c] To provide training for its staff
- [d] To test the systems before implementation

Module 2- Audit working guideline

Policies and strategies- Communication and management Part 2

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Communication and management of policies and strategies	1. Management involvement 2. Communication 3. Adherence 4. Allocation of resources 5. Quality assurance 6. Evaluation and updation 7. Security 8. Internal Control 9. Ownership 10. Detailed policies	Not applicable for this activity

Audit Process

The Audit process has been covered in two parts. In the first part, the preliminary understanding and analysis have been covered. In the second part, the test of controls and substantive testing have been dealt with. This article is second in the two-part series.

Tests of controls

A clear picture of the functioning of the controls can be gained by

- Obtaining evidences
- Reviewing the deliverables

Tests: The following tests have to be done, before an opinion is formed on the functioning of IT tasks in the organisation.

1. IS environment is positive towards control as understood in the preliminary analysis stage
2. Employee awareness of the ethical standards
3. Communication of management's policies on internal control
4. Allocation of resources for implementing the internal controls
5. Regular review by the management of the policies, procedures and guidelines and ensuring that they are flexible
6. Commitment of the management in implementation of internal controls
7. Defined quality policies are consistent with the overall quality policies of the organisation
8. Procedure for ensuring that the defined quality policies are implemented
9. Procedure for measuring quality
10. Review of the exceptional reports, comparison reports, trend analysis at regular intervals relating to the IT functioning, security and internal controls by the management
11. Communication of the roles and responsibilities of the personnel
12. Documents relating to the decisions of the management and its signing by the management

Tests should be performed to ensure the above identified control measures in the preliminary analysis section

Substantive Testing

This step is undertaken so as to substantiate the auditor's view of controls objectives either not being met or not existing. The control weaknesses observed and its impact will have to be documented. In order to further substantiate the viewpoint

1. Comparative benchmarks, from similar organisation, industries can be identified.
2. Review of security and internal controls to establish whether the tasks were prioritised on the basis of risk and other factors.

Identification of shortfalls

The auditor should identify:

- Areas where internal controls are weak regarding communication of policies and procedures
- Failure of the management to communicate its policies on internal controls
- Shortfall in allocating resources for implementing internal control policies
- Failure to keep its plans up to date
- Non-compliance with the policies, procedures, standards and guidelines
- Failure in meeting the quality standards or in defining and communicating them
- Flaws in the security and internal controls

Answer: [a] To communicate its policies on internal controls

Question: The auditor can obtain preliminary understanding of an IT activity by interviewing the relevant management and staff and reviewing the related documents. Which of the following is not relevant to understand human factor?

- [a] HR department representative and associated staff
- [b] Security management representative and associated staff
- [c] IT human resources representative
- [d] Chief Executive Officer

Module 2- Audit working guideline

Managing the human factor

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Managing the human factor	1. Defining of the roles and responsibilities for each IT position 2. Required qualification for each position 3. Recruitment and promotion 4. Security clearance 5. Orientation 6. Training and cross training 7. Job performance evaluation 8. Job rotations and terminations	Not applicable for this activity

Audit Process

The Audit process has been covered in two parts. In the first part, the preliminary understanding and analysis have been covered. In the second part, the test of controls and substantive testing have been dealt with. This article is first in the two-part series.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. HR department representative and associated staff 2. Security management representative and associated	1. HR Policies and procedures 2. Job description

staff 3. IT human resources representative 4. IT management and associated staff 5. Representative of personnel involved in sensitive IT functions	3. Job evaluation 4. Training 5. Job enrichment 6. Personnel records of selected position and personnel

Preliminary analysis

The next step is analyse the effectiveness of the control measures adopted and the degree of reliability that can be placed on the control measures. This can be done through ensuring

1. Selection and recruitment of the personnel is based on a defined criteria
2. Qualifications for new recruits are based on the requirements laid down by the relevant professional bodies.
3. Job specifications are acceptable to the management and the personnel
4. Training provided to personnel is in accordance with the defined training programme
5. Management is interested in providing the training and educating the personnel
6. Appropriate steps are taken to identify gaps between technical and management skill and to eliminate them
7. Vital IT functions have continuous cross training and back up of personnel
8. Personnel are encouraged to take leaves
9. Security policies are adequate
10. Evaluation of the personnel based on the job specifications are done at regular intervals
11. Resources are safeguarded in case of change of jobs and terminations
12. HR policies and procedures comply with the laws and regulations applicable to the organisation

Answer: [d] Chief Executive Officer

Module:2

Reference No:M2064

Question: Which of the following statement is "TRUE" with regard to the audit guideline on management of human resources?

- [a] Personnel should be aware of their responsibilities and have adequate knowledge of their roles
- [b] Security and internal controls should be documented
- [c] Involvement of the personnel in defining the audit guideline for management of human resources
- [d] All of the above

Module 2- Audit working guideline

Managing the human factor - Part 2

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls

Managing the human factor	1. Defining of the roles and responsibilities for each IT position 2. Required qualification for each position 3. Recruitment and promotion 4. Security clearance 5. Orientation 6. Training and cross training 7. Job performance evaluation 8. Job rotations and terminations	Not applicable for this activity

Audit Process

The Audit process has been covered in two parts. In the first part, the preliminary understanding and analysis have been covered. In the second part, the test of controls and substantive testing have been dealt with. This article is second in the two-part series.

Tests of controls

A clear picture of the functioning of the controls can be gained by

- Obtaining evidences
- Reviewing the deliverables

Tests: The following tests have to be done, before an opinion is formed on the functioning of IT tasks in the organisation.

1. Recruitment and promotion process meet the objective and relevant to the requisites of the position
2. Personnel's awareness of their responsibilities and adequate knowledge of their roles.
3. Job descriptions are current and reviewed at periodical intervals
4. Assessment of personnel on their understanding of the organisation goals, their roles and responsibilities and the like
5. Personnel performing vital IT functions have continuous training and education programmes
6. IT personnel are trained in the security procedures and practices
7. Security investigation procedures are as per the laws and regulations applicable to the organisation

Tests should be performed to ensure the above identified control measures in the preliminary analysis section

Substantive Testing

This step is undertaken so as to substantiate the auditor's view of controls objectives either not being met or not existing. The control weaknesses observed and its impact will have to be documented. In order to further substantiate the viewpoint

1. Comparative benchmarks, from similar organisation, industries can be identified.
2. Review of activities of the IT human resource department can be performed

Identification of shortfalls

The auditor should identify:

- Any opposition, complaint, criticism by the personnel with regard to the HR policies and procedures
- Failure in allocating appropriate funds and time for training and development activities
- Personnel who have not been on vacation and are performing vital functions
- In case of recruitment, promotion, termination and transfers
 - Non-compliance with the defined policies and procedures
 - Non-compliance with the criteria specified for recruitment and promotions
 - Actions taken without the consent of the management
 - Decisions made without considering the job specifications and qualification of the personnel
- In case of personnel
 - Mismatch of qualification and position.
 - Mismatch of training and development opportunities and competency of the personnel.
 - Job performance of the personnel not evaluated
 - Non-performance of security investigation not performed
 - Non-signing of the security policy acknowledgment
 - Inadequate provision for training and cross-training

Answer: [a] Personnel should be aware of their responsibilities and have adequate knowledge of their roles

Module:2

Reference No:M2066

Question: Who is responsible for developing the intranet strategy and monitoring policies, standards and training?

- [a] Intranet administrator
- [b] Publisher
- [c] Editor
- [d] Webmaster

Module 2- Intranet organisational development - II

The previous article had provided an introduction to intranet organisational development. This article dwells on the first step in the implementation of the development programme -creation of organisation roles. The remaining steps will be discussed in the next article.

I. Creation of organisational roles: -

The administrator, publishers or content owners, editors or content managers, authors or content creators and webmasters are the different basic organisational roles that are required to be created. Their responsibilities and the skills required are also explained in the following paragraphs.

Intranet administrator: - A senior professional should be given this position. The main objective of an intranet administrator is to ensure effective communication and smooth functioning of an intranet.

Responsibilities

Intranet administrator is the head of the Web council and he has to

1. Develop the intranet strategy, and monitor the policies, standards and training.
2. Develop intranet skills within the organisation by creating awareness and training programs.
3. Preserve the documents pertaining to intranet standards and the enterprise map.

Skills:

1. The intranet administrator must be able to identify the business needs and understand the intranet technology.
2. He should have an interest in facilitating decision-making.
3. He must be capable of utilising intranet resources efficiently.

Publisher. - The publisher is directly responsible to the functional head of the organisation. His main responsibility is to determine the information that will be supplied by the organisation to insiders and outsiders.

Responsibilities:

The publisher is the head of the Editorial council, and represents the Web council as well

1. He creates the process for content to be approved and hosted, and identifies the input and output information requirements.
2. He also sets standards and supervises their implementation.

Skills:

1. The publisher should possess good leadership skills to implement standards and policies. He must also be able to understand the importance of information in achieving organisational objectives.
2. He should link intranet technologies and business functions to facilitate in decision-making.

Editor. - An editor creates and manages the information related to a particular area like software logic, product specifications product designs and manufacturing processes. Therefore an editor is also referred to as the product manager, marketing manager, software development manager.

Responsibilities:

An editor is the member of Editorial council

1. His main function is to recognise the resources and information essential to finish the project with in the predetermined schedules.
2. He has to ensure the availability of access controls and backup facilities.

Skills:

1. An editor should have good organisational and leadership skills to identify the project requirements, and manage the policies and standards of an organisation.
2. He must be capable of setting a realistic project schedules and manage it.

Author: - He is the content creator of an intranet. The content developed for one purpose can be redirected to another. Therefore, an author should remember that the content must be flexible to change and meet future requirements.

Responsibilities:

1. The author must provide the necessary information according to the standards.
2. The information supplied must be flexible and reusable.

Skills:

1. An author must be able to generate and present content with good presentation skills and programming tools.
2. He should understand intranet standards and protocols thoroughly.

Webmaster: - The Webmaster's main duty is to bring technology and non-technical specialists together, and to maintain Intranet-related technical infrastructure. A grand-webmaster is responsible for coordinating the work done by several webmasters performing different aspects of the Webmaster's role.

Responsibilities:

1. His technical responsibilities include administration of web server, access control, security requirements and providing proper backup and effective search engines.
2. His supporting responsibilities include responding to the 'webmaster' emails, screening out junk mails and answering common site mails

Skills:

1. The Webmaster should have a thorough knowledge of system administration, system programming, web servers, web-based applications, programming languages, database management systems and object-oriented approaches.
2. He must also help non-technical users to understand the technology.

Answer: [a] Intranet administrator

Module:2

Reference No:M2067

Question: Which of the following workshops is not a part of the adoption process in the intranet organisational development programme?

- [a] Planning workshop
- [b] Administrators' workshop
- [c] Publishers' workshop
- [d] Editors' workshop

Module 2- Intranet organisational development - III

Organisational development and the first step involved in the implementation of the development programme have been explained in the previous articles. The remaining four steps are dealt with in this article.

II. Functionality

Organisations can improve the efficiency of the development programme using:

- Easily accessible intranet
- User-friendly HTML
- Sufficient space for publishers and editors to publish their pages

- An intranet council
- Spider based search engine
- Space to conduct workshop

III. Adoption process

A series of staged workshops help participants to identify the roles, undertake the challenges and key decisions, and gain from effective strategies. An awareness seminar and three different workshops facilitate the adoption process

Awareness seminar

First, an executive awareness programme must be conducted. It should enable executives, publishers and editors to understand intranet concepts like background, benefits, issues and management and implementation models.

Planning workshop

The planning workshop must be able to:

1. Identify the user and the publisher's role
2. Identify the publisher's responsibilities
3. Recognise the technical knowledge required by publishers to provide different levels of information.

Publishers' workshop

The publishers' workshop must be able to:

1. Identify the publishers' role
2. Help the publisher to manage information
3. Establish the Web council and outline the publisher's role in the management map.

Editors' workshop

The editors' workshop must be able to:

1. Identify the editor's role
2. Facilitate the editor in decision-making
3. Develop intranet management skills and strategies
4. Outline the editor's role on the management map

In all the above three workshops, participants must identify their requirements and understand commitments to realise the community goals. They must help each other in decision-making.

IV. Participation

Simple technology, simple policies and rules and reasonable publishing standards will enable publishers, editors and authors to effectively participate in the programme. Permanent publishing space has to be provided to participants to encourage participation.

A Web council attempts to improve the quality in the participation phase. Further, policies, map pages and organisational roles help to manage the process. A spider-based search engine is an essential function in this phase.

V. Developing standards and policies:

The objective of the policies is to guide individuals to attain their goals with minimum effort. The following three rules help to do so:

1. Policies, which are applicable to other communication media, should also be applied to the intranet.

2. Owner's identification, date of changes last made, method to contact owner must be mentioned on a formal or informal page.
3. A clear guideline on confidentiality is also essential.

Standards for formal publishing

When an organisation officially publishes any page, it is referred to as a formal page. The following are some rules:

1. There should be an explicit review process.
2. Formal content pages should carry a logo of the organisation.
3. Details of the persons authorised to access must be stated.
4. Content must be specific to the organisation requirements.

Answer: [b] Administrators' workshop

Module:2

Reference No:M2068

Question: Which of the following is not a function of project manager?

- [a] Setting objectives for the project
- [b] Conducting feasibility study of the project
- [c] Executing the project
- [d] Ensuring effective utilisation of resources

Module 2- Functions of Project manager

A project manager has to don multiple roles viz. organiser, facilitator, planner, problem solver, decision maker and resource manager while managing a project. He is also required to maintain proper personnel relations with the team members.

He is essentially responsible for conducting the feasibility study of the project and chalking the necessary activities to attain the objective set by the user management. He develops the environment conducive for project implementation and ensures its smooth progress. He executes the project with proper planning and manages the project resources. He is responsible for successful project that entails its completion within the specified cost and time.

Responsibilities

Project manager has to perform the following group of functions: -

Integration management

Project manger plays an important role in project integration management by framing a plan for the project and executing it. He has to monitor the changes, if any, in the project.

Scope management

Project manger identifies the scope of the project and divides it into several sub-projects. He should maintain proper control over any changes to the scope of the project.

Time management

Time management functions include identifying the activities and their duration in the project, finding the

sequence in which they have to be performed and developing a complete schedule for the project.

Cost management

Cost management is another important function of project manager. He should identify the resources required for the activities and estimate the cost. He should prepare a cost budget and establish control over costs.

Quality management

Project manager has to establish standards for quality and hence a methodology to achieve that. He should appraise the performance of a project in terms of quality standards and encourage quality improvement.

Human resource management

Recognising the staff requirements and planning for their acquisition are important human resource functions of a project manager. He should support employee as well as organisational enhancement.

Communication management

Project manager is responsible for planning and distribution of communication throughout the project management team. He has to evaluate the performance and analyse the results.

Risk management functions

His risk management functions include identifying the risk, evaluating risk and taking measures to mitigate the risk.

Procurement management

Project manager is required to make procurement planning by recognising the probable sources and selecting a feasible source.

Knowledge and expertise

Project manager must be well versed with decision making, problem solving and resource allocation techniques. He should have excellent communication, presentation, mediation and negotiation skills. He should have a thorough understanding of organisation development, design methods, IT principles and planning techniques. Project manager must be aware of different aspects of IT like system development life cycle, programming and its techniques, databases, networks and information systems design.

Project manager needs to maintain proper contacts with users and user management, knowledge workers, system and network administrators, system analysts, software vendors, hardware vendors and IS service companies.

Answer: [a] Setting objectives for the project

Module:2

Reference No:M2069

Question: Which of the following goals focus on organisational and individual development?

- [a] Existential goals
- [b] Referential goals
- [c] Organisational goals
- [d] Individual goals

Module 2- Intranet organisational development - I

Efficiency of an intranet is not judged by its sophisticated design or its automation level but with its ability to communicate in a supportive way. The organisation and its members play an important role in developing an efficient intranet.

The foremost step is planning in order to determine the objective of the intranet. The vision of an intranet must be clear, without which success cannot be measured. The organisation's vision may take two forms: -

1. **Existential vision:** The focus is on organisation and individual development. The technical infrastructure will help the development.
2. **Referential goals:** Here the focus is on the technical infrastructure like web-based applications and processes to provide efficient network services at low cost.

We discuss about the organisation and individual development in the series of three articles. We begin with a brief discussion on web-based applications made.

Web application development

If the potential intranet application development is based on an existing application, its development is fast and easy. However, it might look more of a back-office database integration process than a web project. In order to derive maximum returns, the emphasis should be on advanced web-based functionality. A thorough knowledge of paradigms and approaches is essential for this.

Good expectation management, change management skills and Rapid Application Development techniques are essential to develop a complex intranet application project. New intranet architectures and tools can be better understood through the length and complexity involved rather than type of the project. This helps to select a standard component with a modular architecture.

Organisational and individual development

As against a complex web-application development, individual and organisational development requires a simple technology. This is because, a complex application development project makes it difficult to adopt intranet for an informal learning and knowledge functions. In the light of this, the technical aspect is taken as the basic infrastructure to understand individual responsibilities and behaviours.

Proper allocation of responsibility and decision-making is essential for organisational development. Its implementation can be made effective through a series of workshops that enable the participants to understand issues and decision making. The workshop method is best suited for the large implementation structure.

The following are the steps involved in the implementation of organisation development programme: -

1. Creation of organisational roles
2. Execute the technical functionality to support the basic organisational development process.
3. Facilitating organisation's people to adopt the necessary roles and skills.
4. Create a critical mass of intranet participation within the organisation
5. Developing standards and policies to ensure free flow of information.

Answer: [a] Existential goals

Module:2

Reference No:M2070

Question: Which of the following is the first and foremost function of a Chief Security Officer?

- [a] Identifying and evaluating the existing policies and procedures for security
- [b] Monitoring the level of service provided by service providers
- [c] Reviewing the certification programs for organisation security standards
- [d] Identifying critical information assets

Module 2- Functions of Chief Security Officer

Security being an essential element in the IT environment, the chief security officer plays an important role in ensuring it. His primary responsibility is to develop policies and procedures to prevent unauthorised access and provide timely information to the business managers. He should also monitor the level of service provided by service providers and outsiders.

Chief security officer's relationship with others is represented in the following diagram.

The existing policies and procedures have to be evaluated and future course of action has to be determined and communicated to the business community.

Responsibilities

The corporate security and data security responsibilities of a CSO are as follows: -

1. The first and foremost duty of any security officer is to identify and evaluate the existing policies and procedures for security. He has to scrutinise the processes and review the reports regularly.
2. Establishing security policies, standards and guidelines is the next step in security officer's functions. For this, he needs to understand the security features of the new computing systems and link them with the existing features. He has to monitor the changes, if any.
3. He should identify the potential disruption areas in the event of any disaster and develop business resumption plan, disaster recovery and business continuity plans.
4. He should supervise the facilities and data processing resources in order to suggest corrective measures in case of any suspicion.
5. Critical information assets and facilities like data centres have to be identified and safeguards must be implemented to protect those assets and facilities.
6. Chief Security Officer must facilitate the internal audit department to evaluate personnel, applications and IT assets to enable its compliance with the security standards.
7. He should develop and review the certification programs for organisation's security standards pertaining to new technology acquisition. He should also check its compliance with over all integration process.

Decision making function

CSO has to make decisions regarding the security procedures and policies necessary for data security, its development and execution.

Human Resource function

He should monitor the training program on corporate security awareness and manage the security staff.

Skill and expertise

Chief security officer should have excellent communication skills and thorough knowledge of security policies and principles. He should have a clear understanding of Internet based security, standard based architectures, compliance monitoring, vulnerability and penetrating testing. He should update his knowledge constantly in the area of security and business resumption.

Reporting

If the main function of CSO is to mitigate technical threats, he is directly responsible to the Chief Information Officer. If it is combined with the corporate function, then he has to report to the Chief Financial Officer. He is also one of the members of Executive Council.

Contacts

Information security officer has to maintain proper contacts with protection service providers, security managers, EDP auditor, application development project managers, data responsible administrators and security staff.

Answer: [a] Identifying and evaluating the existing policies and procedures for security

Module:2

Reference No:M2071

Question: Which of the following is the primary responsibility of Computer Operations Supervisor?

- [a] Preparing budgets
- [b] Designing policies and procedures for operations
- [c] Managing operating systems, operating staff and peripheral equipment
- [d] Installing application software

Module 2- Functions of a computer operations supervisor

Computer operations supervisor is primarily responsible for managing operating systems, operating staff and peripheral equipment. He should solve software and hardware related problems so as to meet their requirements on time. The following are the important duties and responsibilities of a computer operations supervisor.

Responsibilities

1. **Supervisory functions:** The supervisory functions of a computer operator consists of scheduling and assigning the operating work to the staff and monitoring their performance for its timely and accurate accomplishment. He should determine the requirements of training to improve their performance.

Computer operator supervisor should also support HR staff in hiring functions. He is responsible for the operating staff's discipline. He should create a working environment that provides personal growth and career development and resolve the personnel related problems at the primary level. He should respond to the user inquiries and assist them in solving their problems.

2. **Operation services:** Computer operator supervisor has to prioritise the tasks and monitor their processing. He should evaluate the processes to ensure accuracy of the output. He should maintain a record of production status, downtime, operation failures and service calls for the use of operating users.

Operations supervisor is required to alter job control language as per specific job requirements and ensure that output is in compliance with the shop standards. Locating the processing errors and solving them through appropriate procedures is one of the important operating functions of supervisor.

3. **Equipment maintenance:** Computer operations supervisor is responsible for maintaining the equipment in order to maximise the production. He should establish schedules for repairs and downtime and support service technicians. He has to regularly monitor the staff log reports to prevent system malfunctions. Operations supervisor should also provide a proper physical environment suitable for operations.
4. **Miscellaneous:** Computer operations supervisor can assist in designing policies and procedures for operations, acquiring operational equipment, preparing budgets and installing application software, computer hardware and operations software. He must be capable of electronic computer operations and peripheral equipment handling without any assistance.

Knowledge and expertise

Computer operations supervisor should have a thorough knowledge of operating systems, procedures, tape drives, disk drives, printers and the like. He must be well aware of hardware, job scheduling techniques, job control languages and data communication networks. He must be competent enough to handle computer systems and its peripherals and manage production schedules. He should be able to identify the problematic areas and suggest appropriate remedial measures. He should maintain a daily record of production status, failures in operation, service calls and problems related to programs.

Contacts

Computer operator should maintain proper relations with programmers, operating staff, vendors and computer engineers, in order to perform his functions efficiently.

Answer: [c] Managing operating systems, operating staff and peripheral equipment

Module:2

Reference No:M2072

Question: Which of the following is not a component of a service level agreement?

- [a] Services that will be provided
- [b] Satisfaction of the service receiver
- [c] Cost of services
- [d] Method of calculating the cost

Module 2 - Audit working guideline

Service level agreement Part 1

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Service level agreement	1. Management guideline 2. Service level agreement 3. Procedures 4. Review 5. Reporting 6. Chargeable units 7. Improvement	Not applicable for this activity

Audit Process

The audit process has been covered in two parts. This article is the first part, and deals with a preliminary understanding and analysis of the process.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. CIO 2. IT management 3. Service level team 4. Operations team 5. Users	1. Policies and procedures with respect to • Service level agreements • Reports • Monitoring of performance • Corrective actions 2. Organisation policies and procedures relating to user services 3. Documents with regard to • Performance appraisal • Cost sheet • Improvements • Alternatives, in case of non-performance of the services • Variances

Preliminary analysis

The next step is to analyse the effectiveness of the control measures adopted, and their reliability. This can be done by ensuring that the following factors are in place:

- Provision in the policy for the existence of service level agreements
- Involvement of users in the framing of agreements and their modification
- Users and providers are aware of their roles and responsibilities
- Continuous monitoring of the performance and resolution of all problems
- Regular review by the senior management
- Alternative sources are identified in case of non-performance of the services
- Service level agreements should be written and at the minimum, include the following
 - o Services to be provided
 - o Cost of the services
 - o Method of calculating the cost
 - o Minimum service level
 - o Resources of other IT functions that will be provided
 - o Security
 - o Measurement of performance
 - o Growth prospects
 - o Improvements
 - o Continuity of operations
 - o Period of the agreement

- o Renewal or non-renewal criteria
- o Procedure for modifying the agreement
- o Comparison of the charges with industry standards and other best practices

The next article focuses on the second part - the test of controls and substantive testing.

Answer: [b] Satisfaction of the service receiver

Module:2

Reference No:M2073

Question: Which of the following statements is "TRUE" with regard to service level agreements?

- [a] The auditor should test whether the users are satisfied with the services provided
- [b] Server security policy should be reviewed
- [c] Service level agreements take into consideration the risk analysis
- [d] All of the above

Module 2 - Audit working guideline

Service level agreement Part 2

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Service level agreement	1. Management guideline 2. Service level agreement 3. Procedures 4. Review 5. Reporting 6. Chargeable units 7. Improvement	Not applicable for this activity

Audit Process

The audit process has been covered in two parts. The first part covered a preliminary understanding and analysis of the process. This article is the second part, and focuses on the test of controls and substantive testing.

Tests of controls

A clear picture of the functioning of controls can be gained by:

- Obtaining evidence
- Reviewing the deliverables

Tests: Before the auditor takes a stand on the functioning of IT tasks in the organisation, he should check whether

1. The service level agreements have been tested, both in the past and the present to ensure that these agreements, at the minimum include the following:
 - Description of service
 - Cost for services provided
 - Minimum service levels
 - Resources of other IT functions that will be provided
 - Security aspects
 - Measurement of performance
 - Growth prospects
 - Improvements
 - Continuity of operations
 - Period of the agreement
 - Renewal or non-renewal criteria for the agreement
 - Procedure for modifying the agreement
 - Comparison of the cost with industry standards and other best practices
2. The agreement has been approved by the service provider and receiver
3. The users are satisfied with the services provided
4. The records and documents of the service providers to determine the reasons for non-performance
5. Records and documents of the service provider for determining whether the performance improvement procedure is defined and implemented
6. Variance between the agreed and the actual charges
7. Trend analysis of the past service performance and improvements
8. Actions taken by the management in case of problematic situations and circumstances

Tests should be performed to ensure that control measures identified in the preliminary analysis are functioning as desired.

Answer: [a] The auditor should test whether the users are satisfied with the services provided

Module:2

Reference No:M2074

Question: Contracts with a third party would include which of the following?

- [a] Approval of the management
- [b] Satisfaction of the service receiver
- [c] Performance appraisal
- [d] Method of calculating the cost

Module 2 – Audit working guideline

Outsourcing/ Managing third party services Part 1

Table of applicability

For IT task	Control objectives	
Outsourcing/ Managing third	Management controls	Operational controls

party services	1. Legal enforceability 2. Identification and supplier interface 3. Owner relationship 4. Contract 5. Qualification 6. Continuity of service 7. Monitoring and maintaining	Not applicable for this activity

Audit Process

The audit process has been covered in two parts. This article is the first part, and deals with a preliminary understanding and analysis of the process.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. CIO 2. IT management 3. Service level team 4. Operations team 5. Security in-charge	1. Policies and procedures with respect to • Third parties • Procedure for selection of vendor • Security • Quality maintenance • Contingencies • Outsourcing 2. Organisational policies and procedures relating to services that are outsourced and maintenance of the relationships with the vendor 3. List of contracts with a third party 4. Contracts and agreements 5. Reports on services of a third parties 6. Minutes of the relevant meetings 7. Privacy agreements 8. Access list of resources and services available to vendors

Preliminary analysis

The next step is to analyse the effectiveness of the control measures adopted, and their reliability. This can be done by ensuring that -

- Policies relating to third parties are in place and are consistent with the overall organisational policies and procedures
- Authorised personnel are responsible for contracts i.e. framing, reviewing, maintaining, negotiating and the like
- Third parties involved are informed about the interfaces

- All the terms and conditions are explicitly explained in the contract
- The contract specifies the continuity of the contract till its is expires
- Contracts provide for contingencies
- Contracts should include the following
 - o Approval of management
 - o Legal approval
 - o Services that will be provided
 - o Cost
 - o Duration in which the amount will be paid
 - o Problem resolution
 - o Fine for non-performance of services
 - o Duration of the contract
 - o Process for termination and making changes to the contract
 - o Reports to be made
 - o The communication process and its frequency
 - o Roles and responsibilities
 - o Security aspect
 - o Non-disclosure statement
 - o The access and audit right
 However, the above list is not an exhaustive one.
- The management has entered into an escrow agreement where required
- An assessment of the capability of third parties is done to ensure their ability to deliver the services

The next article focuses on the second part - the test of controls and substantive testing.

Answer: [a] Approval of the management

Module:2

Reference No:M2075

Question: Which of the following statements is "FALSE" with regard to the audit guideline on managing third party services?

- [a] Contracts with third parties explicitly provide all the terms and conditions including the contingency provision
- [b] Policies and procedures related to third parties are consistent with the overall organisational policies
- [c] Third parties should be aware of their roles and responsibilities
- [d] Services that are received need not be limited to those defined in the contract

Module 2 - Audit working guideline

Outsourcing/ Managing third party services Part 2

Table of applicability

For IT task	Control objectives	
Outsourcing/ Managing third	Management controls	Operational controls

party services	1. Legal enforceability 2. Identification and supplier interface 3. Owner relationship 4. Contract 5. Qualification 6. Continuity of service 7. Monitoring and maintaining	Not applicable for this activity

Audit Process

The audit process has been covered in two parts. The first part covered a preliminary understanding and analysis of the process. This article is the second part, and focuses on the test of controls and substantive testing.

Tests of controls

A clear picture of the functioning of controls can be gained by:

- Obtaining evidence
- Reviewing the deliverables

Tests: Before the auditor takes a stand on the functioning of IT tasks in the organisation, he should check whether

1. The contract list provided is accurate
2. Services are provided only by those with whom a contract is entered into, including PBX contract
3. Services are delivered as per the contract
4. Third parties are aware of their roles and responsibilities
5. Policies and procedures related to third parties are consistent and comply with the overall organisational policies
6. Authorised personnel are responsible for contracts i.e. framing, reviewing, maintaining, negotiating and the like
7. Contracts explicitly provide all the terms and conditions including the contingency provision
8. The contract at the minimum includes
 - o Approval of the management
 - o Legal approval
 - o Services that will be provided
 - o Cost
 - o Duration in which the amount will be paid
 - o Problem resolution
 - o Fine for non-performance of services
 - o Duration of the contract
 - o Process for termination and making changes to the contract
 - o Reports to be made
 - o Communication process and its frequency
 - o Roles and responsibilities
 - o Security aspect

- o Non-disclosure statement
- o Access and audit right
- 9. Only a necessary number of vendors are included in the access list for access to resources
- 10. Access to resources is as per the access list
- 11. Actual delivery of services is as per the contracts
- 12. Performance delivery is as per the expectation
- 13. Continuous review of services by the management
- 14. Audit of third party services is undertaken
- 15. The capability of the third party is derived on the basis of assessment reports
- 16. The provision of interfaces provided to third parties in the contract is documented

Tests should be performed to ensure that control measures identified in the preliminary analysis are functioning as desired.

Answer: [d] Services that are received need not be limited to those defined in the contract

Module:2

Reference No:M2076

Question: Which of the following requires careful management in relation to Information system Management?

- [a] Change management
- [b] Security management
- [c] HR management
- [d] All the above

Module 2 – Management practices in Information system management - 1

Introduction

The Information systems (IS) department has come to play an indispensable role in the working of the organisation. Therefore it is essential to ensure the proper management of information systems. The duty of the IS Auditor, in this context, is to evaluate the efficiency of the IS department.

Information systems can be managed with the help of general management principles. However a few critical functional areas have to be managed with extra care.

1. **Change management:** - Change is inevitable to any business, more so with the deployment of IS. Change has to be efficiently managed for a smooth transition without affecting the existing systems. Improper change management decisions may cause huge damage to the organisation. There should be enough policies and procedures in place, which include procedures for planning, impact analysis, version control, security and quality aspects.
2. **Third party management:** - Generally some of the functions of IT department like data centre operation, application system development, system maintenance are contracted or outsourced to a third party. Outsourcing brings many advantages to the organisation like reduction of in-house operations and sharing the expertise of the third party. Apart from outsourcers, IS department is also required to deal with several other third parties who are engaged in supply of systems and networking. Therefore third party management is an important function of management.
3. **Security management:** - management should develop a comprehensive approach vis-à-vis the company's mission and objectives for protecting the systems, networks and information. A security programme that enables development and implementation of procedures must be properly documented and communicated across the organisation. Users must be well aware of the security policy and

implement it.

Disaster recovery and business continuity plans must ensure the continuity of operations even in case of disaster. Disaster recovery planning, part of business continuity planning, refers to a set of steps that an organisation must undertake in case of a natural or man made disruption to the functioning.

4. **Process management:** - Process management is one of the critical functions of management as they play an important role in the functioning of IS. Strong policies and practices, which define the process, improve the performance of systems.
5. **HR management:** - IT professionals' recruitment and retainment is the major problem for companies. Switchover tendency of the IT professionals is the root cause of the problem. However companies have to manage Human Resources through proper recruitment, retaining, training, and restructuring practices. An opportunity for training plays a critical role in IT staff recruitment and their retention. Proper HR policies that deal with the employee management must exist. Training provided to IT staff brings advantages in long run. Training must consist of technical as well as interpersonal competencies.

Answer: [d] All the above

Module:2

Reference No:M2077

Question: Which of the following can be determined with the help of evaluation methods in relation to Information systems management?

- [a] Deviations in the actual performance from the expected performance
- [b] Right amount of funds to be allocated required activities
- [c] Future capacity requirements
- [d] Organisational goals

Module 2 - Management practices in Information system management - 2

Introduction

The Information systems (IS) department has come to play an indispensable role in the working of the organisation. Therefore it is essential to ensure the proper management of information systems. The first part of the article dealt with the management principles for information systems. The present article deals with some more aspects, which are essential in determining the effectiveness of management of information systems.

Evaluation methods for information systems, budgets, goal attainment, benchmarking, capacity and growth planning, user satisfaction and financial management practices are different aspects that need to be considered in IS management.

1. **Goal attainment:** - Company's goals in relation to IS may be expressed in terms of technical, operational and economic goals. Goals have to be defined in advance in order to have a direction for the functioning. Later the actual performance is measured against these predetermined goals.
2. **Information system budgets:** - Budget is often referred as a forecasting and monitoring tool. It helps to allocate right amount of funds to the required activities. Further it serves as a helpful tool in evaluating the cost-effectiveness.
3. **Benchmarking:** - Benchmarks or the standards collected from outside sources like industry publications or publications by professional associations refer to the best performance that an organisation can expect from the information systems. These benchmarks enable organisations to

evaluate the performance of their information systems. Benchmarks are available for several activities like online transaction processing environment, back-end server, order entry systems and decision support systems.

4. **Capacity and growth planning:** - With increasing technological advancements, growth and capacity must be well planned properly in order to attain the business objectives. Capacity planning refers to the hardware capacity essential for server load. System performance, transaction volume and application interface must be considered in determining the capacity.

The systems must be regularly monitored to determine the capacity requirements. Identify the current usage of network and server facilities and determine the future requirements. Additional hardware must be added to meet the future requirements.

5. **Evaluation methods for information systems:** - Information systems need to be evaluated to determine the performance of IS activities. Evaluation methods enable to determine the deviations if any, from the expected performance and thereby provides an opportunity for corrective measures.
6. **User satisfaction:** - User satisfaction is one of the objectives of information systems. Processing operations can be evaluated through the level of satisfaction derived by the users. User satisfaction can be measured with the help of regular monitoring and interviews.
7. **Financial management practices:** - Financial management practices occupy a predominant role in the information systems arena. The high cost involved in the information systems demands right financial management practices to assess the performance of information systems and processing facilities. It ensures the effective utilisation of information system resources.

Answer: [a] Deviations in the actual performance from the expected performance

Module:2

Reference No:M2079

Question: Which of the following is least likely to be tested by the auditor to obtain an understanding of the training in the organisation?

- [a] In house facilities for imparting training
- [b] Employees attendance for training
- [c] Assessment of the required training
- [d] Employees level of awareness of the organisational plans

Module 2 - Audit working guideline

Training

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Training	1. Identification of needs 2. Training syllabus and contents 3. Organising training 4. Imparting training 5. Security knowledge	Not applicable for this activity

Audit Process

The audit process has been covered in two parts. This article is the first part, and deals with a preliminary understanding and analysis of the process.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. HR team 2. Training team 3. IT managers and its team 4. Users	1. Policies and procedures with respect to training on controls and security 2. Organisation policies and procedures relating to • Training on security and controls • Training which benefits employees • Continuous education facilities • Users of training programmes 3. Training programmes that are available to the employees at present

Preliminary analysis

The next step is to analyse the effectiveness of the control measures adopted, and their reliability. This can be done by ensuring that the following are in place:

1. Policies and procedures exist for
 - Making the employees aware of security and control aspects
 - Training the employees and that such training imparts knowledge that is in accordance with the IT resources used by the organisation
2. Training
 - Emphasis on IT security and controls should be implemented
 - There are in house facilities available for imparting training
 - Employees attend the training
 - Assessment is made of the requiring training
 - Providing it either internally or externally
 - Employees provide an assurance for non-disclosure of sensitive information
3. In case of employees
 - Security and control features of IT resources are explained to the new employees
 - There is a continuous training programme that the employees are required to attend. The training programme focuses of the following:
 - o Security and their related responsibilities
 - o Ethical conduct

Tests of controls

A clear picture of the functioning of controls can be gained by:

- Obtaining evidence

- Reviewing the deliverables

Tests: Before the auditor takes a stand on the functioning of IT tasks in the organisation, he should check whether

- New employees are aware of the security and control features of IT resources
- Employees are aware of their responsibilities related to security and controls
- There is a continuous assessment of the training needs for the employees
- Signing of non-disclosure forms by all the employees
- All the employees are regularly assessed for the training that needs to be imparted to them

There are designated individuals in the organisation for imparting the training and educational programmes. Tests should be performed to ensure the above identified control measures in the preliminary analysis section are in place.

Substantive testing

This step is undertaken to substantiate the auditor's viewpoint that control objectives are either not being met, or do not exist. The shortcomings in controls and its consequences also should be documented. He can also:

1. Review the training manuals to ensure that they are adequate
2. Interview the staff to ascertain that the required training needs have been assessed and also the extent to which they are fulfilled

Identifying shortcomings

The auditor should identify:

- Failure to impart the training as per the identified needs
- Lack of awareness among the employees in security and controls

Answer: [d] Employees level of awareness of the organisational plans

Module:2

Reference No:M2080

Question: Which of the following is cash benefit of performance benchmarks?

- [a] Enhancement in productivity levels
- [b] Reduction in mistakes
- [c] Reliability of information
- [d] Optimisation of turnaround time

Module 2 – Benchmarks for performance assessment

What are performance benchmarks?

Performance benchmarks are standards set by the management or by recognised body to measure the performance of the IT activities in the organisation.

Need for performance benchmarks

Whenever new technology is introduced there are no defined standards of performance for it. In a rush to implement it the management may not frame any performance criteria. Hence, in the absence of such

measurement criteria the performance assessment will be based on opinion rather than any objective criteria. For this, the organisation must define the benchmarks for technology. It should determine the benefits that are derived by implementing the new technology both in terms of cash and non-cash benefits.

Cash benefits can be

- Enhancement of productivity levels
- Decrease in costs
- Wide availability of information
- Fewer mistakes
- Increase in communication
- Better management control

Non-cash benefits could include

- Reduction in mistakes
- Reliability of information
- Optimisation of turnaround time
- Faster data storage and access
- Increased efficiency
- Better services to customers
- Improved public image and the like

Defining performance benchmarks

The organisation should define the methodology of computing the performance in measurable terms. Performance benchmarks define the key performance indicators and measure the results. In other words it helps in measuring the performance of the enablers in the process. IT is one of the important enabler in the information system based organisation. Hence it is also necessary to measure and define the relationship between organisation goals and their performance and IT activities goals and their performance.

Performance indicators

General performance indicators: The general performance indicators of the IT activities are

- Computing the performance of activities
- Determining the probability of the continuation or breakdown in the future
- Improvement in the IT processes
- The activity is both process and IT based
- Measurable
- Improvement in performance of resources most vital to the process

Generic IT indicators: The generic IT indicators would include

- Cycle times
- Quality
- Optimum utilisation of bandwidth
- Continuous availability of services
- Customer satisfaction
- Number of employees who are well versed in IT
- Satisfaction of the shareholders
- Cost benefit comparison
- Increase in productivity
- Analysis of non-compliance reports

- Comparison of the organisation performance with the defined benchmarks and standards and the like

Auditors and performance benchmarks

Performance benchmarks are not only useful to the management but also to the auditors. Auditors who are required to give their opinion on the performance of the IT activities can now assess the performance of the organisation based on this defined standards.

Conclusion

Performance benchmarks make organisation more efficient and effective. The benchmarks should be continuously monitored for modifications to accommodate the changes in the business activities, environment and technology.

Answer: [a] Enhancement in productivity levels

Module:2

Reference No:M2081

Question: The ISO 17799 that is based on BS 7799, a British Legislation is used as

- [a] International Standards
- [b] British Standards
- [c] European Standards
- [d] None of the above

Module 2 - Comparison between Common criteria and ISO 17799

Today there are many products and systems available in the market so much so that a layman will find it difficult to choose from the various alternatives. e Also there is no assurance that the product will live up to its claims. .

This led to the framing of international standards that the vendors and developers of products and systems should abide by.

In this article we compare the two most widely recognised security standards - Common Criteria (CC) and ISO 17799.

Common Criteria	ISO 17799
1. It is a joint venture of National Institute of Standards and Technology (NIST) and National Security Agency (NSA) and other similar organisations of different countries	1. It was developed in United Kingdom as BS 7799.
2. In the year 1999 it became an International Standard.	2. In the year 1999, the earlier version was revised and regulations related to the British Standards were removed. It came to be known as ISO 17799.
3. It evaluates the security features of IT products and systems.	3. It is a set of controls that include the best practices of information security.

4. This criteria is useful to consumers, developers and evaluators. Consumers are benefited as it helps them to determine which products meet the defined security requirements, to developers by defining the security requirements that should be embedded in the product and the evaluators the standards against which the systems should be tested.	4. It is basically a range of controls that should be embedded in different products and systems. It is also helpful to the consumers and vendors.
5. It is divided into three parts. Part 1 in the general introduction and describes the general concepts related to evaluation of security. Part 2 deals with functional requirements of security. Part 3 focuses on standards to express the assurance specifications for products and systems. It also describes the Evaluation Assurance Levels (EAL) the scale on which the CC rates its confidence on the security provided by the different products and systems.	

Answer: [a] International Standards

Module:2

Reference No:M2082

Question: Which of the following is not a part of contents of ISO 17799?

- [a] System Access Control
- [b] Physical and environmental security
- [c] Vendor evaluation criteria
- [d] Computer and operations management

Module 2 - ISO 17799

Information is a significant asset of a company. It is vital for any organisation to protect and secure its information by implementing controls and security procedures. The need for a common standard on the best industrial practices for information security management led to the development of BS 7799 standards. BS 7799 was originally developed in 1993 and published in 1995 as British Standards. It provided the best practices in information security. The keen interest shown by the other countries in BS 7799 led to its revision in 1999 to remove any UK specification and to take into accounts the developments in technology related to e-commerce, third party arrangements and the like. This version was released as BS 7799-1:1999. Later again in 2000 it was released as international standard BS ISO.IEC 17799:2000 or ISO 17799.

Contents of ISO 17799

ISO 17799 is divided into ten major chapters, each dealing with different aspects of security in an organisation. The brief outline of the chapters is as follows:

1. Business continuity planning: This chapter provides a guideline on measures to be taken to prevent business interruptions and disasters.
2. System Access Control: This chapter provides a guideline on providing access control to information, protecting it from unauthorised users, ensuring security of information on the network and mobile computing and the like
3. System Development and Maintenance: Guideline is provided relating to security issues to be incorporated in the operating and application systems, to prevent misuse, loss or modifications to data, to ensure that the integrity, confidentiality and authenticity of the data is maintained, and the like
4. Physical and environmental security: Objective of this chapter is to protect the business assets including information from loss, damage, theft, interruptions, disasters and the like, to protect from unauthorised users and the like
5. Compliance: The aim of this section is to ensure compliance to the organisation security policies, procedures and standards, compliance with the laws and regulations as application and any other security requirements
6. Personnel security: The purpose of this chapter is to provide a guideline on confirming that the users are aware of the security threats, implementing the security policy, minimising the risks of human error, to prevent misuse of facilities and the like
7. Security organisation: To ensure the security of information within the organisation and when processing of information is outsourced to third parties, and the like are included in this chapter
8. Computer and operations management: This section ensures integrity and availability of processing of information and its communication, protecting the information which is on the network, protecting the assets and any other supporting infrastructure, and the like
9. Asset classification and control: To ensure that appropriate protection is provided to organisation assets and information assets is the objective of this section
10. Security policy: The purpose of this chapter will be to ensure that management provides the necessary direction and required support

Within each chapter they are more detailed statements. But not all the controls and guidance in the standard may be applicable to all the organisations.

Answer: [c] Vendor evaluation criteria

Module:2

Reference No:M2084

Question: Application programmers interface assist in -----

- [a] Interoperability
- [b] Site administration.
- [c] Archiving.
- [d] Deployment.

Module 2- Content Management - Part 6

This is the sixth and concluding part of the series on content management. In the fifth part we explained a few features of a content management system. In this article we have given the rest of the features.

Hosting, deployment and retirement

After staging, the next step involves hosting onto the public server. This requires a complete replication of the web content, including application components, access control lists etc. Some content management systems only help in replicating web elements like pages, graphics, multimedia files etc. Certain systems aid in complete replication. They must also help in updating multiple servers at a time. Transactional replication systems also help in rolling back if any mistake occurs during deployment. Certain deployment systems also allow for automatically scheduling incremental deployments. These systems also aid in archiving the site to a separate destination.

Analysis and intelligence reports

These systems help in analysing the customer behaviour. They help in identification of most visited areas, usage time etc. These systems are found only in large sites and are expensive to use.

Interoperability

Some vendors provide for interoperability by Application Programmers Interface. This helps in other third party vendor to integrate his service areas into the system.

Administration tools

This assists in team member management by assisting in tasks like configuration for a new member, participation etc.

Search facilities

By embedding meta data, these systems provide for a search facility for the customers. These systems also help in integrated indexing.

HTML editors

These are the basic web content integration tools. But the features of these tools have increased and now provide for facilities like site development, positioning of elements, deployment and even a simple workflow.

Templates, Layouts and style sheets

The content management systems aid in creation and development of templates for the web pages. This will give the site a uniform look. These are also modifiable to alter the appearance. Other devices that can be created include style sheets, layouts and themes.

Find and replace tools

These tools can be used for common changes to be made across web pages like for instance logos etc.

Source code management system

These systems provide a version-based control for documents. Through these systems, all changes to the document can be tracked and identified. Authors of content can share the documents, make independent changes and later merge the changes.

Application development

These help in design, program, debug, and all the rest of the tasks connected to application development. Ultimately these help in development and deployment of application content. And also these systems help in working in isolated mode independently and later transferring it to the main destination

Staging

These systems provide a duplicate of the actual location for testing and quality assurance purpose.

Caching

The content is cached in the server memory for effectiveness to increase the site performance.

Answer: [a] Interoperability

Module:2

Reference No:M2085

Question: ----- type of tools can best handle the task of deploying middle tier application component

- [a] Developer tools
- [b] Workflow based content management systems
- [c] Object oriented repositories
- [d] None of the above

Module 5- Content Management- part 5

This is the fifth of a six part series on content management. In this part we have given few details about the features that a content management system tool should possess.

Types of content management systems

A variety of tools are available these days in the market for content management. These could be in the form of documentation systems, automated management tools and integrated systems.

Traditional content management systems: These traditional systems are generally strong in the areas of workflow, collaboration and version control. But these systems do not have strong integration facilities.

Storage management systems: These only serve a part of the entire content management process. They provide an object-oriented repository for storing content of any type. This helps the developers in creation of dynamic pages consisting of re-usable objects.

Developer tools; These manage the task of deployment of middle tier application components. The other functions handled by them include the site deployment management, link testing, templates, navigation design etc.

Source code vendor's tools: These tools vendors are now providing web document templates, workflow features and extensive auditing features.

Content management system features

Given below are some of the features found in most of the content management systems:

Workflow management and automating tools: Workflow system defines the various steps involved in creation, hosting and management of content. These define the functions that are to be carried out. Workflow systems help in tracking, assignment of roles and responsibilities and provide visibility to the entire process.

Some tools provide workflow templates while some advanced tools automate the entire process like setting up roles and responsibilities, designing the workflow etc.

Metadata: These systems help in classification of the content. Content classification helps in assigning

metadata value, search results, content targeting etc.

XML repositories: These help in storage of content as XML. This provides an easy search facility for authors, easy validation against certain document definitions. XML segregates the content from format and logic. Combining the individual elements from the repository can dynamically create web pages and documents.

Roles-based security: Such workflow management systems aid the administrators in controlling the actions based on each personnel's role. Each team member is given access to content at different levels based on the stage in which the person is functioning.

Customisation/personalisation: Many content management systems provide facilities for personalisation of web content. By analysing the customer's previous behaviour it is possible to predict the pattern and customise the content accordingly. Adding the metadata into the content can do this. It also requires a member's database to store the customer's attributes and history.

Part 6 of the series contains the rest of the features.

Answer: [a] Developer tools

Module:2

Reference No:M2086

Question: The term web content includes ----- type of content

- [a] Creative content
- [b] Application or processes
- [c] Both creative and application content
- [d] None of the above

Module 2- Content management-part 1

This is the first article of the six part content management series. The objective of this article is to provide the reader a broad view of the various issues in content management, the structure of a typical B2C website and features that a content-management systems should possess.

The scope of the term website content

The term web content includes anything and everything that is available on the web site, which is sent to the user's browsers. It also includes the processes software or otherwise that is used to support the delivery to the users. These processes could either directly or indirectly support the delivery of content to the ultimate user. The main challenge involved in management of web content is the volume or the size of the web or the number of pages a website has. It is estimated that number of pages on some large web site are doubling every year.

Content management - issues that need to be considered.

Some of the common issues related to content-management of e-commerce web sites are as follows:

1. Documented procedures for management of all types of web content
2. The procedures adopted by the product manager for initiation and launching of new product
3. Procedures related to pricing decisions
4. Legal approval for new content

5. Approval for graphics and multimedia for new launches
6. Integration of new creative content with the existing application content
7. Testing procedures
8. Responsibility for testing and compliance testing
9. Guidelines for web developers, authors, testers and graphics specialists
10. Tracking changes to content and roll back to earlier versions.
11. The existence of a content management system
12. Guidelines for updation of content
13. Uniformity in the content
14. Storage
15. Determination of the status of a web content project

Significance of content management

An effective content management can ensure that fresh, high quality content is made available to the clients. This helps in building a better customer relationship. This also helps in cost reduction for the entire management process. This may include developing new products as per market conditions, modifying the promotion campaign etc. Content management also ensures that accurate and timely information is posted on the website. Content management also ensures that proper testing procedures are framed and complied with for the content. This prevents situations such as low site availability, poor performance etc.

Content-management definition

An exact definition of the content management is difficult to pen down. The reason being, the ambiguities arising out of wide scope of the term "content". Content could be anything from items or elements that provides or helps in provision of meaningful information.

The various components of the content and processes involved in the content management have been dealt in the subsequent parts.

Answer: [c] Both creative and application content

Module:2

Reference No:M2087

Question: The product database forms a part of ----- type of content

- [a] Creative content
- [b] Application content
- [c] Transaction content
- [d] Ancillary web sites

Module 2- Content Management- part 2

Content management

This is the second of a six part series on content management. In the previous article we described the scope of content management and defined the term content.

Components of the term content

There are basically the following components in the definition of the term content:

1. Creative content
2. Supportive content or application content
3. Transactional content
4. Ancillary corporate websites
5. Downloadable files

Creative content

This is the most popular component of the term content and the most visible too. This includes text, graphics, multimedia, ads, and scripts. In other words everything that is found on the web page.

Supportive content or application content

This is the supportive component or the backend component. It includes all those processes and applications that help in the creation and maintenance of an e-commerce website. For instance, the application and software components like programming logic are known as application content. The application content regularly interacts with the creative content and is one of the critical components.

Transactional content

The third type of the content is the transactional content. This is the information that is usually contained within the databases. Examples of transaction content include product catalogues, order databases etc. The transaction content is used to create dynamic web pages, which is transformed into HTML text pages and then delivered to the ultimate customer.

Ancillary corporate websites

These also perform the function of supporting the e-commerce website. For instance some websites have their own customer relationship systems to satisfy the needs of their customers more effectively. These sites also access the same customer information and database or at least a same version. The main issue in the maintenance of such a website is that all the developments in the main website will have to be carefully duplicated in these websites also.

Downloadable files

These could be PDF files, word documents, images or archives or any other type of file.

The process of content management

The process of content management covers the following aspects of website management

- Design
- Creation of content
- Review process
- Approval process
- Data conversion
- Storage management
- Testing and deployment

Once the content has been hosted it needs to be maintained, regularly monitored, updated and eventually retired and archived.

Clearly defined roles and documentation and approval procedures play an important role in the process of content management.

The process flow for four specific types of web sites**1. Process flow for news sites**

In the news site the main emphasis is on providing timely and accurate information to the customers. The website mainly consists of text, images and in few cases the streaming of audio and video.

The process flow in a news site would be as follows:

- Selection of a story

- Designating an author for rewriting
- Editing, review and approval by managers
- Editing the support images, audio and video content
- Presentation of the article
- Provision of links, sidebars and other elements
- Integration and staging by the technical staff
- Testing
- Final approval and hosting on the public site

A fresh news story is hosted on the main page or the home page. Thereafter it is shifted to another column say for instance recent news items and then to an archive and finally it will be removed after it loses its relevance altogether.

The process flow for the remaining three types of web sites has been described in part 3 of three of this series.

Answer: [c] Transaction content

Module:2

Reference No:M2088

Question: The life cycle of news article on news site is ----- than technical article on tech support site

- [a] Shorter
- [b] Longer
- [c] Similar
- [d] Similar or shorter

Module 2- Content Management- part 3

This is the third of a six part series on content management. In the second part we described the process flow for one of the scenarios involving a news website. In this part we will be describing the process flow for next two scenarios in the following areas

- Technical support site
- B2C e-commerce website

Technical support site

In a technical support website the major portion of the content will be in the form of technical information in the text form. The content could be white papers, which are downloadable, codes or information about products, news items etc.

Normally for such a site, the time taken for creation, review, approval and hosting/publishing time for such articles is much longer. Once the article has gone through the initial stages like authoring, editing and approval (for both legal and technical authenticity) it is ready for integration into a web page. The metadata also may be added to enable the search facility. The final article is then formatted using a standard template, in compliance with certain compulsory standards. The next step is staging. And then it undergoes a final testing process. For this it is assigned a URL. After the final testing, it is hosted/replicated onto a public server through an automated process.

The life of a technical article is usually much longer than a news item. And hence may remain at its original

URL for months. For some time it may even be kept updated by the editorial staff to maintain its relevance. Subsequently it is archived and finally retired and moved out of the site. This process may be faster due to lack of reader's interest.

B2C E-Commerce web site

In such websites the main content is product information and information about various deals and retail services offered. The content on the websites can be highly volatile due to frequent changes in the products promoted, offers and price availability and various actions by competitors.

For such websites, it is important to be able to quickly develop and manage such product promotions. Once the decision to promote a product is taken then the product manager needs to co-ordinate with various people to bring the product to the website. Decisions will have to be taken for timing the launch, price details, images and texts to be placed, cross selling offers etc. These decisions affect the developers, creative content personnel and other cross-functional personnel. Any adjustments to the prices will have to be reflected in the product database. If the new product is to be stored in search catalogues, then the catalogues will have to be refreshed.

Once the content is ready and approved, the developers will have to integrate it into the web page. Then the next process of staging, testing and hosting on public website takes place.

The life of such promotion depends on each product. It could range from few days to months or longer.

The process flow for the fourth scenario of application development is given in subsequent part of the series.

Answer: [a] Shorter

Module:2

Reference No:M2089

Question: ----- is the first common function in the content management process

- [a] Approval
- [b] Design
- [c] Testing
- [d] Any of the above

Module 2- Content Management- part 4

This is the fourth of a six part series on content management. In this article we have described the process flow for the application development scenario and the common functions for the content management process.

Application development scenario

Application content is applicable for all types of websites, more so for the e-commerce scenario. Certain organisations use standardised processes for application development.

The standard procedures could include requirements specification stage, design, development, testing and final deployment. Various reviews and approvals are also involved in all these stages. For an e-commerce web site these are normally compressed and expedited. Both unit testing and integration testing are conducted. The unit test is conducted in local mode, which is an isolated environment. The integration testing is done at the staging server. Here the application content and the creative content are brought together and tested.

After the final testing the components are registered and installed on the appropriate servers.

Functions in a content management process

Based on the process flow for the above scenarios we can list a few common functions for the content management process.

Design: This is the first phase in the entire process. In this stage the original content is created. The personnel involved in this stage could be technical writers, advertisers, application developers, photographers etc. For better control, the authored content is usually subject to version management. For this, either document management systems or code management systems are used.

Approval: Formal approvals are required at all stages of content management until the final stage of deployment.

Conversion: Conversion includes transforming the word text documents, images like bitmaps etc. are handed to web development staff. The word documents are converted into HTML pages. For these purposes standard templates, layouts etc. are used.

Storage: Normally file systems or version control systems are used to store the content. Some vendors also offer repositories that can hold any type of content.

Testing: This includes load testing, component testing, script testing, identification of missing links, broken links etc. Access testing of the database and integration testing will also have to be done.

Staging: In some websites there is no difference between the staging server and testing server. However in some large websites staging server and testing servers are different. In such cases once the final testing is over, then the content is assembled and hosted on to the production system

Deployment: Some of the large websites have automated system for transferring the final content to the public live system. Care should be taken that all content including middle-tier application content, transactional content are also pushed to the live system

Updation and maintenance: The data will have to be constantly monitored, kept alive and working.

Archival: Old and stale pages will have to be regularly removed from the public websites. Monitoring process should clearly indicate the stale and unpopular pages.

Analysis: Regular analysis of the site usage and customer profile will have to be done.

In part five of the series we will describe the features of a content management system.

Answer: [b] Design

Module:4

Reference No:M4263

Question: To overcome the employee weaknesses in the security programme -----

- [a] Creating end user awareness
- [b] Training
- [c] Management awareness
- [d] All of the above

Module 4 – Role of employees in IT security

Surprising though it sounds, employees constitute one of the main weaknesses in the security set-up of an organisation. Many of the best security set-ups are threatened not just by experienced hackers but also by naïve employees. Lack of training and end user awareness many a times leads to security breaches.

In order to further strengthen the security systems the employees will have to be educated on security issues. The following methodology will serve the purpose:

- Creating end user awareness
- Training
- Management awareness

To be able to address these issues, a comprehensive audit of the existing security policies and practices is required. This involves getting answers to three basic questions during such audit.

1. Does a security policy exist? If so what is it?
2. Is it possible for the existing security set-up of the organisation to detect security breaches?
3. Are the employees, managers and other specialists of the organisation aware of the steps to be taken in case of security breach?

Each of the components of the above methodology has been dealt in detail below

Creating end user awareness

The auditor needs to obtain an understanding of the end-user computing environment and determine if the users are adequately trained in the usage of the systems. And also the auditor needs to determine if any special circumstances exist like remote users or wireless devices, which warrant additional security requirements. And also the auditor has to verify if the employees are following the security policies in full.

Based on the observations a complete security awareness programme should be charted out. The security programme should consist of easily understandable usage policies. The managers should ensure that all employees are made aware of this programme. The communication method could include posters, actual training or e-mail reminders.

Specialised training

In addition to the basic end-user training, special security training is required for personnel like security staff, remote workers, frequent travellers who use mobile devices. As mentioned earlier, an audit should be conducted to determine the adequacy of such specialised training and effective usage of the same. And based on the observations, the organisation can decide on further strengthening the specialised training programme. In this regard the organisation can also make use of the programmes offered by training vendors.

Management awareness

As is it well known no programme in the organisation is successful without the involvement and support of the senior management. In this regard the auditors as part of their venture should determine if the management could take lead in enforcing the security policy throughout the organisation, support the practices, and are aware of further action to be taken if any security breach is detected.

Following the above three steps of the methodology would ensure that employees are aware of the security practices to be followed and are well informed of further course of action to be taken in case of detection of a security breach.

Answer: [d] All of the above

Question: Who has the authority to delegate the operational responsibility of an organisation's security?

- [a] Data owner
- [b] Senior manager
- [c] Data custodian
- [d] Data user

Module 5 - Layers of Responsibility

Layers of Responsibility for organisation security

Organization security is the responsibility of the whole organisation. Each layer of management has a role to play in organisational security. They need to select the best practices and procedures for the required level of protection. Three layers have been identified according to their functions.

Management clearly defines the goals and objectives of an organisation.

Functional management has a clear understanding about the work of individual departments. They also know the effect of security on the department.

Operational management the last layer in the organisation and are involved in the actual operations of the systems. They have knowledge about the technical information, procedural requirements and system usage.

Data owner, data custodian and the user play specific roles in the organisation's security.

I. Data owner: Data owner is a person generally from the management. His functions include data protection, data usage and classification of data, alteration of classifications and delegating the operational responsibility to the data custodian. He has to carry out all these functions carefully and diligently. In case of any corruption of data, he will be held responsible.

II. Data custodian: The network administrator and other IT department staff perform this role. The data custodian's main duty is maintenance and protection of data . His functions include:

- Data backup creation
- Security mechanism implementation
- Data integrity validation
- Data restoring
- Following security policy, standards and guidelines.

III. User: Operational staff are the users. A user is a person who can access the data to perform his operational duties. His functions include protecting data confidentiality, integrity and availability.

Others include

Senior manager who has the ultimate responsibility of security,
Security professional who act as per the senior manager's directives, and
Auditor who verifies the security practices of the organisation

Essential requirements for effective security

1. Establish a senior level committee to gain senior management attention.
2. Strategic security procedures that can define the security needs. Chief Information Officer and the senior management should together draft these procedures.
3. Business managers should identify the level of protection required.
4. Security administrator must create new system user accounts, implement new security software, test security patches and issue new passwords.
5. Information security specialists should not be given the responsibility of decision-making. Though they have the technical knowledge of security implementation and configuration they are not suitable for decision-making.
6. Security function should be undertaken at all levels of management. It should follow a-down approach. If undertaken at the security administrator level alone, there are chances for improper risk analysis, risk unawareness and funds shortage for security.

Resources, activities, people and practices of an organisational environment affect the success of a company's security programme. Personnel and structure are the key components. Therefore, they should be properly managed.

Personnel: Human errors, frauds and lack of training are the main causes for security failure. Recruiting qualified staff, providing training facilities proper controls over access and detailed job descriptions are some of the preventive measures that can be taken.

Structure: The structure should provide a clear understanding of responsibilities and authority. Job description should be clearly specified. Separation of duties is one technique that circumvents frauds. In this process, one employee is not allowed to perform more than one work. In this way, work performed by one is automatically checked by another.

Answer: [a] Data owner

Module:2

Reference No:M2033

Question: When the company acquires custom made software it enters into a custom software agreement with the vendor. What should company not consider before entering into such agreement?

- [a] Present and future demands of the company
- [b] Contingency plan of the vendor
- [c] Frequency at which the vendor updates the software
- [d] Number of users of the software

Module 2 - Software Purchase Vendor Agreements - Part 1

A company may have modified software that is developed exclusive for the company as customised software. When the company acquires such software it enters into a custom software agreement. The company should never accept the vendors' standard form, as they are would be in most cases, one-sided favouring the vendor.

This is first of two part series on Software purchase - vendor agreements.

In this article we deal with the issues that must be focussed upon when entering into a custom software agreement.

Projecting the needs: When the customised software is purchased the company enters into a license to use the software but does not acquire all the rights related to it. The company before it enters into the agreement should take into consideration the following

- The license must clearly state the exclusive rights if any, the authorised users within the organisation and the location limits.
- The company should take into consideration the present and future demands. Otherwise the company in future would have less negotiating power and the software would become dearer.
- The users of the software should be clearly defined. If the users include subsidiaries or third party like independent contractors or customers mention must be made of such a clause in the license.
- The company may change its software over a period i.e. transit to a new product. In such a circumstance the company would be required to convert data to a new format. The custom software development agreement and license should include this aspect on how to migrate to a new system.
- When the company is transiting to the new software it would be required to give the developer access to the data and software to assist it in transition. This should be included in the license otherwise it would lead to violating the user, trade secret and such clauses in the license.

Updates, modifications and fixes: With the changes in technology the software is also becoming obsolete at a faster rate. What is in demand today becomes antique in a year's time. Therefore the company must before entering into the software must take into consideration the updates, modifications and fixes. The updates, modifications and fixes should be included in the license and must be agreed upon before entering into the agreement. The following should be considered:

- **Periodical updates:** Whether the vendor would market the product to others and update and improve it periodically.
- **Custom created software:** When the software is only being customised for the company then the company would be required to fund all the future developments. In such a case the agreement should have pricing parameter included.
- **Custom-modification to pre-existing software:** In this case the price should be based on the most favoured customer price or any other arrangement as the vendor would already have market for its updates and the company need not fund it for its future development.
- **Custom modification to an earlier version of the software:** The modifications that exist in the present software may not work in the new version. For this the software would be required to be redeveloped to the meet the required modification. Such an arrangement must be included in the agreement.
- **Latest version of the software:** The agreement should not include any clause where the company is obliged to purchase always the latest versions of the software. If this is included it would become a costly affair for the company.
- **Functioning of the software:** In the case of the customised software the company should carefully state the functions required of the software. For example the features of the software, tasks that it should perform, how should the interface look like? The best way to do is ask the vendors to send Request for Proposal (RFP). On the basis of the response it would be easy for the company to frame a contract.

Answer: [b] Contingency plan of the vendor

Question: Custom Software Agreement should include a pre-acceptance performance standard to measure the software's abilities in the contract. Which of the following test is performed to assesses the performance of the software?

- [a] Unit Testing
- [b] Regression Testing
- [c] Load Testing
- [d] Acceptance testing

Module 2 - Software Purchase Vendor Agreements - Part 2

A company may have modified software that is developed exclusive for the company as customised software. When the company acquires such software it enters into a custom software agreement.

This is the concluding part of the series on custom software agreement.

Performance standards: The usual complaint following the installation of software is that it is too slow or it does not function as desired. To overcome this problem it is necessary to include a pre-acceptance performance standard to measure the software's abilities by testing. For this purpose the length of time to complete the task and the hardware that will be used to run the test should be specified. The test to be performed should include

- **Load testing:** The software should be tested with the maximum load that the company would expect. For example if the company expects that 100 employees will access the same network then the test should include 100 employees.
- **Response time test:** The time taken to process the data and go to the next screen is tested. If any test fails the agreement should provide for reporting the problem and further actions needed. It should also provide for the time frame within which the problem should be set.

Warranties: The warranty becomes important as some or the other problem would accompany the software. The warranty should make a distinction between the failures that are critical and the others that are of less importance. In case of critical and the basic essential functions the agreement should provide for an immediate response.

The length of the warranty should also be agreed upon. Usually it is a six-month warranty with an annual maintenance agreement at a specified fee after the initial period. But should be seen that the maintenance agreement includes the same clause as the warranty and that they are not narrowed down. The operations that have not been tested during the warranty period should be specially emphasised in the maintenance. For example, the year-end operations would not take place when the warranty is in existence. They would take place after the warranty period expires. The maintenance agreement should provide for it.

Payments: The agreement will include a payment clause. The payment is usually made at specified intervals i.e. the payments are not made in lump sum. For example a certain percentage will be due on execution with additional payments due on completion of preliminary testing, upon training of the personnel, on delivery of documentation and completion of acceptance testing and the final payment when the software goes live.

Source code: Source code is human readable computer language. Source code is required to make modifications in the software. The company would really be in trouble when the vendor goes bankrupt or if he refuses to cooperate. The vendor would not be ready to give the source code as he considers the same confidential that cannot be shared with others. For this purpose the source code should be kept with third parties with an escrow agreement. According to this agreement when the vendor goes bankrupt or does not exist then the third party will release the source code to the company.

Custom software agreement is a complex area. There can be no standard format for the agreement. They should be tailor made for each company.

Answer: [c] Load Testing

Module:2

Reference No:M2078

Question: Which of the following is not an essential feature of effective computerisation system in a bank?

- [a] Effective customer service
- [b] Effective back office integration
- [c] Focus on manual records
- [d] System should identify the inter branch transactions

Module 2 – Bank computerisation

Introduction

Today most banks are computerised. This is a desirable trend because banks are spread across large geographical areas. The quantitative results of computerisation by nationalised banks though impressive have to be evaluated in the light of qualitative achievements.

An effective computerisation system should:

1. Have an efficient and effective customer service
2. Establish effective controls in the system
3. Aim at effective back-office integration
4. Identify inter branch transactions
5. Possess the required statistical information
6. Link the current, savings, cash and cash credit departments.

Instead of improving customer service computerisation has led to various problems. As a result, customers

1. Have to spend more time in service line
2. Are denied service during system breakdowns even if temporary and the service does not require a system.
3. Do not receive timely periodic statements.
4. Face problems as the staff are unclear about the technology
5. Find wrong balances/entries at the time of closing the books or at the time of computerisation.

Concerns in automation: Advances and inter-branch transactions become the main concern of the bank in the absence of back office integration. Hence, the need for back office integration.

- Sometimes the focus of audit is on manual records. Audit trails are merely a report. This obviates its storage and maintenance.
- Exceptional transactions may be dealt differently in computerised and manually generated reports.
- Absence of back office integration leads to duplication of work.
- Poor system quality may affect input quality
- Absence of standardised software across the branches makes accessing the data difficult.

1. Advances

The advances department is the income-generating department of a bank. Bills, which are a part of the department's products, generate income to the bank in the form of discounts at the time of purchase. These transactions involve complex calculations. Hence, they must be correct. Further, a single system integrating the loan documentation and advance documentation improves efficiency. Effective controls must be established over different products of the advances department. The documentation required by the advances department must be accurate.

2. Inter-branch transactions

Inter-branch transactions are in the form of issue of bank drafts and telex transfers. These have to be reconciled correctly lest problems should arise. Inaccurate reconciliation amounts to fraud which can be revealed by an analysis of the reconciliation items. However, identifying the person responsible for fraud is difficult in the case of an old entry. Therefore, the reconciliation should be made frequently. This can be done by acquiring inter-branch transactions on a magnetic media like floppies and sorting out the variances through the Central computer.

Answer: [c] Focus on manual records

Module:3 Reference No:M3004

Question: The smallest unit of information on a hard disk is called:

- [a] Track
- [b] Sector
- [c] Cluster
- [d] None of the above

Module 3- Hard Disk Drives-Concept

With a lot of data being generated in every organisation it is very important to have backups as a contingency measure. Since primary memory or RAM is an expensive option, secondary memory turned out to be cheaper in comparison, and feasible for holding voluminous data. Secondary storage consists of various kinds of devices. One such device being the *hard disk drive*.

Hard Disk Drives

Hard disk drives or HDD as they are commonly known, are an assembly of various parts. Let us first discuss as to how these parts are internally assembled which would facilitate a better understanding of the working of a HDD.

The Architecture

An HDD consists of a central *spindle* that can rotate in both clockwise and counter-clockwise directions. Over this spindle, multiple platters are mounted that are the actual storage devices. The platters are disc-shaped, usually made of aluminium or glass and has two surfaces covered with a magnetic material. Unlike the flexible media in floppy diskettes, these platters cannot bend or flex, and hence the term hard disk. Another popular term for a hard drive is fixed disk, so called because the platters are fixed firmly in place and are not removable. Spindle is driven by a *motor* and is responsible for its rotation. For every platter, there is a read/write head on either sides, all of which move across the discs at the same time since they are all

connected to one arm called the arm assembly. The movement of the motor and the *arm assembly* are driven by a mechanism that is explained hereunder.

Working

A formatted disk is divided into *tracks and sectors*. Tracks are logical concentric circle that are drawn on the entire circum-area of the platter on each side. Sectors are logical lines that are drawn from the centre of the circular platter extending to its edges. The intersection of the tracks and sectors are *clusters* that are the smallest unit of information that can be read from or written to the disk.

When some data has to be written to the disk, the operating system looks for empty clusters and determines the corresponding tracks and sectors that form the cluster. The platter is then rotated to bring the required sector under the head. Arm assembly then moves forward or backward to reach the respective track. The read/write head then stores the data by magnetising the cluster.

For retrieving the data same procedure is followed the only difference being, instead of looking for empty spaces, the operating system looks for magnetised clusters and matches them with the required data.

Answer: [c] Cluster.

Module:3 Reference No:M3005

Question: With respect to hard disk, seek time is described as:

- [a] Time taken by the arm assembly to reach the respective track
- [b] Time taken by the arm assembly to find the respective sector after the heads have reached the track
- [c] Total time taken to access the data
- [d] None of the above

Module 3 - Hard Disk Drives-Performance

Hard disks form a very important part of any computer system, be it a stand alone PC or a state-of-the-art client/server architecture. They form the basic infrastructure for storing all kinds of data. To improve the efficiency of these data repository, it is important that they are maintained properly. Maintenance is what urges us to know the intricacies of the hard disk drives. Let us study some basic concepts that help in enhancing the performance of a hard disk

Disk Controller

We know that it is the operating system (OS) that drives all the functionalities of the hard disk. But there has to be some interface between the sophisticated technology like the OS and the hard disk. The disk controller performs this job. It takes the high-level commands to read or write data and transforms them into actions resulting in the to-fro motion of the arm or rotation of spindle. It performs a few other functions:

- *Checksums:* When a data is written to the disk, specifically a cluster, a checksum is attached to it. This checksum is computed based on algorithms and depends on the data for the corresponding cluster and stored. At the time of retrieval a checksum is carried again and compared with the stored checksum. If the results match, data is retrieved successfully. In case of a mismatch, controller tries to read several times until it is done successfully. If the error continues, a read failure is reported.

- *Remapping of bad clusters:* With time and use, some of the clusters get corrupt. While reading/writing to the disk, the controller detects it and logically maps the cluster to another location, the address of which is stored in a non-volatile memory.

Performance

Performance of a disk is largely dependant on the time taken to read from or write to the disk. When we talk of accessing data on a disk, we should first understand that a hard disk is actually a collection of logical cylinders. Let us see how. We know that a platter has many concentric tracks. Similarly there are many platters constituting a hard disk. All the concentric tracks falling below one another form a logical cylinder. This concept is useful to understand the time involved in reading/writing data to the disk. Time involved can be divided into two parts:

- *Seek time:* Seek time is the time taken by the arm assembly to reach the respective cylinder i.e. the respective track that holds the data.
- *Latency time:* Latency time is defined as the average time (in milliseconds) taken for a sector to be available after the heads have reached a track.

Hence the total access time can be derived as:

Total access time = Seek Time + Latency Time.

Precautions

By now we have seen that hard disks are of technological and strategic importance to an organisation. But there are instances when even these technological masterpieces become vulnerable to failures. Although the heads are responsible for writing data to the discs, they are never in actual physical contact with the platters. These heads are kept suspended by an extremely thin cushion of air, and thereby float just a fraction of a millimetre above or below the platter. If dust or other small particles ever get into this part of the drive, the head easily comes into contact with the platter and cause physical damage to it. This is called a "head crash". This can corrupt the data which is fatal for the organisation.

Answer: [b] Time taken by the arm assembly to find the respective sector after the heads have reached the track.

Module:3 Reference No:M3006

Question: Given below are major types of storage devices 1) Cache 2) Magnetic -disk 3) Flash 4) Main Memory 5) Tape Storage 6) Optical Storage.

Rank them in the increasing order of their reading/writing capability.

- [a] 1,2,3,4,5,6
- [b] 5,6,2,3,4,1
- [c] 6,5,4,3,2,1
- [d] 2,5,3,1,6,4

Module 3 – Physical Storage Media

Earlier, computer memory was only confined to two small acronyms, RAM and ROM. But with rapid growth of business, data storage became quite a job. This apart, the stored data is of no use unless it can be retrieved

at the right time. Various types of storage devices came into existence with an aim to reduce the cost of storage and increase the speed of accessing the data. Let us now see the different types of storage devices available:

Cache Memory

It is the fastest and costliest form of storage device. It is a very small piece of chip and is managed directly by the operating system. They work on a very basic principle. The piece of data that is used frequently by the user is stored here. Hence when the user requests for the data, it is retrieved at a much faster rate. For example, a web browser cache stores the pages, graphics, sounds, and URLs on the hard drive so that when these pages are accessed again, they need not be downloaded all over again.

Main Memory

This is nothing but the PC's primary memory. The complete functioning of the system depends upon the machine instructions that are written on a small segment of the memory. This forms the backbone of all the computer functions. It is next to cache in speed, but is not large enough to store an entire database. Main memory is volatile which means the contents are usually lost in case of a power failure or system crash.

Flash Memory

This is called the **E**lectrically **E**rasable **P**rogrammable **R**ead-**O**nly **M**emory or the EEPROM. Since it is non-volatile, data is not lost in case of a power failure or system crash. Its cost per unit storage is roughly the same as compared to main memory as is the accessibility. Writing data is more complicated in the sense that data can be written only once for a location. Also, in order to overwrite, the previous data has to be erased first and only then fresh data can be mounted on top of it. EEPROM supports only a limited write/erase cycles.

Magnetic-disk Storage

This is the most extensive among all the storage devices and easily the most popular. It is the primary medium for holding long-term data and stores the entire database. Data is magnetically stored on a rotating disk with the help of read/write heads. Data on magnetic disks cannot be directly accessed but has to be moved to the main memory. Moreover, only sections of the data are moved to the main memory depending on its size. This results in much slower access of data as compared to main memory. It is a direct-access device thus making it possible to retrieve the data in any order. This again is a non-volatile memory and can survive power failures.

Optical Storage

This is also one of the most popular forms of storage. CD-ROM (Compact Disk-Read Only Memory) or the DVD are devices that apply the concept of optical storage. Data is stored optically on the disk with the help of laser beams. When the beam strikes the surface, a pit is formed which denotes the presence of data. When the head encounters a pit, a data patch is recognised. A clean surface denotes no value. As the name suggests, CD-ROM does not allow data to be written on it. On the other hand WORM (Write Once Read Many) also do not support data to be re-written on them with the difference that while CD-ROMs are provided by the vendors, WORMs can be used by a common user to store data. It's reading and writing capabilities are slower than the magnetic disk.

Tape Storage

It is a non-volatile memory used primarily as backups for archival data. It is a sequential access device, because to reach a particular data at any location, the user must first scroll through the entire preceding block of data. It is the slowest in reading/writing capabilities when compared to the other devices.

Answer: [b] 5,6,2,3,4,1

Module 7:3 Reference No:M3007

Question: A scanner with 36-bit depth gives the output in:

- [a] Less than 36 colour depth
- [b] More than 36 colour depth
- [c] Depends on the document being scanned
- [d] 24 bit depth only

Module 7 - Scanner

The scanner basically analyses and processes an image. Optical Character Recognition (OCR) allows this information to be saved in a file on the computer.

Different parts

Charge- Coupled Device (CCD) array	Mirrors	Scan head
Glass plate	Lamp	Lens
Cover	Filters	Stepper motor
Stabilizer bar	Belt	Power Supply
Interface port(s)	Control Circuitry	

The most important part of the scanner is the CCD array, which is commonly used for capturing an image. It is a collection of tiny light-sensitive diodes, which convert photons (light) into electrons (electrical charge). These diodes are called photosites. Each photosite is sensitive to light—the brighter the light that hits a single photosite, the greater the electrical charge that will accumulate at that site. The CCD array receives the image of the document through a series of mirrors, filters and lenses.

Working

The document is placed on the glass plate, and closed in by a cover plate. This provides a uniform background, which the scanner software uses as a reference point for determining the size of the document being scanned. Although some types may allow the cover to be removed, for scanning a bulky object.

- The document is illuminated using a lamp, which is a Cold Cathode Fluorescent Lamp (CCFL), a Xenon lamp, or a standard fluorescent lamp (in older scanners).
- The scanning process is done by the scan head, which consists of mirrors, lens, filter and a CCD array. The scan head is moved slowly across the document by a belt that is attached to a stepper motor. It is also connected to a stabiliser bar to ensure that there is no wobble or deviation in the pass (a single complete scan of document).

- A mirror that is placed at an angle to another mirror reflects the image of the document. In some scanners, there are only two mirrors, while others use a three-mirror approach. Each mirror is slightly curved to focus the image it reflects on to a smaller surface.
- The last mirror reflects the image onto a lens, which in turn focuses the image through a filter on the CCD array.
- The filter and lens arrangement varies based on the scanner. Some scanners use a three pass scanning method. Each pass uses a different colour filter (red, green or blue).
- Most scanners use the single pass method. The lens splits the image into three smaller versions of the original. Each smaller version passes through a colour filter (either red, blue or green) onto a discrete section of the CCD array. The scanner combines the data from the three parts of the CCD array, into a single full-colour image.

Resolution and interpolation

The resolution and sharpness of the machines differ. Most scanners however have a hardware resolution of 300x300 dots per inch (dpi). The scanner's dpi is determined by the number of sensors in a single row (x-direction sampling rate) of the CCD array, by the precision of the stepper motor (y-direction sampling rate).

Sharpness depends mainly on the quality of the optics used to make the lens and the brightness of the light source. A bright xenon lamp and high quality lens will provide a much clearer, and therefore sharper image, than a standard fluorescent lamp and basic lens.

The scanning software can increase the resolution of an image by a process called **interpolation**. This is done by creating extra pixels in between the ones actually scanned by the CCD array. These extra pixels are an average of the adjacent pixels. For example, if the hardware resolution is 300 X 300 and the interpolated resolution is 600 X 300. Then the software adds one pixel between those pixels scanned by a CCD sensor in each row, to make the final count of 600 pixels.

The number of colours that the scanner is capable of reproducing is termed bit depth or colour depth. Each pixel requires 24 bits to create standard true colour, and scanners available in the market generally support it. Even though some models offer bit depths of 30 -36 bits, they can give an output of only 24 bits, but can perform internal processing to select the best possible choice of the colours available in the increased palette.

Answer: [d] 24 bit depth only

Module:3 Reference No:M3008

Question: Which of the following statements is true with regard to Operating Systems (OS)?

- [a] It may allow many users to operate simultaneously.
- [b] It can run on systems with different memory and storage space after minor changes.
- [c] It takes control of the computer as soon as the power is turned on.
- [d] The user can customise RTOS (Real Time Operating System) by making changes to the interface.

Module 3 - Operating System

An Operating System (OS) is the software that enables applications to run. It organises and controls the hardware devices attached. An OS in its most basic form performs two functions.

It manages the hardware and software system resources such as the processor, memory, disk space and the like. Various programs and input methods require memory, storage and input/output bandwidth in the Central Processing Unit (CPU). The OS takes care of all these things, and allocates the necessary resources, while taking care of other applications and users.

It allows applications to interact with the hardware by providing a consistent application interface. Such an Application Program Interface (API) allows the software developer to write an application on one computer, which can be also run on other computers of the same type, even if the memory, quantity of storage, processor et al. differ. The OS manages the hardware and software and hence enables the applications to run even if the computer is unique.

The OS can be classified into four types.

Real Time Operating System (RTOS): It is used to control machinery, scientific instruments and industrial systems. It has very low user interface capability and no end user utilities, since the system comes as a "sealed box" when delivered to the user. The main job of the RTOS is to manage the resources of the computer so that a particular operation takes precisely the same amount of time, whenever it is executed.

Single User, Single Task: It is designed for a single user to carry on a single task at a any point of time. The palm OS is an example.

Single User, Multi Tasking: This equips the user to carry out more than one task such as writing in notepad, painting, accessing email and the like, simultaneously. Windows XP and Mac OS X are examples.

Multi User: It enables simultaneous sharing of resources by multiple users . It ensures that the requirements of various users are taken care of, and that each program has sufficient and separate resources so that a problem with one user does not affect the entire community of users. Examples are Unix and mainframe operating systems such as MVS.

Loading Of OS

When the computer is turned on, it is only capable of finding the BIOS ROM (Read-Only Memory) chip that is on the main board. This board has a programmed chip that finds various expansion slots, ports, drives, and the OS.

- The computer begins the start up process also termed the boot sequence, by loading the program code and instructions on the BIOS chip into memory, and then carries out the instructions in order.
- It checks all the devices attached to it, both internally and externally, and performs several self-tests.
- It looks for the video card, loads its information and drivers into Random Access Memory (RAM), then looks for any other cards in expansion slots and loads their configuration into memory.
- The BIOS program then does a simple memory check count.
- It then sets up divisions of memory that hold the operating system, user information and applications.
- The information gathered is compared with the information stored in the Complementary Metal Oxide Semiconductor (CMOS) chip's set up program.

In case of discrepancy the boot process is halted, and the operator is informed of the same.

The computer now tries to locate the OS. By default, it first scans the floppy drive. If a floppy is present, then it must have a copy of the OS system files that is then loaded into RAM. If it doesn't have the files, then the computer halts to display an error message. In the absence of a floppy, the computer checks the hard drive, and loads it into the memory, once it is found.

Answer: [a] It may allow many users to operate simultaneously.

Module:3 Reference No:M3009

Question: Embedded Systems make use of software called -

- [a] Middleware
- [b] Shareware
- [c] Firmware
- [d] None of the above

Module 3 – Embedded Systems

Introduction

Most of us flick the TV on and surf channels without even giving a thought to how we are able to switch between the funky George Michael and our very own Asaram Bapu just by sitting at a distance and pushing a button. Today, we can even restrict children from viewing certain channels with the help of passwords.

This brings us to the next question. How are these systems so smart? Even though they are not as sophisticated as a PC, they are intelligent enough to perform certain tasks that they are programmed to do.

Concept and Working

All embedded systems make use of either a microprocessor or a microcontroller that acts as a brain. The software for the embedded system is called Firmware and is written in Assembly Level Language or Middle Level Languages like C or embedded C. Since they perform certain tasks, these programs are stored in Read Only Memories (ROMs). Moreover they may need only minimal inputs from the user and hence a user interface like monitor, mouse or keyboard may be absent. Embedded systems are also known as Real Time Systems since they respond to an input or event and produce the result within a guaranteed time period. Real Time Systems are classified into two parts:

- *Hard real time systems:* They are systems that complete the specified task within a stipulated time frame. A failure to do so is considered as a failure of the system.
- *Soft real time systems:* These are systems that are not so rigid. Not completing a task within the specified timeframe is pardonable, provided it does not affect the overall system performance.

A real time system may perform certain tasks that require decision loops. For this RTOS or Real Time Operating Systems are used. RTOS help schedule and execute tasks based on priority in a predictable manner and hence it is multithreaded.

Embedded Systems perform a variety of tasks from dispensing of cool drinks by an automatic vending machine to controlling an aircraft. Let us take the typical example of an embedded system that controls a printer. This system has to execute complex functions like checking for paper availability, printer ink, paper jam, and communication with host computer, etc.

Applications

The application of embedded systems extends to many areas Aircraft, Air-conditioning systems, Alarm systems, Automatic Vending and Teller Machines, Traffic control systems, Automobiles, home appliances,

toys, musical instruments, satellites, biomedical equipment, telecommunication equipment, lifts, answering machines, palm tops, pocket PCs, Digital organisers, Digital Personal Assistants (DPA), etc. are few of them.

Conclusion

Internet Technology has enabled the rapid growth of Embedded systems. Today, we are talking about Intelligent Refrigerators which will check your stocks, dial the departmental store and place an order for your grocery and provisions, check the shelf life of your frozen foods and discard expired food, etc. We can even envisage the "Smart House" where electronic systems interact with each other to make life more comfortable.

Answer: [c] Firmware.

Module:3 Reference No:M3016

Question: In a two-tier client server architecture, the client is called-

- [a] Fat client
- [b] Thin client
- [c] Very thin client
- [d] None of the above

Module 3 - Client Server Architecture

Earlier networks used *file-sharing* architecture when a server downloaded files from a shared location to the desktop. The requested user task is then performed in the desktop environment. The drawback with this is that when a particular data is requested, the entire file holding relevant data is sent instead of just the required piece of data. The architecture thus had a huge flow of traffic and worked well only when the usage was low with a maximum of 12 users attached to the structure. With speed being an important criterion, the client-server architecture came into existence.

Client Server Architecture

The Client-server architecture is a very efficient and safe means of sharing database information in a multi-user environment. The file server is replaced by a database server that responds to queries for information or resources made by clients. This server, using a DBMS, answers user queries and allocates responses instead of performing the total file transfer. The client server architecture also allows multi-user updating from a GUI front-end to the shared database. There are different kinds of client server architectures.

Two-tier architecture

A two-tier architecture has a client and a database. The client makes a request to the database that responds accordingly. All the applications and the required software is stored at the client end and hence called a *fat client*. The database stores all the required data to be used by those applications.

Three-tier architecture

In a two-tier architecture, any software that has to be installed is done separately on all the systems that are connected to the network. This could be a costly affair. The limitation was worked on and the three-tier architecture has a middle-tier used to store applications and other software. Thus, while the presentation

logic i.e. the GUI is stored at client side, application logic is stored in the middle-tier with the database server as backend. The clients in a three-tier architecture are thus called *thin clients*.

N-tier /Multi_tier architecture

With Internet gaining popularity, three-tier architecture has also become obsolete. The problem under a three-tier architecture was that the presentation logic had to be stored at the clients end. Therefore, all web pages that interacted with the backend server had to be at the client side. This was not possible. Systems designers then felt the need for a mechanism that would store the entire presentation logic in a separate layer. This is how the n-tier architecture came into being. The N-tier architecture includes another layer that is used to store the presentation logic. In Internet jargon, the client is the web browser, the web server containing web pages becomes the presentation layer, and the application logic is in the application layer with database server as the backend. Clients in such architecture are called *very thin clients*.

Answer: [a] Fat Client

Module:3 Reference No:M3019

Question: The primary difference between a buffer and a cache is in terms of _____

- [a] Memory space
- [b] Temporary storage
- [c] Process speed
- [d] Operational level

Module 3 - Buffers

In a computer system there is frequent transfer of data between peripherals and the CPU. Since, the CPU and the peripheral components function at varying speeds, there is a frequent mismatch between these devices. This results in a bottleneck. Data gets stuck and no transfer actually takes place. A temporary storage area in the RAM solves this problem.

What is a buffer?

A data area that is shared by hardware devices or program processes that operate at different speeds or at different sets of priorities are termed as a buffer. In the context of programming, buffering is the need to screen data from the location it is finally intended for. This enables editing and processing of data before it is moved to a regular file or database.

Principle

Buffers act as holding areas, enabling the CPU to manipulate data before transferring it to a device. The size of a buffer and the algorithms used for moving data into and out of the buffer are main considerations for an effective buffer design. A buffer acts as an "interface midpoint holding place" playing no role to accelerate the speed of an activity. The processes of reading and writing data to a disk are relatively slow. Due to this, many programs keep track of data changes in a buffer and then copy the buffer to a disk. In the case of a word processor it employs a buffer to keep track of changes made to files. Then as the file is saved, the word processor updates the disk file with the contents of the buffer.

Common applications

- Buffers find extensive usage in printing documents. When a PRINT command is issued, the operating system copies the document to a print buffer. The printer thus prints the document at its own speed. This way the computer is made free so that other tasks are performed and the printer runs in the background. This print buffering is known as spooling.
- Many keyboard drivers contain buffers that help in editing type errors before sending the command to a program.
- Some operating systems like DOS use a disk buffer to temporarily hold data that has been read from a disk. The disk buffer acts as a cache.

Cache

The difference between a cache and a buffer has to be understood since a disk buffer can act as a cache in operating system applications. The primary purpose of a buffer is to coordinate communication between programs or hardware. Cache is concerned with improving process speeds. A cache is a place to store something temporarily. Computers use caches at different levels of operation as cache memory and disk cache. Caching is done for the Internet content by distributing it to multiple servers that are periodically refreshed.

Some of the commonly encountered caches include:

- Web browser's cache, which contains the most recent Web files that have been downloaded. It is physically located on your hard disk.
- A disk cache that contains a copy of the most recently accessed data and most likely to be accessed data stored for faster access.
- RAM itself is considered as a cache for data that is initially loaded in from the hard disk.

Answer: [c] Process Speed.

Module:3 Reference No:M3028

Question: Which aspect of storage management incorporates redundancy into the system to maintain performance:

- [a] Scalability
- [b] Performance
- [c] Reliability
- [d] Manageability

Module 3 – Storage Management

In today's information driven environment, an organisation's success is gauged by its ability to store and manage huge amount of information. Storage systems have become a critical part of an organisation's network infrastructure and with data growing at an incredible rate; organisations felt the need to have a storage strategy in place. A good storage strategy must include the right technology and implement solid backup procedures. Here we will explore the critical issues related to data storage in a network and the goals that a storage management system is expected to achieve.

Storage Strategy Design Issues

Technology cannot solve all the issues that have an impact on the organisation's storage strategy. Several factors come into play while selecting storage options. Here we will discuss the basic concerns relating to storage strategy.

Capacity

Storage system must be able to handle the appropriate quantity of data. While designing the storage strategy, the system analyst should be aware of the organisation's storage needs and expected rate of growth.

Scalability

Storage technology must match well with the overall size of the organisation's data needs. Storage strategy implemented when the organisation's network is relatively small often cannot be expanded beyond a certain point. Similarly, large-scale enterprise networks may be burdensome for a departmental LAN. From the very beginning, the storage systems must be designed to scale larger data capacities so that the need is met without any difficulty when it actually arises.

Costs

The least expensive approach that is able to meet the objectives must be selected. Cost issues like the initial purchase cost of the hardware, productivity cost related to the network downtime when the database is being installed, personnel cost associated with each technology option and the like must be considered. Complex solutions will demand time and attention of network administrators, technicians and operators that would add to the overall cost of implementing the solution.

Performance

Storage technology must be able to deliver the information to the user as quickly as possible. Designing a storage solution for a relatively small number of users is relatively simple but networks with an extremely large number of users poses challenges to network administrator to design a system that can handle queries at an extremely high rate and still deliver rapid access.

Reliability

Small-scale networks may be satisfied with a data system that can potentially fail, provided it can be restored with little or no data loss within a reasonable time. It is simple to have a system that is available 99 percent of the time but it is the marginal 1 percent that involves all the complexities and costs a fortune. To achieve this one percent organisations go in for redundancy so that there is no downtime.

Manageability

Once a storage system has been designed and implemented, the organisation must maintain it. System administrators aim for systems with the simplest operational concerns. As systems increase in complexity it becomes increasingly important to be able to monitor their performance, anticipate failures and manage storage media with as little effort as possible.

Answer: [c] Reliability.

Module:3 Reference No:M3033

Question: Which of the following employs client-server computing?

- [a] Interactive multimedia
- [b] Networked multimedia

- [c] MPEG video
- [d] Virtual reality

Module 3 - Multimedia

Introduction

Music and dance have always been a popular source of entertainment. The introduction of silent films with a background score marked the beginning of multimedia. Multimedia is a form of communication that uses more than one type of media.

What is meant by multimedia?

To be precise, more than one simultaneous presentation medium is termed as multimedia. A combination of text, sound, and motion picture is called as multimedia application. Examples are a CD-ROM, websites and the like. These various media types are stored in a digital form. They are presented by using a language like HTML (Hyper Text Mark up Language) or CD ROMs.

Interactive multimedia

The scale of production of a multimedia application differentiates it from typical motion pictures, which are expensive and consume much storage space. The scope for user or audience interactivity and involvement with the application led to the development of a subset of multimedia called interactive multimedia. Interactive medium includes mouse manipulation, voice command, touch screen, text entry, video capture of the user, or direct live participation. Here the delivery of the service is based on decisions made by the user at the time of viewing the application. Interactive multimedia programming aims at providing greater flexibility of choice for the end user.

Networked multimedia

The rapid growth in client-server computing has led to the usage of a wide range of business computing applications involving multimedia. The multimedia industry consists of four tiers.

- The top tier consists of the multimedia content providers. These include the news industry, the television industry, and the entertainment industry. The multimedia content providers are using network as a platform for delivering their content to a larger set of consumers and are also engaged in producing multimedia CD-ROMs.
- The second tier constitutes the multimedia application developers. Applications like multimedia kiosks, e learning, distance learning, desktop videoconferencing, workgroup collaboration, edutainment, and imaging.
- The third tier comprises the multimedia platform builders. Many hardware vendors and companies like Intel, Apple, Silicon Graphics, and Sun are delivering multimedia-capable computers.
- Network infrastructure occupies the fourth multimedia industry tier. The two different networking environments that use multimedia applications are present day's business networks and the emerging public networks. Networking of multimedia initially was confined to businesses over the private networking infrastructure. Now the requirement is for multimedia applications across public networks like Internet for home, education, business, and entertainment.

Bandwidth

A wide range of bandwidth requirements arises for multimedia applications of today. The bandwidth that is required is strongly affected by the size of the frame, the frame rate, and the quality of the image. The video encoding scheme that is used determines these factors. Following are some of the data rates for typical multimedia applications:

- 64 kbps -- Telephone-quality audio
- 100 kbps -- Simple application sharing
- 128 kbps to 1 Mbps -- Videoconferencing
- 1.54 Mbps -- MPEG video
- 8 Mbps to 100 Mbps -- Imaging
- Greater than 100 Mbps -- Virtual reality.

Answer: [b] Networked Multimedia.

Module:3 Reference No:M3036

Question: Which of these enable a super computer's CPU to share operations for enhanced performance?

- [a] Pipelining
- [b] Parallelism
- [c] RISC (Reduced Instruction Set Computing)
- [d] SMP (Symmetric Multi Processing)

Module 3 - Super computers

What are Super computers?

Computers designed for specialised mission critical scientific applications that are concerned with massive amounts of mathematical manipulations are called super computers. The term, 'super' refers to inherent features of the system like high speed and high processing and storage capacities. These are the fastest and most expensive computers in the market today.

A Distinguishable Feature

A supercomputer performs dedicated processing of a small number of applications at ultra speeds. However there are certain limitations with respect to the number of programs that can be processed at any given time. This is not the case with a mainframe computer, which is capable of executing a large number of programs simultaneously.

Structure

Two basic parts of a supercomputer are the CPU and the memory. The CPU is concerned with the execution of commands that it needs to process. The memory is for storing data. The line of demarcation between ordinary PCs and super computer lies in the fact that CPUs in super computers run at much faster speeds because of state-of-art technologies and superconductor circuits that are used.

Design types

There are two main kinds of supercomputers namely vector machines and parallel machines. They perform the same functions but differ in the way processes work.

There are two processes aimed at enhancing the performance of the system to work at optimum levels. They are:

- *Pipelining*: It accomplishes complex operations at the same time by grouping the processes in an orderly manner. Once, the processes are grouped the calculations are done and sent in the priority which was set. The CPU continuously performs operations on a continuous basis.
- *Parallelism*: Calculations are performed in a similar manner rather than in an orderly way. Various operations are done simultaneously and step-by-step processing takes place. This is brought about by connecting several CPUs together, so that they perform calculations collectively.

Most supercomputers make use of parallelism or pipelining separately or can even combine them. Several machines are connected together to attain a high level of parallelism. Massive parallel processing supercomputers command a higher demand and usage in the market due to mission critical operations.

Technology drivers

Clusters of Reduced Instruction Set Computing and RISC-based Symmetric Multi-Processing (SMP) nodes connected by fast networks are gaining usage. This is considered as a natural architectural evolution. The ready availability of relatively low-cost (RISC) processors, network products and standardised communication software has enabled the development of super computers for relatively low-end functions.

Applications

Some typical real-time mission critical applications include:

- Weather forecasting
- Animated graphics
- Fluid dynamics calculations
- Nuclear energy research
- Petroleum exploration
- Space expeditions
- Defence/Military research

Answer: [b] Parallelism.

Module:3 Reference No:M3047

Question: The Fibre Distributed Data Interface (FDDI) is a dual ring LAN that uses a fibre optic cable. The ring is segmented when -

- [a] One ring fails
- [b] One station fails
- [c] Two rings fail
- [d] Two rings fail

Module 3 - Fibre Distributed Data Interface (FDDI)

The FDDI is a dual ring LAN connected using a fibre optic cable with a capacity of 100Mbps token passing. FDDI consists of dual rings - one primary and the other secondary. This allows data to flow in opposite directions. The dual ring gives superior reliability and robustness.

Mode of Transmission

Fiber optic cables are used as the transmission media in FDDI cables. This gives increased security, reliability and performance, as the fibre doesn't emit electrical signals like copper cables.

Two types of optical fibres used for this purpose -

- **Single Mode:** It allows a single ray of light at a particular angle to travel through it.
- **Multi Mode:** It allows multiple rays of light to travel. It uses LED (Light Emitting Diode) as a light source.

Specifications

FDDI is a combination of four specifications.

Media Access Control (MAC): It specifies the method by which the medium is accessed, the frame format used, algorithms accessed for calculating token handling, Cyclic Redundancy Check (CRC) value, addressing and error-recovery mechanisms.

Physical Layer Protocol (PHY): It deals with data encoding/decoding procedures, framing, clocking requirements etc.

Physical Medium Dependent (PMD): It specifies the characteristics of a transmission medium such as fibre optic links, power levels, bit error rates, connectors and optical components.

Station Management (SMT): It specifies the FDDI station configuration, ring configuration and control features, including station insertion and removal, initialisation, scheduling, statistics collection, fault isolation and recovery.

Station - Attachment Types

A unique characteristic of FDDI is that it facilitates many ways to connect FDDI devices. There are four types of devices.

Single Attachment Station (SAS): SAS connects to the primary ring through a concentrator. The benefit is that the device when not connected with the FDDI ring or when switched off will not affect the ring in any way.

Dual Attachment Station (DAS): It connects FDDI through two ports. These ports are connected to the dual ring and therefore connect both primary and secondary rings. Devices connected through this when disconnected or powered off affect the rings.

Dual Attached Concentrator (DAC): It is directly connected to primary and secondary ring. Its main function is to avoid breakdown of the ring due to failure and power-down of any SAS. This is helpful in devices such as PCs which may be powered on and off every now and then.

Fault Tolerance

FDDI has a number of fault tolerant features such as dual ring, implementation of optical bypass switch, dual homing support that makes FDDI a resilient technology.

Dual Ring: The main advantage of FDDI is the dual ring. FDDI continues to operate even if there is a station failure or cable failure. Whenever any of the above failures occur, the station or devices on either side wrap up into a single ring and continue to transmit data. FDDI provides fault tolerance only to single failures and when more than two occur the whole ring is divided into different rings and this makes it impossible to communicate.

Optical Bypass Switch: This helps in maintaining the communication even if there is a device failure. This is done by passing light using optical mirrors directly to a DAS device during a normal operation. When a device failure occurs, the optical switch will pass the light using internal mirrors. This avoids wrapping condition. Optical bypass switches may create unnecessary digressions.

Dual Homing: It is used to guarantee smooth operation and provide redundancy. For this, a critical device such as a router or a mainframe host is attached to two concentrators. One is declared as the active link and the other is a passive link. The passive link stays in backup mode until the primary link is determined to have failed and when it does fail, the passive link activates automatically.

Answer: [b] One station fails

Module:3 Reference No:M3048

Question: Steganography is the art of dealing the data by -

- [a] Hiding it to make it necessarily invisible and not easily detectable.
- [b] Hiding but not necessarily invisible and not easily detectable.
- [c] Detecting and destroying the hidden data.
- [d] Only encrypting it.

Module 3 – Steganography

Steganography can be defined as the art of hiding data in other harmless source in such a way that it is not easily detectable. Derived from Greek, steganography means secret writing. A simple example of steganography is the image or watermark that appears on bank notes when held against the light. Steganography can be implemented using a number of techniques such as invisible ink (based on fruit juice, milk and so on; it darkens when heated and becomes clearly legible), microdots, digital signature, covert channels and spread-spectrum communications, text, images, sounds, signals and the like.

Some of the terms used in steganography are:

Cover: It refers to the original harmless message, data, audio, still, video and the likes. For instance when data is to be transmitted through audio signal, the cover signal is called "host" signal.

Embedded: The data hidden inside the cover is called embedded.

Stego: It refers to the data, which contains both the cover signal and the embedded information.

Embedding: It is the process of hiding the data into the cover data.

Container: The cover image in image steganography is referred to as Container.

Use of steganography in different media

The message being hidden under the cover need not compulsorily be encrypted. But if encrypted, it has the advantage of an extra layer of protection to the data. The Kerckhoff Principle in cryptography states "the security of the system has to be based on the assumption that the enemy has full knowledge of the design and implementation details of the steganographic system". The only missing information is the secret key without which it would be very difficult to even suspect that on an observed communication channel, hidden communication has taken place.

Following points should be taken care of when embedding data in a cover data -

- The embedded data should be unnoticeable to the extent possible and should not distort the cover data.
- The data should not be stored in header or wrapper but in to the media in which data is to hidden that could be text, audio, video and the like so as to maintain consistency across formats.
- The embedded data should not be affected by modifications from intelligent attacks or manipulations such as filtering and resampling.
- Error correction codes should be used so that when cover data is modified distortion can be easily traced and rectified.
- The embedded data should be self timed or arbitrarily re-entrant. This means if only a part of image or sound file is available, even then the hidden embedded data with in the file will be available.

Steganalysis

While steganography deals with hiding the data behind the cover so as not to be discovered Steganalysis deals with discovering the data, which is embedded in, cover data and then making it ineffective.

The embedded message can be attacked in two ways: one is detection and the other is destruction.

Answer: [b] By keeping it visible but not easily detectable

Module:3 Reference No:M3052

Question: The 'Resolution power' of a Printer measures its:

- [a] Speed
- [b] Quality
- [c] Type
- [d] Memory

Module 3 - Printers-Overview

Printers are hardware devices used to generate hard copies (data in a printed format) of documents. Printers are used extensively in offices and homes.

Types of printers: Printers are divided into two categories: -

- 1) Impact printers.
- 2) Non-impact printers.

Impact printers: Printers that print by making physical contact with the paper. For example

- **DOT Matrix Printers:** Have a moveable print head with pins that strike the ink ribbon creating a dot on the paper. A number of dots are combined together to form a text or graphic. The print quality of these printers is poor.

- **Plotters:** These printers use a pen to draw a graphic or image on a paper.
- **Thermal printers:** These printers use electrically heated pins to burn an image on a heat sensitive paper, coated with a special material.

Non-impact printers: These printers do not make any physical contact with paper while printing. For example

- **Inkjet printers:** They print by squeezing quick drying heated ink through a syringe like needle. Inkjet printers are commonly used for colour printing. The print quality is good. The drawback of an inkjet printer is that it requires high maintenance, it is slow and it cannot be used for heavy-duty printing.
- **Laser printer:** These printers use laser technology for printing. The laser beam recreates the image on a negatively charged drum that attracts the positively charged ink. Since the paper is negatively charged, the ink is attracted towards it and fixes itself on paper. Laser printers are gaining popularity and are used in offices. Advantages include fast speed, high print quality, low maintenance cost, and high durability. Laser printers are however not used for colour printing as they can be rather expensive.

Characteristics of a printers

1. **Print quality:** Printer quality is rated in terms of its resolution power which is measured in terms of dots per inch (DPI) (number of dots that a printer creates per square inch of paper). The higher the DPI, the better the resolution and print quality. A 300 X 300 DPI printer prints 90,000 dots per square inch. 300 DPI is considered as moderate printing quality and 2400 DPI is regarded as the best.
2. **Speed:** The speed of the printing process is very important in order to minimise the waiting time, especially in offices where multiple users share the same printer. There are two things that affect the overall speed of the printer: -
 - **Warm-up time:** The time taken by printer to start printing after the print command is issued. Less warm-up time means better printer performance.
 - **Pages per minute (PPM):** The number of pages that the printer can print per minute. PPM for a Laser printer can range from 6-24.
3. **Printer memory:** Printers also have memory, used to store print jobs in a sequence while the current job is underway. This also saves time because the user can simply give the command and continues his work without having to wait for the completion of a previous print job.

Answer: [b] Quality

Module:3 Reference No:M3053

Question: In a Mouse, there are three rollers that can rotate. How many rollers are actually responsible for the movement of the curser?

- [a] One
- [b] Two
- [c] Three
- [d] None

Module 3 – Mouse-Overview

The input device called the 'Mouse' is a popular and convenient tool and performs a function that is analogous to pressing the enter key.

History

Douglas Englebart was the first person to design the Mouse in 1964. The original Mouse was a wooden box like structure and gained popularity in test groups because it was easy to handle and gave more accurate results than trackballs or joysticks. The first PC vendor to feature the one button mouse was Apple Macintosh (1984), which gained immense popularity in the market. Although Microsoft had launched PCs with the Mouse in 1983, it was not implemented on the windows operating system and hence customer in the market did not adopt it.

Operations

The Mouse we are using today works by tracking the movement of a ball located on the underside, which rolls against the surface. There are usually three rollers inside the mouse: -

- A roller for horizontal direction.
- A roller for vertical direction.
- A spring-loaded tension roller.

The mouse ball is always in contact with two rollers- Horizontal and vertical, each moving in a different direction. As the mouse moves over the surface, the data collected from rollers is sent to operating system via the mouse port (this moves the cursor all over the screen).

The biggest drawback in using a mouse is that, the rollers gather dust particles while the mouse ball moves over the surface. This makes the cursor to get stuck at a particular position on desktop.

This problem can be dealt in two ways: -

- Cleaning the Mouse regularly
- Use of sophisticated technology.

Similar devices that have gained popularity are-

- **Optical mouse:** It uses a low intensity light source located at the bottom, which shines on a mouse pad specially designed for this purpose. This imprints a grid of lines. The Mouse reads the movement of light, as it reflects back from the pad surface. Based on this, the position of the cursor is changed on the monitor.
- **Honeywell mouse:** Developed by Honeywell, it is now manufactured by Key Tronic under the name Key Tronic lifetime mouse. This mouse has two oblique disks that are used to determine the movement of cursor in the vertical and horizontal directions.

Both these devices don't allow dust particles to enter, and hence they are more reliable.

Mouse specifications

1. **Cord length:** The standard length of a Mouse cord is 2 meters. It should not be less than two meters.
2. **Resolution:** The Resolution is the smallest movement that the mouse can identify. It is measured in Dots Per Inch (DPI). For example a 400 DPI mouse can detect a movement as small as 1/400th part of an inch. The standard DPI range of a mouse is between 350 DPI and 600 DPI. Higher DPI implies that the mouse is more sensitive to cursor movement.
3. **Number of buttons:** Usually a Mouse used for the windows operating system has two buttons. The Macintosh operating system Mouse has one button. Sometimes there is also a third button. Depending upon the application that is being used, the user can select the most appropriate mouse.
4. **Interface:** A Macintosh mouse uses ADB (Apple Desktop Bus) interface, and a Windows Mouse uses a 9-pin serial port interface. One should select a mouse depending upon the interface he/she is using.

5. **Mouse pad:** The quality of the mouse pad also determines the mouse movement and reduces dust accumulation. The surface of pad should be covered with firm and smooth plastic

Answer: [b] Two

Module:3 Reference No:M3069

Question: Which of the following image formats is for the Apple Macintosh range of Computers?

- [a] GIF
- [b] JPEG
- [c] PICT
- [d] TIFF

Module 3 - File Formats I

All information is stored in files in the real world. Since there has to be a distinction on the type of information being stored, files are classified into different "file types" or "file formats."

It is difficult to list out all the file formats in existence, so formats for three common categories have been listed here. It is to be noted that the list is by no means exhaustive, as new file types are created everyday.

Images

A single still video image, whether created by a drawing or paint program or scanned from a book or grabbed with a video camera, can be stored in any of a wide variety of file formats. The data will be stored in a raster or a vector file format.

A raster image is one composed of a set of pixels, each specified by a colour. This type of image is usually created using paint programs, by scanning a picture or by grabbing an image. A vector format is created almost always by a drawing/Computer Aided Design program and consists not of pixels, but objects such as curves, shades, and characters.

Raster formats can be generally separated into two categories: Lossy and Lossless formats.

Lossy formats lose resolution (sharpness) when converted to, while lossless formats preserve image information. For example, when converting from a GIF (Graphic Interchange Format), which is lossless to a JPEG (Joint Photographic experts Group), which is lossy, some information is lost. However, lossy formats tend to be much smaller than their lossless counterparts, and for most photographic images, there will be almost no discernible difference.

The following list of image file formats comprises the majority of files encountered on the Internet. All of the following formats are raster formats unless otherwise stated.

.gif

GIF, which stands for Graphics Interchange Format, is a graphics file format originally popularised by CompuServe. GIF files are encoded, 256 colour (8-bit) images which use a lossless compression technique and can be opened by almost all graphics programs including xv, Lview, and Photoshop.

.jpg, .jpeg, .jfif

JPEG stands for Joint Photographic Experts Group. JPG (more accurately JFIF) files are true colour images that are compressed using a lossy compression algorithm called JPEG. This means that files may degrade in quality when they are JPEG encoded. However, this reduction in quality is not noticeable for most scanned

photographs and images with smoothly coloured areas.

However, JPEG encoding should not be used for line art or cartoon images. JPEG files are significantly smaller than most other formats and can be opened and saved with many graphics programs on all platforms.

.tif, .tiff

TIFF (Tagged Image File Format) files are uncompressed true colour images. Most graphics programs allow you to store TIFFs with compression. Many graphics programs including xv, Lview, and Photoshop can open these files.

.tga

TGA (Targa) files, like TIFFs, are uncompressed true colour (24-bit) images

.pict

A PICT file is a standard Macintosh image file format and can be either a raster image or a vector image, depending on the program that created it. Most Macintosh applications will open them.

.bmp

BMP files are Windows Bitmap files. They are usually 8-bit colour images (256 colours) and can be viewed by many programs including Windows Paintbrush. BMP files can be used as backgrounds for the Windows desktop.

.pbm, .ppm, .pgm

Portable Bitmap, Portable Pixmap, and Portable Graymap respectively are all file formats used by the PBMtools set of Unix graphics utilities. They are most commonly used on Unix workstations.

.psd

PSD signifies an Adobe Photoshop graphic file. They open on Pentium and Macintosh systems by Adobe Photoshop.

.cgm

A Computer Graphics Metafile, CGM, is also a vector format.

.wpg

WPG are WordPerfect graphics files that can be opened with Lview.

.wmf

WMF files are Windows Metafiles that can be opened by Canvas.

.xpm, .xbm

X PixMap or X bitmap files are usually small files used in the X Window System.

.ps, .eps, .epsi

PostScript (PS), Encapsulated PostScript (EPS), and Encapsulated PostScript with preview image (EPSI) are all vector graphics file formats. They are mainly used to store printed or printable documents and are in widespread use.

.pdf

PDF stands for Portable Document Format and is created by Adobe Acrobat. An Enhancement of the Postscript language, PDF files contain all the same text and page layout information but can include many WWW features such as images, links, and heading references. PDF files can be viewed using Adobe Acrobat

software.

Different file formats work with different programs, although almost all drawing/paint programs will read and write JPEG, GIF, and TIFF formats. GIF and JPEG formats are popular for FTP and the WWW because they are much smaller than other formats, so more of them can be stored. GIF and JPEG formats are not compressible, so it is generally a waste of effort to run a compression program on them. However, other file formats often compress by large amounts. PICT and TIFF formats work best with word processing and desktop publishing programs like Microsoft Word 6.0 and Adobe PageMaker 6.0.

Answer: [c] PICT

Module:3 Reference No:M3070

Question: Which of the following is a Movie file format?

- [a] .ra
- [b] .au
- [c] .mp3
- [d] .mpeg

Module 3 - File Formats II

1. Movies

Movies, as they are popularly called, consist of a series of still images, sometimes with embedded audio information, encoded in such a way as to produce a single playable file.

.avi

AVI is a file format developed by Microsoft and primarily used in Windows. AVIs are compressed movies that can be viewed in Windows environments with Media Player and on Unix workstations with xanim.

.mov, .MooV, .qt

Any of these file extensions means that the file is an Apple Quicktime movie. Applications that can view QuickTime video include: Simple Text, WordPerfect, and Microsoft Word. Flattened QuickTime video clips can be viewed on Unix workstations with xanim and on IBM-compatible personal computers with Media Player.

.mpg, .mpeg

MPEG files use the MPEG-1 video compression routine, a universal protocol for creating and displaying time coded data created by the Motion Picture Experts Group. MPEG video clips can be viewed with mpeg_play on Unix workstations, Sparkle on Macintoshes, and MPEG_PLAY on IBM-compatible personal computers.

.flc, .fli

An FLC is an AutoDesk Flick movie and is a raw, uncompressed series of frames. They take up more space than other formats, but the image quality is higher. You can play them within Windows with Media Player.

MPEG and QuickTime are the two most commonly encountered movie formats on the Internet.

2. Sound

Files containing data used to recreate audio on a computer are called audio files and are also available in many different formats. Similar to image formats, audio files can either store a digital sampling of the sound wave

(sound files, like a raster image) or contain a digital encoding of the type, shape, and timing of all the notes used in the composition (music files, like vector images).

.au

An AU is an audio sound file native to Sun workstations. It is playable by wplany on Pentium computers or with Netscape's built-in AU player. .

.iff

An IFF is a sound file playable on Pentium computers with wplany and on Unix workstations with xanim.

.mid, .rmi

MIDI files can be played with the Windows MIDI sequencer. They are music files that conform to the MIDI standard. Play them with Media Player on the Pentium computers, or load them into MusicProse or Finale on a Macintosh.

.ra

This file format is introduced by Real Audio Networks and is widely popular on the Internet for streaming audio.

.mp3

The latest craze in the audio formats, this format allows for compression levels of more than 3 times than what is possible in other formats. Most of today's music is being stored or converted to this format.

.mod

A MOD file is a music file format, which is now popular on IBM-compatible computers.

.qt

A QuickTime movie can contain just sound and no video. Any program that can play QuickTime can play QT sound files.

.snd

An SND is a Macintosh clickable sound format. It is playable on any Macintosh and on Pentium computers with wplany.

.voc

VOC (voice) files were originally popularised by Creative Labs. They are sound files similar to WAV. These files are openable on Pentium computers with wplany.

.wav

WAV (wave) files are Microsoft's native audio sound format. WAV files can include 8-bit or 16-bit sound, in mono or stereo. They can be played on Pentium computers with Media Player and wplany.

Answer: [d] .mpeg

Module:3 Reference No:M3072

Question: In distributed computing all the jobs are processed in:

[a] Serial order

[b] Altered

[c] parallel order

[d] Depends upon the application to be processed

Module 3 - Distributed computing

Introduction

With technological advancement, processing speed has increased tremendously. To utilise processing time more productively, the concept of distributed computing came into existence. It is concurrent computing with a processing node in different locations interconnected to provide supercomputing capacity.

How distributed computing works:

It requires specific software to be installed on client machines and one or more servers controlling the computing process. The agent on the client's system detects an idling system and requests the server for an application package. The server sends the package for computation and receives it back from the client when the job is accomplished.

The server meets several such requests by condensing the processing stage into smaller tasks and then distributing it to various client computers. The server monitors the process being executed by client computers. All the processes are completed simultaneously and returned to the server.

If the server is busy and unable to accept the processed job from client then the client may send the application package to another idle system. The server also manages the security aspect of the whole process.

Securing Distributed computing

To secure transfer of data over a distributed network from intrusion, high-level encryption like Triple DES is used. The application packages sent by servers to client computers are digitally signed i.e. protected with public key Infrastructure (PKI), to avoid any intrusion.

Kerberos is a service that makes use of secret keys or cryptography to establish a secure communication path between the server and the client in a distributed network. Key Distribution Center (KDC) is the basis for any kerberos implementation. The main advantages of kerberos are:

- *Authentication:* It proves the identity of the user.
- *Confidentiality:* It ensures protection of data.
- *Integrity:* It ensures that there is no data modification.

Beside the number of advantages, kerberos has a few disadvantages too. Some of them are:

- The time taken and resources needed to implement keberos is very high.
- Secure implementation in multiple enterprises is difficult.

Pros and cons of distributed computing

Pros

- It improves flexibility and responsiveness to organisational needs
- Greater availability of resources
- Closer alignment with organisational structure
- Increased end-user empowerment
- Supports formation of virtual teams due to its distributed nature
- It is not dependent on a single vendor

Cons

- Inadequate control over information resources
- Greater potential for massive data redundancy
- Complex and expensive
- Difficulty in managing network resources
- Testing and detecting errors in the application is difficult

Answer: [c] Parallel order

Module:3 Reference No:M3076

Question: Which of the following is not a component of Graphical User Interface?

- [a] Pointer
- [b] Icon
- [c] File
- [d] Window

Module 3 - Graphical User Interface

Most of the software are designed with certain icons and menus on the screen that facilitate an easy understanding and operation. This is made possible through the Graphical User Interface (GUI).

What is Graphical User Interface?

A Graphical User Interface (GUI) is a mechanism that makes the computer user-friendly. GUI helps the user to effortlessly move from one application to another. The user will not feel the need to memorise the commands.

The common characteristics of the GUI are windows, icons, menus, push buttons and the like.

Xerox Palo Alto Research Centre was the first to design GUI. But they were not commercially successful. It was Apple Macintosh that made the GUI popular.

Components:

The basic components of GUI are:

- **Pointer:** It is used to select objects and commands. It is usually the small arrow that appears on the display screen.
- **Pointing device:** It is used to select objects on the screen e.g. Mouse, trackball and the like.
- **Icons:** Icons represent the commands, files or windows in pictorial form. By clicking the pointer with the mouse button on the icon we can execute the command or open the window and the file therein. The icons can also be moved on the screen and are not static. Picture of the icon can also be changed. Example is the computer icon in MS Word for saving a file, printer icon for printing the file content and the like.
- **Desktop:** It is the area on the display screen that we see when the system is switched on. The icons are placed in this area.
- **Windows:** The screen can accommodate different windows. Each window can run different programs or file.

- **Menus:** Menus have different commands. By selecting a command from a menu we can execute it. E.g. By clicking "File" in MS Word, it again drops a list of activities that could be carried out say copy, open, delete etc.

De Facto Standards: GUI evolved with the designs of Apple Macintosh, IBM SAA and X-Window System. A brief description of each standard is given below:

- **Apple Macintosh:** Macintosh was the first to introduce menus, icons and mouse driven processing.
- **IBM SAA:** Their design involved an interface that could span between machines say from personal to mainframe computers. Networking and database tools were also included.
- **MIT X Windows System:** It is the most popular GUI for Unix systems. They are similar to the IBM SAA.

Designing:

Human considerations: While designing GUI, certain human considerations should be taken into account. They are

- **Visual acuity:** The human eye can only focus on a small part on the computer screen. Therefore the amount of information on the screen should be limited. Otherwise it will cause unnecessary and tiring eye movements.
- **Information limits:** There is a limit to the amount of information that a human can process at any given time. In the design of GUI, it is desirable that the options should not be more than five or six.
- **Gestalt principle:** According to this principle, humans use top down approach for organising data. In GUI design, the like options should be placed in one group.

Design considerations:

- **Amount of information to be presented:** GUI should present information in a contextual and consistent manner. Information should be presented in a concise form. It should be limited to what the user will need to perform a particular operation.
- **Grouping of information:** Information should be properly grouped to improve the readability. For example information can be grouped using colours, graphical boundaries and the like.

Information sequencing: Information should be presented in a manner that the user could easily find it.

Answer: [c] File

Module:3 Reference No:M3084

Question: Which of the following is "FALSE" in relation to the types of computers?

- [a] Workstations can be connected to a LAN
- [b] Laptops and notebooks are portable computers
- [c] Another name for handheld computers is laptop
- [d] Minicomputers are also called as personal computers

Module 3 - Types of computers - Part 2

This is concluding part of series on types of computers. In the earlier article we discussed

- Super computers

- Main frame computers
- Minicomputers.

In this article we discuss workstations, personal computers, laptops, hand held computers and pen based computers.

Workstations

Workstations lie between personal computers and mini computers. They are usually single user computers. They can be connected to the network to form a LAN. They have high-resolution graphic screen and at least 64 MB of RAM. They may or may not have a storage capacity. Where the storage capacity is not available they are termed as diskless workstation. The most common type of operating systems that are used in workstations is UNIX and Windows NT.

Beneficiaries of workstations are engineering companies, architects, and graphical designers.

Microcomputers or Personal computers

Personal computers are relatively inexpensive systems designed for individual users. The advent of personal computers has brought about a revolution in the computer industry. Prior to them, the computers were very expensive and were used as terminals attached to a large computer where resources were shared among all the users. Technological advancement has made it possible for computers dedicated for individual users. Compared to mainframes and mini computers they have less processing speed and storage capacity.

The PC consists of a visual display unit, system unit, keyboard and mouse. Visual display unit is the screen on which the user views the data that is being entered into the computer and the processed output. The system unit consists of the processor, primary memory and disk drives. The input and output devices are connected to it. The processor processes the data that is keyed, stores and retrieves it. The keyboard and the mouse are the input devices that are used for feeding the data.

The components of the personal computer are not fixed. The user can alter it to meet his needs. It is possible to have built in fax capabilities, communication devices or any other additional features as desired by the user.

Personal computer are usually used in business for word processing, spread sheets accounting purpose, desktop publishing and the like.

Laptops and Notebooks

Laptops and notebooks are portable computers. They integrate the display unit, memory, storage area, keyboard and trackball (similar to mouse in operation) in a single battery operated unit. Any additional features such as fax capability, CD-ROM or input and output devices can be linked.

The basic difference between laptops and notebooks is the size and weight. The laptops are small enough to fit into the lap of the user and notebooks are larger than average hard cover book.

People who need to travel extensively generally use laptops and notebooks.

Hand-held computers

Hand held computers are mainly used for collecting field data. They are smaller in size than the notebooks. Beneficiaries of hand-held computers are archaeologist, police and the like.

Pen-based computers

As the name suggests, pen based computers do not use keyboard as a means for keying in the data. They use electronic writing pad and light sensitive electronic pen instead of the keyboard. As the user writes on the pad, it is converted into the digital input.

Sales representative, insurance agents, delivery people and the like benefit from them.

Answer: [c] Another name for handheld computers is laptop

Question: Minicomputers can be used

- [a] As file servers in LAN
- [b] As a server in client/ server environment
- [c] As a communication link between mainframes and terminals
- [d] All of the above

Module 3 - Types of computers - Part 1

Computers are classified into different types depending on their memory size and processing speed. They are classified as organisation wide, work group and personal information system.

Organisation wide systems are computers providing overall information of the company

- Super computers
- Mainframes

Work group systems facilitate decision making and exchange of information

- Midrange computers
- Workstations

Personal information systems are meant for individual needs

- Microcomputers
- Laptops
- Hand-held computers
- Pen-based computers

We shall now discuss each of them in detail.

Supercomputers

Supercomputers have a large memory and high processing speed. They are equipped to process around billion instructions per second. They are considered to be the fastest and the largest computers at present. The two main characteristics of supercomputers are fault tolerance and parallel processing.

Fault tolerance: A backup mechanism is used for fault tolerance. The mechanism automatically isolates and reconfigures the hardware when there is failure in the system during system operation. The companies that require reliable data and the ability of the system to process large volume of data usually use this mechanism.

Parallel processing: Parallel processing is the processing of multiple instructions by multiple processors. Parallel processing greatly reduces the processing time. Instances where parallel processing can be applied are image processing, resource optimisation, graphics, drug industry, financial portfolio analysis and weather forecast.

The main disadvantage of super computers is that they are very expensive and hence are used only for specialised applications that require immense mathematical calculations.

Mainframes

Mainframe computers were defined as those that occupied the whole room or large floor area. At present with reduction in size of the computer and increase in processing speed, the term has undergone a change.

Now it is referred to as systems that have high processing speed, capable of a million instructions per second.

Mainframes consist of central processing unit, which controls and directs the operations. They usually have memory capacity of at least one gigabyte. They can support many input/ output devices, peripherals and users simultaneously. Mainframes are large general-purpose computers and can support both batch and online processing. The applications where they are usually applied are weather forecasting, airline reservation, financial applications, investment analysis, payroll and the like.

Midrange machines/ minicomputers

Minicomputers fall in between mainframes and microcomputers. They have similar features as mainframe but lack the speeds and storage capacity. The memory size can be up to several gigabytes. They can support many users simultaneously. The minicomputers are usually used in small and mid-size businesses and in businesses as large as departmental level operations. Minicomputers can be used

- In LANs to act as file server
- In a client server environment as a server
- Between mainframes and terminals to act as a communication link.

Answer: [d] All of the above

Module:3 Reference No:M3097

Question: In a file management system, proper controls are established over check-in and checkout of documents to avoid

- [a] Usage of file by different users at a time
- [b] Duplication of files
- [c] Problems in a search engine
- [d] Wrong uploading and downloading of files

Module 3 - File management System

The information entered into the computer is stored in a file. The files have to be stored in an order to facilitate easy location when required. Right methodology has to be adopted in order to avoid wastage of time. There are different types of file storage devices. Floppy disk, Zip removable disk, CDs, Zip share drive and Hard drive are a few to name.

Back up of stored files is also very essential. There might be chances of accidental deletion of files and also diskettes or hard drives getting corrupted. File management is a very important process. There should be an appropriate file management system in the organisation. The following are the essential requirements of a file management system.

Control over different versions: It is difficult to trace different versions of documents lying with different persons. If an appropriate version control system exists, the changes made at each level and the respective persons, time and date can be identified easily. The system keeps a record of all the versions of a particular document.

Checkout and check-in: There should exist a proper control over check-in and check-out of the documents in order to avoid usage of file by different users at a time. For example, if an authorised user is working on the file, others should not be permitted to make changes to the said file. This is possible if there exists a proper control over granting permission to check-in and check out.

Meta data: The data relating to files is referred to as Meta data. This pertains to file type, data creation, modified, keywords, description, owner of the file, creator, and the like. Users must be able to create and store Meta data with the help of file management system.

Indexing: Files must be indexed properly for easy location. This requires an indexing engine, which automatically adds the new files to the respective folders.

Search engine: A good file management system should have an efficient search engine, to quickly search for the relevant files. This is possible when the keywords from the files are found out through indexing and a search index is created.

Capable of dealing with groups: A particular activity may require usage of different types of file formats like PowerPoint, charts and graphics. In such a case, the file management system must be capable of dealing with these interdependent groups.

Multiple file types: MS-Word, MS-Access, MS-Excel and Text are some of the standard file types. User must be able to upload and download them easily through the system.

Security: User must be able to develop security functions like read, write, delete and update with the system.

File expiry date: File expiry date has to be established for each type of file or files. This helps the system to find and delete them as per the pre-stated dates. This results in the efficient management system.

Interface: The system should allow the user to access the interface and gain a sufficient experience.

Storage facility: Creation and storage of folders, movement of files between folders should be user-friendly.

Answer: [a] Usage of file by different users at a time

Module:3 Reference No:M3100

Question: The primary objective of a data classification scheme is to

- [a] To meet the business requirements
- [b] To increase the integrity value of the data
- [c] To assign different security levels
- [d] To ensure optimal utilisation of resources

Module 3- Control objectives for planning block

Building the information architecture framework

Introduction

Once the long term and the short-term plans are formulated, the next logical step is to frame an information architecture model. This information architecture should define appropriate systems that are required to generate accurate information.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
An optimal information system organisation	To ensure effectiveness, efficiency, confidentiality and integrity of the information that is fed into, processed, generated by the information system	1. Data dictionary 2. Data repositories 3. An information architecture which represents the needs of the organisation 4. Data syntax rules 5. Information architecture standards.	• Data • Application technology

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **The information architecture framework:** The information that is generated by the system should be the basis for the decision support system of the management. Accordingly, an optimal information structure has to be built to serve the needs of the organisation. This information model should provide a process or methodology for regular collection and communication of data that is generated and required by the organisation. It should have a timeframe to ensure that people carry out their responsibilities in an effective manner. The information architecture should be consistent with the long-range IT plans. It should be regularly updated and changed as per the changing environment of the business.
- **Data dictionary and syntax rules:** All information architecture models should consist of a data dictionary, which incorporates the organisation's data structure. It must also be ensured that the data dictionary is regularly updated for any changes in the business environment. The data dictionary should also define the data syntax rules.
- **Classification of data:** The information model framework should consist of a data classification scheme for the corporate data. Data is classified to assign different security levels to each category. This also facilitates in managing the access rights that are to be given to each category of users.
- **Assignment of security levels:** The information model adopted by the organisation should constitute a mechanism for definition, assignment and maintenance of security levels for each category of data. A minimum set of security measures should be adopted for each security level defined. The assignment of different security levels to different categories of users should be based on some pre-established criteria. Such a criteria and the security levels defined should regularly be evaluated and modified if the need arises.

II. Operational Controls

Not applicable for this activity.

Answer: [c] To assign different security levels

Module:3 Reference No:M3106

Question: Which of the following is not the preventive system internal control?

- [a] Automatic logoff
- [b] Account balances
- [c] Auto encryption
- [d] File deletion

Module 3 – Preventive Controls – Printing operations

Businesses have to take reasonable care while printing important documents for use by others. For example, some companies print payment cheques to pay the suppliers. Such a task, which is a part of payment management, requires a very high level security. The risk of counterfeit cheques looms large, in event of which the management will have to bear heavy expenses in the form of bank fees. A new technology, Laser Cheque printing has been introduced to counter this problem to a great extent. The main functions of Laser cheque printing software packages are cheque printing and payment management operations. It ensures proper control over fraud and hence reduces operating costs.

The organisation should also realise that any change in the technology would certainly warrant a change in the existent internal controls of the organisation. It is necessary to understand the types of internal controls for evaluating their effectiveness before implementing them. The cost effectiveness of the controls need to be appraised in relation to the benefits (like reduction in operating expenditure) accrued from the controls.

Internal controls are segregated into preventive and detective controls. **Preventive controls** are those, which prevent the occurrence of any error or irregularity. On the other hand **detective controls** aim to identify the error after its occurrence. Both the controls can be again divided into system controls and manual controls. Preventive controls are being discussed in the present article, while detective controls and the audit of printing operations will be discussed in the second part of the article.

I. Preventive Controls: -

A. Preventive system controls: The following are the preventive system controls

1. Auto encryption: When cheques have to be printed, the system first receives input from accounting data authorising the payment. This file is then formatted to cheque image file, and encrypted. In addition, the digital signatures data and bank account details of receiver (if any) are also encrypted. Logs for system activity, cheque prints and the like are kept.

2. Automatic deletion of a file: After cheque printing, the data file should be automatically deleted by the system.

3. Automatic logoff: If the system is used for a specific time limit, it must be controlled by automatic log-off.

4. Login controls: Laser printing system should provide adequate login controls. Users must be allowed to login through a set of procedures, different from general procedures. Some systems may have separate passwords for different processing operations to ensure security.

5. Pause with warning: The system should warn the user in case of any interruption caused to the process to avoid reprinting that give scope for frauds.

6. Positive pay system: Under a positive pay approach, bank verifies each cheque with the details sent by the customer through MICR. It rejects and informs the customer of those that do not match. Banks may provide this service free of cost or charge a fee.

7. File deletion: Cheque image files must be deleted after processing. If they are retained for the purpose of reprinting, it must be ensured that they are deleted after particular time limit.

8. Reprint authorisation: Only an authorised supervisor with a different user ID must perform the cheque reprinting operations.

9. Printer related security features: Background images on the cheque can be done using security features like void pantographs or wicker. Void pantographs are small dots, which cannot be captured while scanning or copying. Wicker features are lines with different lengths printed at different angles that are not compatible with scanner or copier protocol. An attempt to scan or copy these lines leaves a garbled image.

10. Two dimensional barcodes and data glyphs: Data glyphs and two-dimensional barcodes are printed on the cheque by a laser printer. A small picture of the complete cheque is contained in these features. It makes fraudulent printing difficult.

B. Preventive manual controls: The following are the preventive manual controls

1.Account balances: The cash balances to be maintained in the checking account must match the predetermined levels arrived through cash budgets. It avoids fraudulent overdrawing of funds.

2. Isolated PC: Cheque printing systems must be separated from other software to avoid interruption in the cheque printing operation. It also reduces the possibility of fraudulent cheque printing.

3. Control on cheques after printing: The printed cheques and the print log should not be made available to the accounts payable staff.

4. Supply control: Cheque supplies such as MICR toner, stock of blank cheques must be controlled properly. It can be ensured by physical isolation.

Answer: **[b] Account balances**

Question: Which of the following is an effective control over paper stock?

- [a] Activity logs
- [b] Printer related security features
- [c] Paper count
- [d] Number log

Module 3 – Detective controls – Printing operations

Businesses have to take reasonable care while printing the important documents for use by others, which otherwise may result in heavy expenses. Laser Cheque printing has been introduced to detect malpractices to a great extent. The main functions of Laser cheque printing software packages are cheque printing and payment management operations. It also ensures proper control over fraud and hence reduces operating costs.

Preventive system and manual controls are covered in another article. This article dwells on the detective controls and the audit aspects of printing operations.

II. Detective controls:

Detective controls, created by the system are referred to as detective system controls. Those requiring human intervention are referred to as defective manual controls.

A. Detective System controls: The following are the detective system controls

- 1. Logs:* System logs, cheque printing system logs and image files must be compared with the independent records to find out the fraudulent runs made if any. Operations staff must maintain the print logs, which shows the details of cheque runs. It helps in reconciling the bank balances and also enables internal auditors to review the process.
- 2. Limiting messages:* Limited encashment through cheques and validity of date could be incorporated.
- 3. Manual and duplicate signatures:* Manual signatures serve as a good control to detect and avoid forgeries. Whenever manual signatures are used, the system should be programmed in such a way that digital signatures are deactivated automatically.
- 4. Control over paper stock:* Using coloured paper for cheques is an effective control feature to differentiate cheques printed by different departments. However, because of existence of colour copiers forgeries may not be easily detectable. But pastel-coloured papers ensure some level of security. In addition, different colours may be used for background and foreground printing.
- 5. Printer related security features:* Non-repetitive printing, secure font printing and warning band controls are some of the detective controls.
- 7. Signature plates:* Signature plates serve as effective control to identify forged cheques. Proper measures should be taken to protect digital signature plates. It should be encrypted and kept in removable disks when printing is not being done.
- 9. Ultraviolet imaging of cheque snippets:* Banks generally use these cheque snippets to record the information on paid cheques. Cheque makers can also use snippets to stop the encashment of modified

cheques.

10. Special ink security features: The special inks that were used in preparing cheques traditionally served as a control to differentiate between the original and duplicate. But with the advent of laser printers this became difficult. However, if two printers were operated in series using special inks, in such a way that the printing is completed only when it is processed through both printers, it would be more secure.

12. Paper related security features: Certain paper related security is available to identify tampering of cheques. They use certain chemicals and toner adhesion coating. In some cases the security feature detects when the cheques are scanned or photo copied.

B. Detective Manual controls: The following are the detective manual controls.

1. Account reconciliation: Lack of accurate reconciliation schedule, delay in reconciling the balances and inefficient staff are some of the reasons for frauds. A good pay system should ensure a precise reconciliation.

2. MICR testing: Appropriate machinery must be selected to process the cheque through MICR.

3. Number log: Operations staff is required to maintain a number log showing the details of cheques printed on each day. It enables to identify the unauthorised printing if any, by comparing the previous day closing numbers and the next day opening numbers.

4. Paper count: Paper count control is an effective control over paper stock.

Audit of printing operations

1. **Preliminary evaluation:** Under preliminary evaluation, an auditor should check the back up, retention and purge policies that are framed in the committee meetings. Ensure that these policies are not changed without prior approval. The committee should consider all the rules and regulations relating to banking contracts and clearing houses before framing the policies.
2. **Personal visit to the location:** Auditor must visit the processing locations. He should examine the documentation of each and every process. He should ensure that the processes are run according to the set procedures.
3. **Evaluation of controls:** Auditor should examine the controls established over processes to evaluate its effectiveness.
4. **Change management process:** Auditor should ensure that adequate controls exist over change process. All new features added to the system should interface accurately with the existing security features.
5. **Restrictions on vendors:** Whenever vendors support the system for its functioning and maintenance, they should not be allowed to access the sensitive information. Updation of software at a remote location may give rise to unauthorised changes.
6. **Audit report:** Audit report should not contain a detailed description of the internal control in place. As the audit report is accessible to many, one can easily beat the controls if they are discussed clearly.

Answer: [c] Paper count

Question: A Deadlock is prevented by

- [a] Rolling back the transaction after it is found deadlocked
- [b] Thwarting occurrence of at least one of the necessary conditions for deadlock
- [c] Running the Banker's algorithm
- [d] Pulling back a resource from the deadlocked process

Module 3 - HANDLING DEADLOCKS

Deadlocks in databases- a threat to performance:

Databases that allow users to modify and view data, face the threat of deadlock. For e.g. When two transactions require the same table / object simultaneously, both are put to wait and the processes end in a deadlock. When two or more processes are deadlocked, the Server has to kill one of the processes and roll back the transactions for every process that is killed by the server. Thus, if a database has too many deadlocks the efficiency of the system drops. (The second sentence confuses the logic. Pl arrange the sequential order i.e. deadlock-kill-rollback) **Rollback** refers to undoing a part of the update in a database due to failure of a database transaction. After the rollback the Server has to process the same transaction all over again from the start. This leads to wastage of time and resources.

Deadlocks can be dealt with using the following methods:

1. Detection and recovery
2. Prevention
3. Avoidance

Deadlock detection and Recovery:

Deadlocks are detected by running a deadlock detection algorithm. In this algorithm the processes that are not waiting for any resources are searched for and omitted since these cannot be a part of deadlock (these processes can run, since they aren't waiting) With the completion of this search, the processes that form a cycle are detected and declared as deadlocked.

The next step: After detection, the deadlock recovery starts off by using either of the following methods:

- Rebooting the system
- Pulling back a resource from a process
- Using checkpoints

Rebooting is usually considered a drastic step and is best avoided unless it is the only option left. A milder approach would be to take away a resource from a process so that the cyclic queue (to mention that the cyclic order is due to waiting in a cyclic order would be more understandable.) is broken thereby avoiding a deadlock. But taking away a resource from a non-preemptive process would cause damage beyond repair. Hence, in such cases one or more processes are killed (stopped from execution) and re-run (rollback), which would at least avert a system crash.

Using checkpoints: Huge database systems make use of checkpoints. If the processes were checkpoint (pl rephrase) Using checkpoints in processes from time to time will simplify rolling back (as rollback to the recent most checkpoints would seem less cumbersome).

Prevention of Deadlocks: It is essential to remember that a deadlock occurs *only if all the four necessary conditions for deadlock are met*. Thus, preventing any one of the necessary conditions can avert a deadlock. Mutual exclusion and non-preemption are difficult to avoid due to the possibility of at least one of the resources being non-sharable. By assigning all the resources at the start up time or by releasing the resources from it before new allocations, would hinder the hold and wait condition.

But this will hamper non-preemptive processes.

Thus, *the ideal way of preventing a deadlock, is avoiding the development of a circular queue.* This is done by an algorithm (known as hierarchical allocation), which allocates resources in a way so as to inhibit the formation of the queue.

Deadlock Avoidance: Avoiding unsafe states can thwart deadlocks the system allocates resources in away that does not lead to deadlocks in the system. For this Banker's algorithm is run and it is ensured that all the processes run smoothly after allocation. If the system seems unsafe then allocation is done again for system stability.

Answer: [b] Thwarting occurrence of at least one of the necessary conditions for deadlock.

It should be clearly understood that preventing the conditions for occurrence of deadlocks can thwart the deadlock. Prevention DOES NOT refer to deadlock recovery.

Module:3 Reference No:M3116

Question: Deadlocks occur when

- [a] Mutual exclusion and non preemption of resources exists
- [b] Processes hold resources and wait for some more
- [c] Processes wait for resources in a cyclic order
- [d] All of the above mentioned occur

Module 3 - Exploring Deadlocks

Definition:

A deadlock is a condition in which two computer processes share the same resource and thwart each other from making use of the resource, thereby putting an end to the functioning of both the processes.

Explanation: Operating systems earlier were designed to run and execute only one process at a time. Thus, the process would have all the resources dedicated to it. But with the evolution of multiprocessing operating systems (multiprocessors are different from multiprocessing OS, hence the correction) (that execute many processes simultaneously) a same set of resources would be required to run and execute a number of processes. Consequently, it leads to deadlocks.

Thus a Deadlock occurs when one process requests for a resource that is already being used by another process. (Sounds conceptually wrong, as deadlock CANNOT occur with just one process waiting for a resource, there has to be many such processes in the system. Please. Correct it accordingly, specifying that many such processes exist). At this rate ultimately, none of them receive the required resources thus leading to a standstill state of the system.

Consider the following example:

Let there be two processes running simultaneously and two resources that are required by these processes.

Process 1 needs Resource A and gets it.

Process 2 needs Resource B and gets it.

Process 1 now requests Resource B and is put in queue, thus waiting for the release of B by Process 2.

Process 2 is held up as it awaits the release of Resource A by process 1.

Thus each of these processes is holding a resource and waiting for another.

Types of resources:

The resources can be classified as -

1. **Preemptable or non-preemptable:** A preemptable resource is one that can be freed from a process that is holding it. An example of a preemptable resource is memory. Non-preemptable resources are those that cannot be borrowed from the process holding them until the process holding them is complete.
2. **Reusable or consumable:** The resources like printers, memory, and so on, which can be used more than once, are known as reusable resources and those like an event or a message that can be used only once are consumable resources.
3. **Sharable:** Resources that can be used by more than one process at a time are known as Sharable resources.

Necessary Conditions for occurrence of Deadlock:

A dead lock occurs if and only if all the following four conditions are met:

1. *Mutual Exclusion:* Occurs when all the resources are non-sharable.
2. *Non-preemption:* Occurs when the resources held by a process cannot be released till the process is complete.
3. *Hold and Wait:* When processes hold some of the resources and are waiting for some others for completion.
4. *Circular wait:* When the processes request for resources in a form that it causes a cyclic pattern then it is known as circular wait.

The following diagram illustrates a cyclic pattern:

Handling Deadlocks:

Deadlocks have a major impact in the performance of Operating systems and Database Structures. The three ways of dealing with Deadlocks include:

- Deadlock Detection and Recovery
- Deadlock Prevention
- Avoidance of Deadlocks

Answer: [d] All of the above mentioned occur

Only when all the necessary conditions are met, do deadlocks occur, OTHERWISE NOT.

Module:3 Reference No:M3129

Question: Which of the following information is stored in the CMOS?

- [a] Basic configuration information
- [b] Integrated peripheral configuration
- [c] Setting the password for the hardware
- [d] All of the above

Module 3 – CMOS – its options

DIP switches (Dual Inline Package Switches) placed on the motherboard were used to identify configuration items like type of the monitor, floppy drives etc. However, DIP switches would engage a lot of space on the motherboard and increase the number of configuration parameters. CMOS RAM (Complimentary Metal Oxide Semiconductor) developed by IBM performs similar functions, but with a difference - CMOS can store large amounts of information, which can be categorised into the following types:

- Basic configuration information that helps to identify the right parameters of the hard drive.

- Settings for performance improvement
- Power saving features selection
- Setting the password for the hardware
- Integrated peripheral configuration

The basic input/output system (BIOS) understands and applies the information stored in the CMOS to configure the system.

CMOS set-up facility and access: - Several CMOS options are available on the menu in the CMOS Setup utility. Changes can be made to the CMOS set-up based on the requirements. It must be ensured that present settings are recorded and the computer is tested between the two changes. Following are some of the options explained in detail.

1. **Standard CMOS set-up:** - Its configuration is easy and simple, as the IDE HDD Auto Detection utility (which is on the other menu selection) automatically provides the applications for hard drives if the date, time, type of the drives and its number are informed to the computer. All the existing hard-drive parameters must be noted in the case of an already configured machine.
2. **Configuring the BIOS features set-up:** - These configuration options check the events that happen during the booting process. They are not essential in determining if the system is running.
3. **Setting Chipset features:** - This feature enables one to configure the Chipset features. Machine performance can be controlled with the help of Chipset features. It is essential to note the existing settings before any changes are made.
4. **Auto-configure:** - An auto-configure option automatically sets some of the Chipset Features' Set-up options on the screen. This is an essential feature in the absence of performance measuring software. However, it may not be feasible to test the settings using several possible combinations.
5. **Power management set-up:** - The power management set-up feature provides the details of the power consumption modes of the monitor, CPU and hard drives in order to discontinue or allow user-configurable power save settings.
6. **PCI configuration:** - Essential rules for plug-and-play devices and the PCI bus are established in the PCI configuration. This only helps to automate the settings configuration but does not affect machine performance. Unless there is a problem in adding additional devices, this option need not be changed.
7. **Load set-up defaults:** - Load Set-up Defaults, an auto-configuration setting, supplies a consistent configuration even if some of the items are not efficiently set. Various settings can be adjusted individually after the configuration.
8. **Integrated peripherals:** - The controllers of devices like serial and parallel ports, integrated device electronics drives, infrared ports, and floppy disks are incorporated into the motherboard. This facilitates the configuration of such devices with CMOS setup facility.
9. **Saving the changes:** - Selecting Save Changes before Exiting will save all the changes made to the CMOS.

Answer: [d] All the above

Module:3 Reference No:M3132

Question: Which of the following statements is not true of floppy disk drives?

- [a] Floppy disks are used for transferring data from one machine to the other
- [b] Floppies are used for backups and storing smaller files
- [c] Floppies have higher track density as compared to hard disks
- [d] Floppy disks are removable memory devices

Module 3 – Floppy Disk drives

An Overview

A floppy disk is a removable memory storage device that is quite similar to a cassette in its construction and method of working. Floppy disk is an electromechanical device that is made up of ferromagnetic tape in a plastic case that can record information. A floppy disk can be reused many times by erasing and re-recording information in the disk. The tape is made up of ferromagnetic substance that stores information when magnetised.

Floppies are accessible by inserting them in the floppy disk drive of the computer. A floppy disk drive is similar to the hard disk drive. The only difference being, floppies are removable memory devices and hence have simpler construction as compared to the hard disk drives.

Uses of floppy disks

Floppy disks are chiefly used in the following:

- **Data transfer:** One of the most common practices in migrating files and application programs from one workstation to the other is through floppy disks.
- **Back up and file storage:** Floppies are used for taking back ups of small amount of information and storing smaller files and application programs. E.g. booting program for an operating system say for Windows or Unix can be stored in a floppy, that occupies less space and at the same time serve as a recovery measure during system crash.
- **Installing software and upgrading the system:** Since most of the software installation programs are compact in size, they are stored in floppy disks. Moreover, software updates are easily carried using floppy as they are removable and allow file transfer from one machine to the other easily.

The capacity and the data storing format varies with floppy disks. Despite the difference in the sizes and data storage formats of floppy disks, the internal construction of the floppy disk drive is similar.

How do floppy disks differ from hard disks?

Unlike the "fixed disks" or the hard disk, floppy disks are not fixed to the computer and are removable. Hence these are not as reliable and long lasting as compared to the hard disks. The chief differences between floppy disks and hard disks are as enumerated below:

- The read/write head of floppy disks are larger than that of hard disk and they are not as accurate in reading and recording information as in hard disk drives. This is because, the track density (i.e. number of tracks per inch of the disk, typically used to measure total number of tracks in a disk) is less in floppy disk than in hard disks and hence, the tracks in a floppy are not precisely laid on the tape.
- Floppy disks use "direct contact scheme" for recording information. In a sense that, the read/write head of the floppy comes in direct contact with the tape while storing data from the computer and hence employs a more reliable scheme of data storage. In hard disks, the read/write head does not come in direct contact with the tape. Data is erased using ultraviolet light. Hence, in terms of longevity, hard disks surpass floppy disks.

The different components of a floppy disk drive are:

- Read/write heads
- Head actuator
- Spindle motor
- Disk change sensor
- Connectors and jumpers

- Logic board
- External packaging.

Each of these are discussed in detail in the subsequent article on floppy disks.

Answer: [c] Floppies have higher track density as compared to hard disks

Module:3 Reference No:M3133

Question: What does the spindle motor of a floppy disk drive do?

- [a] It positions the read/write head in the correct tracks of the tape enable read or write operations
- [b] It converts digital data to electromagnetic pulses and vice versa
- [c] It controls the rotation of the tape of the floppy disk
- [d] It detects the presence or absence of the disk in the drive

Module 3 – Construction and Operation of Floppy Disk Drives

An Overview

Floppy disks vary in size, capacity and the data storage format. But the internal construction of all floppy disks is similar. The major components of floppy disk drives and the respective functions of each are explained in detail:

- **Read/write head:** The read/ write heads of the floppy disks convert digital data to analog pulses and vice versa. While writing to a floppy, i.e. storing information in the floppy, the read/write head converts the binary data or the digital data into analog signals. And while reading data from the floppy, the read/write head converts the electromagnetic pulses to digital data. Typically, the read/write head of a floppy disk is made up of ferrous electromagnetic material that remains in contact with tape while performing read and write operations.
- **Head Actuator:** Head actuator places the read/write head on the corresponding track from where the data is to be read or to which the data is written. The head actuator is controlled by a stepper motor. Generally, floppy disks have 80 tracks per side. As the tape moves in the floppy disk drive, the actuator places the read/write head at various positions (i.e. at different tracks). The stepper motor rotates on pre-defined track positions so as to place the read/write head on the specific track, where the data is to be written or read from.
- **Spindle motor:** The rotation of the floppy disk tape is controlled by the spindle motor. The floppy disk is clamped at its centre after it is inserted. These clamps are attached to the spindle motor that rotates these clamps. Subsequently, with the motion of the clamps, the tape of the disk starts rotating. Typically, floppy disks rotate at the rate of 300 RPM (rotations per minute).
- **Disk change sensor:** As the name suggests, the floppy disk sensor is a sensor that indicates whether a disk is inserted or ejected. This avoids the problem of checking whether the disk is in the system or not prior to accessing data from a floppy, thereby saving system time.
- **Connectors and jumpers:** Connectors connect the floppy with the rest of the computer like printer, hard disk drive and the like. Jumpers set up the floppy disk drive (i.e. whether drive A: or B: etc. is used as floppy disk drive). Conventionally, drive A: is taken to be the floppy disk drive, however this can be changed and configured accordingly. The two connectors used by a floppy disk drive are power connector and data interface cable.
- **Logic board:** The logic board of the floppy disk drive is an integrated electronic circuit board that establishes the interface between the floppy and the CPU. In fact the logic board acts as the drive controller interfacing rest of the physical components of the floppy disk like the read/write heads, spindle motor and the like.

- **External packaging:** Floppy disks are essentially magnetic tapes packed in a plastic cover. The external cover has a latch, which is manually operated in order to enable or disable read/write operations in a floppy disk.

Answer: [c] It controls the rotation of the tape of the floppy disk

Module:3 Reference No:M3138

Question: Which of the following statements is not true about an acoustic digitizer?

- [a] It is a passive digitizer
- [b] It is an active digitizer
- [c] It is used to monitor medical applications
- [d] None of these

Module 3 – Digitizers

Definition: As the name suggests, a digitizer is a device that converts an analog signal to a digital signal. A digitizer samples out the analog signal at a constant pace and encodes each block of analog data into digital representation based on the amplitude at every point of the analog signal. In other words, a digitizer is an input device that generates a two-dimensional image and sends it to the computer.

The chief components of a digitizer are:

- A *hand-held stylus* or a cursor that provides the input
- A *flat tablet* that generates corresponding x and y coordinates from the input data
- *Controller* (that consists of sophisticated electronic implementations) that converts the input data into digital data
- *Driver software*

Working

The flat tablet over which the stylus or the cursor moves determines the precise location of the input data (i.e. represents the data in terms of its x and y coordinates). This data is then sent to the controller, which digitises the data (i.e. converts analog signals to digital representation). The computer then draws images (e.g. charts, blueprints, plans etc.) on the basis of the input received. This enables the user in preserving the accuracy of data while generating graphs or plans from them.

Types of digitizers

Digitizers are basically classified into active and passive digitizers on the basis of the type of input devices used by each of these.

- **Passive digitizers:** Passive digitizers, also referred to as *resistive digitizers*, are used in most PDAs (personal digital assistants). In such digitizers, the input device does not contain any electronic component (typically a stylus, or a cursor). In such devices, the user simply touches the flat tablet (the screen or the surface that takes in the input). Current flows to all four corners of the point of contact, thereby indicating the precise location of the input to the controller. Subsequently, the controller converts the input into coordinates (x and y) based on the fluctuations in the current flow and direction.

The different kinds of passive digitizers are:

- **Capacitive digitizer:** In a capacitive digitizer, voltage is applied to the four corners of the screen. The position of the stylus is calculated from the flow of current from these corners to the point of contact. These kinds of digitizers are used in video games, kiosks etc.
- **Acoustic wave digitizer:** In acoustic wave digitizers, ultrasonic transducers are fixed on the two edges of the display screen. These transducers set up a specific pattern of sound waves, which is disturbed the moment a stylus or any input device touches the screen. The controller then determines the input point basing on the fluctuations in the sound wave pattern. These kinds of digitizers are usually employed in monitoring medical applications and information kiosks.
- **Infrared digitizer:** Infrared digitizers are similar to acoustic wave digitizers except for the fact that, instead of sound waves, the controller uses infrared rays . Infrared digitizers find use in military applications and banking machines.
- **Active digitizers:** In active digitizers the input device (say for example a pen or a stylus) comprises electronic components. These components are present in the display screen. Active digitizers are usually employed for higher resolution and accuracy. Such devices also have the capability to hover. E.g. such technology is used by portable electronic applications that transmit data, allow the user to save a hard copy of the data, as well as produce an electronic copy that can be detained in their PDA. An active digitizer transfers data about the pen's location using electromagnetic technology, i.e. the electronic component present in the input device provides the controller the data about the point of contact of the input device with the display screen.

Answer: [b] It is an active digitizer

Module:3 Reference No:M3139

Question: Drum plotters and Flatbed plotters are

- [a] Types of pen plotters
- [b] Types of printer/plotter drivers
- [c] Types of inkjet plotters
- [d] Platern / drum types

Module 3 – Plotters

Definition: A *plotter* is a device (analogous to a printer) that draws images, using commands given by the computer. Plotters interpret the commands and draw images using automated pens. They can draw continuous lines unlike printers, which can only simulate lines by plotting a series of points. The plotter can directly draw from *vector graphics* (developing images or pictures in a two or three dimensional space using a sequence of commands or mathematical statements). Plotters are actually the first kind of printers. Since coloured images are drawn using coloured pens, plotters prove to be more expensive than printers.

Plotter types

- **Pen plotters:** Pen plotters, also known as vector plotters, are plotters that draw images using automated pens. The two types of pen plotters are:
 - **Upright Pen Plotter:** In upright pen plotters, the pen and the penholder can move in a single direction (typically in the Y-direction) only. Images are drawn by simultaneously moving the paper (in X-direction) and the pen (in Y-direction). The paper is moved over a platern. A *Platern* is a thin curved horizontal surface on which the pen draws. These plotters are also referred to as *drum plotters*, since the paper is in fact wrapped around a drum or a platern

that keeps rolling in one direction. The other direction is provided by the pen in order to draw a two dimensional image.

- **Flatbed Plotters:** In a flatbed plotter, the pen and the penholder are fastened to a beam horizontally over a flat slab of a specific length and width. The pen is moved in the Y-direction, while the beam is moved in the X-direction. Images are drawn by synchronising the movements of the pen and the beam. The paper is dragged over the flat slab (known as the flatbed) for plotting. Sketching alphabets becomes cumbersome in case of flatbed plotters as it entails a lot of pen movements. In case of long images (that require a number of frames), the frames are aligned in advance, prior to plotting the image completely. This maintains continuity of lines.
- **Inkjet Plotters:** In inkjet printers (also known as the raster plotters), the plotting device is not a pen but an inkjet head that sprays ink on the paper. The inkjet sprays ink on the paper without directly coming in contact with the paper. The image is drawn by moving the inkjet head in Y-direction and the paper in the X-direction. Thus, the image comes out as a series of horizontally printed stripes. Unlike, pen plotters, inkjet plotters do not require any frames in advance. However, inkjet plotters require a lot of maintenance (cleaning, aligning etc.).

Information transfer between the computer and the plotter

A specially designed software (typically, a CAD program) is installed in the computer in order to convert data into plot files (files that consist of a sequence of commands instructing the plotter how to plot or draw the image). A *plotter management program* is used to read plot files. This program translates plot files to a comprehensible format for plotters. Eventually, the plotter takes the data from the plot files in order to draw the image. Communication between the computer and the plotter is established and maintained by a printer/plotter driver during the course of data transfer through the cable.

Answer: [a] Types of pen plotters

Module:3 Reference No:M3140

Question: Which of the following statements about the motherboard is not true?

- [a] Motherboard comprises basic components like memory, microprocessor and the like
- [b] It can be configured either manually using jumpers or by using built-in BIOS settings
- [c] The functionalities of a motherboard are collectively referred to as form factors
- [d] Individual components of a motherboard are interfaced using buses

Module 3 – The Motherboard

What is a motherboard?

The fundamental circuitry of the computer consisting of the basic components like memory, microprocessor etc. arranged on a logic board is referred to as a motherboard. In other words, a motherboard is just a physical arrangement of circuits that are vital for the functioning of a computer on a plain board. Typically, motherboard comprises the following parts:

- Microprocessor
- Memory
- Basic input/output system (BIOS)
- Connecting circuits

Additional components can be integrated with the motherboard, and interfaced using buses.

Motherboards generally vary from one computer to the other. Though configured in different ways, two

motherboards can be similar in terms of performance and functionalities. The generalised design giving an outline of the motherboard, briefing the power supply systems used by it and physical arrangement is referred to as *motherboard form factors*. The two types of form factors widely in use are:

- **AT and Baby AT version**

AT and baby AT versions were one of the popular form factors in use for motherboard construction. Both these form factors chiefly differ in their width. Rest of the features are similar in both. In AT and baby AT form factors, the sockets to connect the processor and memory are placed in the front of the motherboard. Long extension cards are provided in order to connect the processor and the memory devices in the respective socket.

Limitations: Since, AT and baby AT were one of the earlier versions of motherboard form factors, they had smaller slots/sockets for fixing processors and memory devices. But now, newer models of processors and memory chips are bigger in size and hence cannot be directly mounted/inserted on to these motherboards. Thus separate expansion slots have to be created along with the existing slots, which makes the motherboard bulkier. In order to counter this problem and to design a more compact model, the ATX and the mini ATX versions came into use.

- **ATX and mini ATX version**

ATX form factor was designed to suit the newer models of processors and memory chips (like the Pentium and Intel processors). These motherboards had a far more elegant and compact design since all the port connectors were soldered directly on to the motherboard instead of connecting through cables (like in AT and baby AT). The ATX form factor was also designed with better air flow mechanism, thereby reducing the heating up of the processor and increasing its performance. They are compatible both with older and newer PCs.

Motherboard configuration

Motherboard configuration refers to installation of a motherboard while constructing a new PC or while upgrading an existing system. Traditionally, motherboards were configured using jumpers (small metal and plastic pieces that are used to modify the circuitry and functioning of the motherboard). But with the advent of newer motherboard form factors, these settings are configured using built-in BIOS settings. BIOS (Basic Input /Output System), is a program saved in the computer's processor, which gets the computer system started after the power supply is switched on. Such motherboards are also referred to as *jumperless motherboards*. Jumperless motherboards involve easier procedures since the user need not go into understanding the details of circuitry of the motherboard in order to configure it. All he needs to do is click the right option when prompted by the BIOS, on the computer screen.

Answer: [c] The functionalities of a motherboard are collectively referred to as form factors

Module:3 Reference No:M3141

Question: What does a switching mode power supply do?

- [a] Converts raw input power to stabilised dc power
- [b] Converts dc to ac
- [c] Enhances output of a circuit
- [d] Switches to and fro between high and low power fluctuations

Module 3 – Switching Mode Power Supply (SMPS)

Introduction

A power supply provides power from the primary power source in a compatible form to the computer. In other

words, a power system is a buffer circuit that acts as a converter and converts the power received directly from the main source into a form that is acceptable to the computer system. Thus, power supply is also referred to as *power converter*. This process of conversion of power in to a load-compatible form is known as *power conversion*. The chief goal of a power supply is to meet the specified load requirements of the system (i.e. supply power that meets the design specifications of the computer system) and convert raw input power to a stabilised voltage current for smoother functioning of the electronic equipment.

Switching Mode Power Supply (SMPS)

A switching mode power supply also referred to as SMPS, is a power supply that supplies power using electronic components that have low loss factor. It uses low-loss components like capacitors, inductors, transformers and the like. It employs switches, which are in 'on' or 'off' state, i.e. if the voltage becomes high during fluctuations the switch gets turned off thus preventing damage to the system.

SMPS chiefly deals with four forms of power conversion:

1. ac to dc conversion known as 'rectification'
2. ac to ac conversion
3. dc to ac conversion
4. dc to dc conversion

Block diagram of SMPS

Working

The figure above illustrates the working of a switching mode power supply.

Typically, SMPS unit consists of:

- Input conditioning and rectifying unit
- Filtering unit
- Conversion unit

In the first stage, the raw input is taken directly from the primary power source, and put to a standard form. This process is also known as *conditioning*. In conditioning, the SMPS unit ensures that sudden and drastic inputs do not damage the system. It safeguards the devices from unconditioned raw input power.

In the next stage, the input is *rectified or smoothened* (i.e. first step in converting ac waveform to dc converting the negative half to positive). This is done using capacitor filters. Since, in dc voltage there is no voltage fluctuations, the resultant wave forms are chopped at a higher frequency by transistor choppers. The third waveform in the figure above shows how a straight line is sketched out roughly. Finally, dc to dc conversion takes place and the raw power input in ac form is completely converted to dc power (final waveform, which is a straight line).

Advantages of SMPS

- Switching mode power supply is versatile and can be employed in any type of unregulated input
- It provides an efficient method for converting ac to dc. Use of transformers would make the circuit bulky and expensive. Thus, SMPS provides an easy solution for regulating raw input power.

Drawbacks

- Configuring and setting up an SMPS unit entails a lot of expertise and is not a job for amateurs. In other words, though SMPS are compact as compared to transformers, they are complicated.
- Switching at higher frequencies produces electromagnetic waves that have a detrimental effect on electronic equipments.

Answer: [a] Converts raw input power to stabilised dc power

Module:3 Reference No:M3143

Question: Which of the following is not a component of the cathode ray tube?

- [a] Electron gun
- [b] Display power management system
- [c] Photosensitive screen
- [d] Anodes

Module 3 – Monitors

Monitor is the computer screen that serves as a display device in a PC. It is one of the output devices, whereby the user sees the outputs generated by his programs, on the screen. In other words, monitor (computer display or screen) integrates all the parts necessary for displaying images on the screen and interfaces these parts with rest of the computer (like the processor, printers, memory devices, keyboard etc.).

Construction and working

Cathode ray tube

A monitor resembles a CRT (cathode ray tube) in construct and working. Cathode ray tube (CRT) is an electronic screen that constitutes a major part of the computer monitor. CRT screen is coated with phosphorous (light-sensitive) material that glows when struck by a stream of electrons. The photosensitive coating on the screen resembles an array of closely packed tiny cells (usually referred to as dots).

Block diagram of a CRT

Typically, a CRT comprises the following:

- Photosensitive screen, which glows when an electron strikes it, thereby displaying the image
- Electron gun that acts as a source for a stream of electrons thereby forming an electron beam
- Anodes that regulate the frequency and intensity of the electron beam
- Deflecting coils that provide electric field to position the light spot on the Screen

Internal controls and electronics

A dedicated circuit board controls the monitor from within. It is responsible for handling input from all the input devices like mouse, keyboard etc. and displays the corresponding information on the screen. The internal electronics/circuit board generates signals (analog or digital) corresponding to the input. Analog signals are generated by continuous points and hence generate finer images in terms of brightness and contrast. Digital signals are generated by discrete points and hence prove advantageous in changing the resolution of the images (e.g. 640X480 or 800X600). Digital signals are very adaptive and do not create any discrepancies in the image if the resolution is changed.

Power supply

Monitor is the only component of a computer that relies on its own power supply, i.e. power supply is built-in within the monitor itself and is not external to it. However, in the older models the power supply for the monitor was integrated with the main supply. The advantage of such a system that was, the monitor would get switched off on its own when the main supply is switched off.

Monitor case

All the above mentioned components i.e. the CRT, internal electronics, power system etc. are encased in a plastic box that protects the internal components. The external case is designed with small slots in order give way to the tremendous heat that is generated by the internal components. It is very important to keep these slots open to let the internal components cool down, failing which, the monitor could overheat and malfunction.

Display power management system

Monitors work at high energy levels, thereby generate tremendous heat and radiation. Display power management system manages and regulates power supply for monitors. It is used for selectively shutting down parts of the monitor circuitry after a period of inactivity. This way, optimal utilisation of power is ensured.

Answer: [b] Display power management system

Module:3 Reference No:M3144

Question: DVD-R stands for Digital Versatile Disc

- [a] That can be recorded only once
- [b] That can be rewritten many times
- [c] That provides interactive environment
- [d] None of these

Module 3 - Digital Versatile Disc (DVD)

Digital Versatile Disc commonly referred to as DVD is an optical disc storage device which has a greater capacity as compared to CD-ROM discs. It stores seven times more data than a CD (compact disc) can store. Typically, a DVD can store up to 4.7 gigabyte of data on one of the two sides. Each side of the DVD comprises two layers that amounts to a capacity of 17 gigabytes of data (i.e. audio, video or computer information). On the contrary, a CD can store only 600 megabytes. DVDs are played in DVD-ROMs.

DVDs (video) are usually designed for full-length movies, due to larger storing capacity. These discs are played in DVD-ROMs.

Data is usually encoded in MPEG-2 format, in order to write and store them on DVDs. The data compression process employs a technique, whereby all the redundant information (such as areas of pictures) does not change. This makes the compression process more efficient. Image quality to a great extent depends on the compression technology employed while writing the data.

DVD formats

Basically, DVDs are of two formats:

1. Physical formats
2. Application formats

Physical formats are the base formats that hold data. For example, DVD-ROM or DVD-R. DVDs specifically devised to store video or audio data come under application formats. *Application formats* that include DVD-video or DVD-Audio formats define how video programs are stored on a disc and played on a DVD-video player. Physical formats like DVD-ROM come in six variations, namely- DVD-R/RW, DVD-RAM and DVD+R/RW. DVD-R and DVD+R can be recorded only once. These are similar to CD-R. Data once rewritten on DVD-R/+R cannot be erased. Hence, these formats cannot be reused. DVD-RAM, DVD-RW and DVD +RW can be rewritten many times. These are similar to CD-RW.

Apart from these basic formats DVDs come in special purpose formats that support interactive game

consoles. These DVDs comprise menus and simple interactive features. For example, games, quizzes and the like.

MPEG -2 (Motion Pictures Experts Group) data-compression, data storing (in digital, audio and video formats) standards are used in DVDs. DVD-videos use MPEG-2 (a standard for full-screen, broadcast quality) to record and store video data.

Advantages of using DVDs

The following features of DVDs make them suitable replacements for CDs:

- The storage capacity of DVDs is far superior as compared to CDs. Typically, DVDs can store up to 17 GB of data in video, audio or digital format.
- DVDs are durable and does not get worn out due to excess playing, thus offer a better way for storing data.
- DVDs are not susceptible to magnetic fields and are heat resistant.
- DVDs offer interactive features through menus that make instant search for a title, chapter or music track possible. This makes DVDs more user-friendly. Compared to CDs.
- DVDs are compact, easy to handle, store and ship.
- Replicating DVDs costs much less as compared to tapes or laser devices.

Answer: [a] That can be recorded only once

Explanation: R stands for Read-only. These discs can be recorded only once and cannot be reused. DVD-RWs are discs, which allow re-recording.

Module:3 Reference No:M3147

Question: ----- component manages the entire printing process

- [a] Spooler
- [b] Printer interface driver
- [c] Printer monitor
- [d] Mini driver

Module 3- Printer organisation and management-part 2

This is the second and the concluding part on printer organisation and management. In the first part we described some of the components and explained a few terms pertaining to printing architecture. This article explains a few more terms and the actual issue involved in the maintenance of the printing architecture in a networked environment.

Definitions-part 2

- **Half toning:** This is a special support provided by the graphics engine to improve the print quality and accuracy of the colour.
- **Print processor:** This acts as an interpreter for the data types that are sent from the spooler. When the task is completed the document is sent back to the spooler.
- **WYSIWYG:** This is an abbreviation for the term 'what you see is what you get'. This term describes an application like word, which displays the document in its print format.
- **Print Router:** This acts as a bridge between the printer and the workstation. This is required only when the document is being printed from a remote printer. The functions of a print router include tracking local printers connected to the remote printer and downloading drivers from servers to the workstation.
- **GDI server:** This is the server, which contains the Graphics Device Interface.

- **Printer driver:** These are a set of files that support a certain type of print services to a particular printer. These drivers are composed of three components or files- the graphics driver, the interface driver and the configuration file.
- **Printer graphics:** This renders the output from the print driver. This is a part of printer driver and is called from the GDI server.
- **Printer interface driver:** This also is a part of print driver. This contains the user interface and is called from the client side of a printer router.
- **Minidriver:** These contain the printer information.
- **Remote printer:** This is a printer connected to another system on LAN or WAN.
- **Spooler:** This manages the entire printing process. Separate spoolers will be available for both server and the client. These two communicate with each other for the printing process.
- **Printer monitor:** This is available on each printing device to indicate the status of the printing job.
- **Printer port:** A port that is used to connect to the printer. For instance the COM1 or a logical port.

Actual usage

Once a printer is created and a print device is available, it is ready to be used. Either multiple devices can be connected to a single printer or multiple printers to a single device. This option will be useful in cases when only some features are available to some users and full features are made available to certain users. This option is more used for control purpose.

Answer: [a] Spooler

Module:3 Reference No:M3148

Question: ----- takes the GDI output from an application

- [a] Graphical device interface
- [b] Graphics engine
- [c] Device driver interface
- [d] None of the above

Module 3- Printer organisation and management-part 1

Printer organisation and management is a very important constituent in any networked environment. The main issue involved is how to maintain the printers on a day-to-day basis and keep them fine-tuned for effective performance. The main challenge involved is not configuration of the individual printers but to balance the load of each printer so that a single printer is not overloaded.

Printing architecture

The objective of this article is to provide an insight on effective organisation and management of printers in a networked architecture. To understand this, it is first important to understand the printing architecture in any networked environment. For instance in a WindowsNT environment it is a modular arrangement which helps in easy management. This means that a print driver is not required to be installed in every NT workstation, it needs to be loaded on to only the server. Some of the terms used in a printing architecture are given below. Some are generic and some are windows product oriented.

- **Printer manager:** The function of a printer manager is creation of new printers on network and management of existing printer.
- **Print device:** The actual physical printer on the network, for instance inkjet is called a print device.

- **Printer name:** This refers to the name of the printer and the software that controls the functioning of the printer. When users see the browse lists, they see the printer's name.
- **Queue:** This is same thing as the printer. The only difference being in Windows NT environment it is called a printer, whereas in the other systems it is called a queue.
- **Network interface printer:** A printer that has an interface to the network directly.
- **Dots per inch:** DPI as it is popularly known, is a term used to define the resolution of the printer. This denotes the number of dots that make up a character or graphic design on the printer. The higher the dots per inch, higher the print quality.
- **Pixels:** This is similar to the dots per inch. But this indicates the resolution of a screen.
- **Graphical device interface:** This is the set of commands that applications give for a printing job. This is the connection between the application and the graphics engine. These commands define both the content and the formats of the print job.
- **Graphics engine:** This is the print processor that takes the GDI output from an application
- **Device driver Interface:** This is the interface between the graphics engine, print processor and the print driver
- **Journal file:** These files contain the commands and data for the print. These are tuned to the individual printer.

This is the first part of the article. The second and the concluding part of the article contains more information on the individual components in a printing architecture and the actual issues involved in the configuration and maintenance of the printers.

Answer: [b] Graphics engine

Module:3 Reference No:M3150

Question: Which of the following is the first step in building storage infrastructure under building block approach?

- [a] Defining business goals
- [b] Categorisation of data
- [c] Setting up a disaster recovery plan
- [d] Identify the importance of data

Module 3- Storage Infrastructure

Introduction

Disasters, whether man-made or natural can strike under various circumstances. In technological milieu such disasters can result in loss of data and can affect the competitive position of the business. Added to this is the cost of damage to reputation and brand image. In worst situations it may even result in closure of business.

Role of storage infrastructure in information recovery post-disaster

Under these circumstances there is an inevitable need for the protection of stored information. A well planned and hence a cost effective storage infrastructure can play an effective role. Building block approach is one such cost-effective method.

Building block approach

1. Define the business goals: Organisation's business goals have to be clearly defined. Top management must

effectively participate in this function.

2. Identify the importance of data: The significance of data integrity and availability must be clearly identified. Because data across the organisation is not equally important. Some applications like transaction systems and data warehouses have to run all the time. In addition, the value of data may change with the passage of time. For example, the data that is not useful tomorrow will not have any value tomorrow. On the other hand, some data may be important for longer period. All this information is essential to set up an effective storage infrastructure.

Building block approach is based on the assumption that there exists bulletproof storage environment. The following are the five components of a bulletproof environment:

1. **RAID storage:** Redundant array of independent risk is a storage system that ensures the data integrity and protection. It is available at various levels with several vendors. The performance, cost, scalability and manageability aspects must be considered before selecting the type and level.
2. **Redundant pipes:** In direct-attached storage and storage area network, redundant pipes are crucial.
3. **Servers and application protection:** Protection of servers and applications is another crucial element. Ensure the protection of servers through redundant heartbeats. Depending on the need for specific applications, support from third parties can be taken.
4. **Backup and recovery:** Backup is essential to protect against any unintentional deletions or human errors. Similarly, backup is of no value if the data is not recoverable. Understand clearly about the process of recovery from the vendor. Further time required for recovery must also be considered. However, selection of approach depends organisation's needs. Therefore, backup and recovery are essential to set- up before establishing a disaster recovery strategy.

Backup is done either on weekly or daily basis. Downtime is essential for full backup. However, a snapshot technology does not require any downtime rather done with little or not disturbances to the applications. It is a general norm to keep the backup tapes at remote site.

Answer: [a] Defining business goals

Module:3 Reference No:M3151

Question: Companies require storage consolidation of huge data for

- [a] Determining the amount of data
- [b] Storing the data in different servers
- [c] Analysis and decision making
- [d] Efficient managing of the data

Module 3- Storage Consolidation

Companies increase their competence by efficiently managing data at the same time reducing waste and cutting costs. This is done by Storage Consolidation. Consolidation is an effective way of streamlining the data-driven applications. There are three types of Consolidation:

1. **Server consolidation:** Shifting applications dispersed in various servers throughout the company to a cluster of centralised servers.
2. **Storage consolidation:** This is of three types
 - i. Shifting of storage in multiple servers to storage on a single server: It reduces administrative complexity and the floor space occupied by the data storage centers.
 - ii. Directly attaching multiple storage servers to a single storage device: This reduces storage costs by creating a single source of high-performance storage for multiple types of servers.

- Therefore doing away with the need of purchasing different storage devices for each server type along with simplifying administration and saving the data centre floor space.
- iii. Grouping storage resources in a Storage area network: With this method a consortium of storage resources is generated and shared among the users. This method enhances the efficiency and reduces management complexity at the same time increasing availability, scalability and data accessibility.
 3. Data consolidation: Shifting of decentralised data on distributed file systems onto a common file system. This results in efficient sharing and ease of management.

Need for Storage consolidation

Businesses, which have extraordinary storage growth and are still using the distributed storage infrastructure, strive to keep up with growing capacity and demanding service agreement levels and enormous costs. The demand for storage consolidation becomes obvious in the following conditions.

- Environments where equipments are very old therefore making it difficult and expensive for components to be replaced.
- When the systems are of different formats and they do not facilitate easy communication with each other. The data has to be replicated, thereby increasing the cost of storage.
- With the growing demand for round the clock availability, data needs to be collected, analysed and protected from disasters. This could be done only with an efficient back up and restore techniques.
- With old systems the administrator cannot manage more than one or two Terabytes of data. This could result in valuable data being left open and unprotected.

Benefits of storage consolidation

- It reduces the floor space required by the data centers to store the data.
- Disaster recovery plans could be done more efficiently.
- Managing and protecting the data becomes easier.
- Improve the network efficiency to which the servers are connected.
- Maintenance costs of the data are considerably decreased.
- Reduces load on server and also the need for general-purpose servers.

Answer: [d] Efficient managing of the data

Module:3 Reference No:M3151

Question: Companies require storage consolidation of huge data for

- [a] Determining the amount of data
[b] Storing the data in different servers
[c] Analysis and decision making
[d] Efficient managing of the data

Module 3- Storage Consolidation

Companies increase their competence by efficiently managing data at the same time reducing waste and cutting costs. This is done by Storage Consolidation. Consolidation is an effective way of streamlining the data-driven applications. There are three types of Consolidation:

1. Server consolidation: Shifting applications dispersed in various servers throughout the company to a cluster of centralised servers.
2. Storage consolidation: This is of three types
 - i. Shifting of storage in multiple servers to storage on a single server: It reduces administrative complexity and the floor space occupied by the data storage centers.

- ii. Directly attaching multiple storage servers to a single storage device: This reduces storage costs by creating a single source of high-performance storage for multiple types of servers. Therefore doing away with the need of purchasing different storage devices for each server type along with simplifying administration and saving the data centre floor space.
 - iii. Grouping storage resources in a Storage area network: With this method a consortium of storage resources is generated and shared among the users. This method enhances the efficiency and reduces management complexity at the same time increasing availability, scalability and data accessibility.
3. Data consolidation: Shifting of decentralised data on distributed file systems onto a common file system. This results in efficient sharing and ease of management.

Need for Storage consolidation

Businesses, which have extraordinary storage growth and are still using the distributed storage infrastructure, strive to keep up with growing capacity and demanding service agreement levels and enormous costs. The demand for storage consolidation becomes obvious in the following conditions.

- Environments where equipments are very old therefore making it difficult and expensive for components to be replaced.
- When the systems are of different formats and they do not facilitate easy communication with each other. The data has to be replicated, thereby increasing the cost of storage.
- With the growing demand for round the clock availability, data needs to be collected, analysed and protected from disasters. This could be done only with an efficient back up and restore techniques.
- With old systems the administrator cannot manage more than one or two Terabytes of data. This could result in valuable data being left open and unprotected.

Benefits of storage consolidation

- It reduces the floor space required by the data centers to store the data.
- Disaster recovery plans could be done more efficiently.
- Managing and protecting the data becomes easier.
- Improve the network efficiency to which the servers are connected.
- Maintenance costs of the data are considerably decreased.
- Reduces load on server and also the need for general-purpose servers.

Answer: [d] Efficient managing of the data

Module:3 Reference No:M3153

Question: In a RF (Radio Frequency) system, the unit that houses both the transmitted and received waves is termed as_____

- [a] Transmitter
- [b] Receiver
- [c] Transceiver
- [d] Transponder

Module 3- Radio Frequency (RF)- Basics

The terms Radio Frequency (RF) and wireless are used interchangeably in practice. This is due to the fact that the term wireless is primarily a marketing term used to describe newer, RF applications, which include things like cellular telephony and paging.. In short it is used to describe a range of frequencies. Some of the basic RF terminologies include watts, frequency, transmitters, receivers, analog and digital signals require

elaboration.

Watts

The unit of measure of power is Watts. Power consumed for a certain time gives energy i.e energy is the product of time and power. For example if a 60-watt light bulb burns for two hours, it equals 120 watt-hours of energy. In the domain of RF, the words power and energy are used interchangeably.

Voltage and current

Voltage is the term related to power, which is nothing but an electric potential. Two kinds exist namely AC (alternating) voltage and is the type found in a wall outlet wiring. DC (direct) voltage is the one found in a battery or pen torch cell. Current is the movement of electrons. Similar to voltage, current can also be made either alternating or direct. Voltage(V), Current(I), and power are related by $P=VI$, (Power is the product of voltage and current).

Circuit and circuit boards

A set of interconnected electrical components makes up a circuit. These electrical circuits are manufactured on something called Printed circuit boards (PCB). A PCB can be commonly spotted inside a computer, VCR, or any other electrical appliance. PCB is a sheet of hard, thin, plastic board with electrical components mounted on it.

Transmitter and receiver

The movement of electrical energy from one place to another takes place in two ways. It can flow as a current along a conductor like a bunch of electrons moving down a metal wire, or it could travel in the air as invisible waves. In a wireless communication system, the electrical energy originates as current flowing along a conductor, gets transformed into waves travelling in the air, and finally gets changed back into current flowing along a conductor again.

Fig: Block Diagram of a general wireless system

In the block diagram above, the electrical signal flows as current along a conductor into the block containing "T". This box T is known as the transmitter, which turns the electrical current into airborne signals or waves. This airborne signal travels at the speed of light and reaches the box marked "R" at the right end. R is known as the receiver, which transforms these airborne waves into electrical current. A combined unit of both the transmitter and the receiver is called as a transceiver, which are suitable for some specific applications.

Answer: [c] Transceiver

Module:3 Reference No:M3154

Question: What does COLD stand for in data mining?

- [a] Crystal Output of Large Data
- [b] Computer Output of Large Data
- [c] Computer Output to Laser Disc
- [d] Crystal Output to Laser Disc

Module 3- Computer Output to Laser Disc

The corporate activities both internal and external (such as communicating to customer) are stored in computer. This is generally in the form of computer documents. They constitute both current and historical

data. These internal reports and outbound customer documents (such as yearly bank statement) are stored in a form, which is standard for electronic storage, retrieval and on-demand printing. This is called as Computer Output to Laser Disc (COLD).

It is generally felt that data storage can be more effectively done online when compared to record oriented system. But documents would still be required for both legal and accounting purposes. This is because online database cannot serve the purpose of recording an individual transaction like accounting. Customer documents such as telephone bill, bank statement, utility bills are required to be stored for more than seven years for record.

The data in the document appears to hold up when the user wants to view it in a different format. This because there is no easy way to analyse the data for business intelligence. This scenario can however be changed with Report mining.

Report Mining utilises features of COLD systems effectively. Some of them are:

- Documents in COLD systems are stored in the same page format, which eases the location of data.
- Since the document is compiled at one point of time, the data to be analysed is sure to exist in the document.
- There are no inconsistencies in the report obtained.
- Data can be stored for a long time in COLD systems.

Also, Report Mining activities such as searching, locating and extracting the data from the documents can be done using the row/column document structure. When the data structure is different then the searching can be done independently and the output combined in required format.

For instance, in a bank statement the relevant data is put in a predetermined format. So a text or string needed to be searched in a column say, Deposit would be done without including Withdrawal or account balance. Since COLD systems are known for data stored over a long time, it becomes very easy to analyse the activity of user. The COLD system therefore serves the purpose of becoming a data warehouse that can be analysed with data mining tools.

Report mining doesn't need any new database or additional human resources. It becomes all the more preferred due to

- Free of cost availability.
- Less implementation time when compared to data warehousing and data mining.
- Output reports are high quality database information, which is a major cost element.

Applications of report mining

- In banks, for historical transaction of reports of a customer in ATM (Automatic Teller Machine).
- In brokerages statements to study the purchases of a specific stock.
- For loan tracking. From the monthly statements of customers one can identify the geographic location, where the loan coverage has been high or where it's low.

Answer: [b] Computer output to Laser Disc

Module:3 Reference No:M3156

Question: Which among the following components of a telephone system uses fibre optics?

- [a] Trunks
- [b] Switching office
- [c] Local loops
- [d] Toll office

Module 3- Public Switched Telephone Network (PSTN)

Introduction

International telecommunication system that was built based on copper wires for transmitting analog voice data is termed as PSTN. The telephone system that functions using the PSTN are generally referred to as Plain Old Telephone System (POTS).

PSTN basics

The present day telephone systems that are typical of any wired connections mostly employ POTS. Each telephone has two copper wires at its output. These lines are connected to the telephone company's nearest end office or local central office. The end office could usually be between 1 and 10 Km from the end user and depends on the city. The two-wire connections between each subscriber's telephone instrument and the end office are known in commercial parlance as local office.

When a caller attached to a particular end office calls another subscriber attached to the same end office, the switching mechanism sets up a direct electrical connection between the two local loops. Each of the end offices have a number of outgoing lines to one or more switching centres located in the vicinity called as toll offices. These offices within an end office are termed as tandem offices. The lines connecting the different offices are termed as toll connecting trunks. There are primary, sectional and regional offices that are connected together to form a network. Through this, the toll, primary, sectional and regional offices communicate with each other. High bandwidth intertoll trunks or interoffice trunks enable the connectivity. Various medias are used for telecommunications. Local loops employ twisted pair cables. Switching offices are connected through coaxial cables, microwaves and fibre optics. Signalling was done through analog means in the past wherein voice signals were transmitted as an electrical voltage from a source to the destination. Digital signalling has taken over with the advances in digital electronics and computers. The earlier telephone systems used analog transmission over copper cables and the new systems use digital transmission on optical fibers.

Components

The three major components of a telephone system are:

- Local loops (twisted pairs: analog signaling)
- Trunks (fibre optics or microwave: digital signaling)
- Switching offices

Local loops (Twisted pairs): The local loop connection is established with a modem and codec-Coder/Decoder for digital transmission. Here there is an avenue created with the help of modems and other interfaces to transmit digital data over analog circuits. A lot of other issues connected to local loop connection are transmission impairments (attenuation, delay distortion, noise), modulation, and echo suppressors.

Trunks: The need for economies of scale is an important issue in a telephone system. Therefore, schemes were devised to send multiple conversations by a channel for communication over a single physical trunk. The schemes called as multiplexing in categories like frequency and time division came into existence. FDM (Frequency Division Multiplexing) and TDM (Time Division Multiplexing) paved way for further developments in the form of WDM (Wavelength Division Multiplexing) and SONET (Fiber optic networks).

Switching offices: The two widely used switching techniques are circuit switching and packet switching. The

establishment of a physical connection all the way from the telephone of the caller to the receiver's telephone is circuit switching. In the case of packet switching, data is broken down into bits as packets and sent by a virtual circuit.

Answer: [a] Trunks

Module:3 Reference No:M3157

Question: Which of the following statements is true with regard to buffer overflows?

- [a] Buffer overflows are caused due to programming errors
- [b] When buffer overflows the excess information gets lost
- [c] Only the subroutines will be lost
- [d] All of the above

Module 3- Buffer Overflows

Buffer overflows have been a problem in software-based systems and applications for a long time. A buffer overflow is like trying to put ten pounds of sugar into a container that only holds five pounds. Once the container fills, the rest spills all over the counter and floor, making a mess that somebody has to clean up.

A buffer overflow is possible because the creator of a computer program wrote lines of code that do not properly check the size of the destination area or buffer. If the data intended for its new home doesn't fit and spills over, it too can create a mess that requires somebody's attention, usually the computer's owner or a system administrator. However, a buffer overflow is only a problem if the buffer in question is overflowed. Until then, it is harmless.

When a buffer overflows, the excess information overwrites the previous contents of parts of a computer's memory space. Unless those overwritten contents were saved or can be recreated, they are lost forever.

Among the information lost is the ordered list of subroutines that had been called by the program up until the time when the buffer overflow occurred. In addition, the information given to those subroutines - called arguments - is also lost. This means that the program can't find a way back through the subroutines it needs to complete its programmed task

The problem is really worse than the program simply losing its way. The intruder overflows the buffer with a carefully crafted exploit script (a program written for malicious use) and then tells the program to treat the buffer as instructions and carry them out - execute them. The program does what the intruder wants, not what the programmer intended. In effect, the intruder becomes the programmer because his or her instructions are executed.

Intruders often reprogram an application to run a different program. For example, an intruder can start a new program that sends private files (checkbooks, password files, or proprietary memoranda) to the intruder using email.

Relevance of buffer overflows to a computer system user

Since buffer overflows are a programming problem, they can only be permanently fixed by repairing the broken program code. But however, a user may not have the source code for the applications nor he requires that code along with the responsibility to fix each and every buffer overflow.

The best course of action is to monitor the web sites of the operating system and application vendors,

applying any patches they provide. This can be tricky because installing a patch may cause another application to break, and the user may not likely to know this until he has installed the patch. User must ask the vendor providing the patch if they know of any interoperability problems and also see if there is a way to remove a patch once it is applied. This gives a recovery strategy.

Answer: [a] Buffer overflows are caused due to programming errors

Module:3 Reference No:M3159

Question: In directional antenna, an antenna tower splits the area into how many parts?

- [a] 2
- [b] 3
- [c] 4
- [d] 5

Module 3- Antenna and Antenna Systems

Antennas

Antennas are used to connect electromagnetic energy from one medium (For e.g. space) to another medium (e.g., wire, coaxial cable, or wave guide). The physical design of antennas need not be similar and could vary greatly. There are basically two different types of antennas. Omnidirectional antennas and Directional antennas.

Omnidirectional antennas: This antenna radiates and receives signals from all directions. It broadcasts signals in the form, which appears like ripples in a pool of water moving from the centre towards the end. It doesn't require the knowledge of user's location and reaches the user with only small percentage of the total energy actually broadcasted into the environment. In order to overcome the loss of energy, the antennas boost the power level of signals. When there are numerous users in the area, this could be a potential disturbance when it misses the intended users and becomes an interference for the users in the adjoining sector.

While uplinking , that is when user has to connect to the base station, omnidirectional antennas cannot differentiate and selectively reject the signals of the intended user from those of others. The spectral efficiency is greatly affected by omnidirectional antennas and therefore limits the frequency reuse.

Directional antennas: This antenna is designed to have certain preferential transmission and reception directions. Instead of adding a new transmitter sites, antenna towers split the direction of transmission into sectors or cells. A 360 degree area is split into three 120 degrees and smaller antennas are used to cover them. Sector antennas provide more gain over a range when compared to omnidirectional antennas. Though sector antennas multiply the use of channels, the general question of co-channel interference is still left unanswered.

Antenna Systems

In order to increase the functionality of antenna, its physical design is modified by adding more elements. The antenna is turned into antenna system that is capable of shifting signals prior to transmission at each of the successive elements. This gives the antenna a composite effect. This process of hardware and software in order to increase the effectiveness of antenna is called Phased Array Antenna

An antenna with more intelligence can be developed in a phased manner.

Sectorised System: The sectorised system sub-divides a given area into sectors and covers each of them using directional antennas. Apart from being treated as a different cell, the range of antenna in each sector also increases. This helps in increasing the reuse of a frequency channel by reducing potential interference across the original cell. With more than one directional antenna, the base station can easily cover all the directions.

Diversity system: In this system, two antennas are kept at base station with slight physical separation. This improves the reception by neutralising the negative effects of multipath. Diversity systems improve effective strength of signal two methods.

Switched diversity: This assumes that one of the two antennas is always in a favorable location at any point of time and therefore switches between the antennas, which receive the best signal.

Diversity combining: It corrects the phase error in two multipath signals and combines the strength of two signals to produce gain.

Answer: [b] 3

Module:3 Reference No:M3161

Question: Transmission of signals in a finite number of fixed, predefined patterns with high sensitivity is done in which of the following?

- [a] Adaptive Array Antennas
- [b] Switched Beam Antennas
- [c] Unlink Process
- [d] Downlink Process

Module 3- Smart Antenna Systems

A smart antenna system is a combination of multiple antenna elements with digital signal-processing capabilities, which helps in receiving and transmitting signals automatically in response to the signal environment. It alters the radiation patterns to counter its signal environment automatically. This helps in increasing the performance of wireless systems. Smart Antenna Systems are of two types:

1. **Switched Beam Antennas:** In this type of Smart Antenna System, signals are transmitted in a finite number of fixed, predefined patterns with high sensitivity. They detect signal strength and then select one of the many predetermined fixed beams. The antenna systems swap from one beam to another as the mobile moves throughout the sector.
The switched beam systems do not shape the antenna pattern with metallic properties and physical design. Instead they combine the outputs of multiple antennas so as to form a beam with more chances of selection of signal. This approach is better than the conventional single-element approach.
2. **Adaptive Array Antennas:** This is regarded as the most advanced smart antennas approach. It uses various signal-processing algorithms and effectively locates and tracks different types of signals. It then dynamically minimises the interference and maximises the chances of intended signal reception.

Both the systems are supposed to increase in accordance with the users location. But it's only the adaptive system, which provides optimal gain at the same time identifying, tracking and minimising interfering signals.

Architecture of Smart Antennas

The switched beam and adaptive array systems facilitate base station to adapt the beams generated for every remote user effectively through internal feedback control. For this each system forms a main lobe towards individual users and tries to reject interference or noise from outside of the main lobe.

Up linking Process: In this process signals are received from the user, which is similar to listening on a cell. Lets assume that smart antenna is employed at base station and not at handset or subscriber unit. Transmission is done in such cases using omni directional antennas. The base station has to selectively separate the desired signals from interference. The received signal is multiplied by a weight, to make a complex adjustment of amplitude and a phase. These signals are combined to yield the array output. An adaptive algorithm, according to predefined objectives, controls the weights.

Downlink Processing: Switched beam and adaptive array systems are differentiated on the basis of transmitting in a spatially selective manner. The switched beam systems connect with users by changing between preset directional patterns, on the basis of signal strength. While, adaptive arrays connect to the RF environment more broadly and transmit more selectively. This process depends on system used such as time division duplex (TDD) or frequency division duplex (FDD).

Smart antenna systems help in improving wireless system performance and economics for a range of potential users. It enables operators of cellular, and wireless local loop (WLL) networks to realise significant increases in signal quality, capacity, and coverage.

Answer: [b] Switched Beam Antennas

Module:5 Reference No:M5067

Question: The answer sheets in most examinations require the candidates to answer by marking the correct choice. This kind of data is converted into computer readable form through:

- [a] Optical Character Reader (OCR)
- [b] Optical Mark Reader (OMR)
- [c] Magnetic Ink Character Reader (MICR)
- [d] None of the above.

Module 5 - Scanning Devices

There is so much of business-related data and information on paper that most of us would have difficulty imaging the amount. Before many of our modern input devices and systems were available, a lot of research was devoted to eliminating the expensive and time consuming steps of feeding all the data on the hardcopy manually by keying it in. As a result, **Optical Character Recognition (OCR)** input devices were developed to read hardcopy data from the source documents into computer-usable form. Today these devices use light-sensitive equipment to scan bar codes, optical marks, typewritten characters, handwriting and magnetic ink. Let us see some of the common scanning devices.

- **Bar code readers:** Bar codes are almost everywhere, be it on groceries, cosmetics, novels, audio cassettes and so on. Bar codes are recorded on the product by the manufacturers and usually carry the inventory stock number. This coding scheme, called Universal Product Code, for recoding the data is based on the width of the bars and the space between them. Two types of devices are used to read the bar codes. The first is a hand-held scanner that is passed over the tag that carries the bar code. The second is found mostly in supermarkets and is built into the countertop along with a computerised cash register. The person on the counter flashes the product over the glass screen and the code is taken by the system and the price displayed on the screen.
- **Optical mark reader:** When we took some entrance test and marked the correct answers with a lead pencil we were contributing to simplest form of optical data recording. Data recorded in this form is converted into computer usable form by a optical mark reader or OMR. The OMR device has a high-intensity beam that scans the marked sheets and detects the number and location of the pencil marks. This data is then converted into electrical signals for the computer.

- **Typewritten and Typeset-Character Scanners:** For many years, typewritten data on source documents had to be keyed again to be fed into the computer. To help reduce the time and cost involved, certain manufactures developed special fonts to be read by a scanning device. To assist this process, the American National Standards Institute (ANSI) adopted a standard type font called OCR-A for use with special reading devices. However, more expensive OCRs can read a variety of fonts.
- **Handwritten-character readers:** Although the percentage of data recorded by hand has dropped substantially over a period of time, quite a bit o data is still recorded in this way. As technology advanced, designers felt that it would be possible to convert handwritten data into computer usable form. Devices with this capability are the most sophisticated and versatile of the OCR devices. Because handwriting varies widely, specific guidelines must be followed so that OCR reader interprets the characters accurately.
- **Magnetic Ink Character Reader:** An unimaginable amount of cheques are processed each day which makes it difficult to be processed manually. To come over this problem, nowadays almost all banks issue cheques that carry the numbers in magnetic ink. These are then read by Magnet Ink Character Readers or MICR which converts them into computer readable form.

Answer: [b] Optical Mark reader (OMR)

Module:3 Reference No:M3024

Question: Concept of charging an end-user on the number of times he/she has used the software is called:

- [a] Shareware
- [b] Samplers
- [c] Meterware
- [d] None of the above

Module 3 - Combating Software Piracy

Software piracy is an infringement of copyright act and deprives the legitimate software developers of their rights and rewards for the valuable and hard-earned product that they design. The loss of jobs, wages, tax revenues and critical investments in new technologies are just some of the destructive results of software piracy. Piracy harms everyone including consumers, honest resellers, the software industry and the national and local economies. As per last year's estimates, companies incurred a loss of whopping \$12 billion, roughly constituting 15% of revenues. The loss is expected to be more as the Third World economies enter the high-tech age and more use of software and computers comes to the fore.

Software piracy manifests itself in different forms; it is necessary that different strategies be designed to combat each problem separately. Let us now see the how software piracy can be tackled.

Trade Sanctions

This is the most common way to combat software piracy wherein a criminal law is enforced against any kind of misuse of the product. This means that any incident of a party involved in misuse of an organisation's software would be punishable by the court of law. United States has a Special 301 law which guards against copyright and patent. This provides for a negotiation period of a few months between the two involved parties. If the negotiations fail and the accuser is not willing to withdraw, the United States would impose trade sanctions

Legal Action

This is usual course when the issue is between two firms. This has cropped up a debate wherein many of the commonly used algorithms are under the threat of being patented that will hamper their use by software

developers. Many software developers use techniques developed by various organisations or individuals. If these were patented, the job of software developers would be hampered. Government of USA has also framed laws to check large-scale duplication of software products. The law says that duplicating software valued at a certain price and is less than six months old, is considered a crime. Legal action may also be taken against hardware vendors who provide free copies of popular software with first purchase of the computers.

Industry Watchdogs

The above two actions were suitable for low-end users but lacked teeth when it came to high-end users like the industries and corporate. This led to the establishment of two interest groups viz. Software Publishers Association and the Business Software Alliance whose efforts are directed against corporate piracy and industrial piracy.

Copy Protection

Duplicating software and selling it to make profits has always been one of the major ways in which the software has been pirated. As a result many software developers have come up with mechanism that restrict the end user from copying the product on to their system and then making multiple copies of it. For example Microsoft Office comes on 1.7MB diskette in a format that cannot be copied.

Shareware and Samplers

This is an emerging trend in software industry where particular software is distributed for free use only for a particular time period. After the time has elapsed, the free copy of the software becomes useless. This methodology is being encouraged as it prevents misuse of software. A sampler on the other hand provides for only partial features of the software for initial use. If the user is satisfied with its functionalities, the whole product can be purchased.

Meterware

As the name suggests, the use of software is metered. It is just like our telephone connection wherein we have to pay a lump sum amount once a month. The users are expected to dial a billing number that provides billing office with the data as to the software use and the number of times it was run. This has resulted in a shift from pay-per-copy to pay-per use.

Answer: [c] Meterware.

Module:3 Reference No:M3026

Question: Which one of the following can be attributed as a loss as a result of poor network performance:

- [a] Lost revenues
- [b] Lost productivity
- [c] Intangible losses
- [d] All of the above

Module 3 – Network Performance Monitoring

Computers have changed the way business is carried out today and network has become the backbone of any organisation. Apart from the traditional key business areas, technology is now considered a deciding factor between the winners and “also-rans.” Any minor interruption in the operation of the technological cycle may result in substantial losses for the organisation. Business practices of an organisation are directly effected by the network performance and more so in IT organisations. Hence more and more companies are directing their efforts towards ensuring the performance of the network at the desired level on a day-to-day basis.

Network Performance Monitoring

Network performance monitoring is thus defined as the ability to spot network availability and performance problems on demand, before they cause service degradations or critical time loss. Because a network enterprise is complex and always evolving, one must have a good idea of what is happening on the network at a given point of time. Here a few such aspects.

- Continuously monitor the network to spot problems in real time.
- Oversee the activity related to each network resource, be it a link, protocol, or application.
- Proactively detect problems before they become user recognisable.
- Be forewarned of sudden changes to respond appropriately.
- Resolve problems quickly to reduce the time it takes to close IT trouble tickets.
- Leverage information from multiple data sources, such as switches and routers, that have embedded statistical data so as to easily track all network errors.

Cost of Poor Performance

Organisations must understand and also spread awareness among its members that even a little slack on the part of the employees could cost the organisation dearly. Let us now see the various areas that are liable for losses consequent to the failure of network.

- *Revenue*: This is the actual money lost for not keeping pace with the transactions because of unavailability of network. For example, a financial transaction that could not be updated on to the network stopped extra money being invested in some savings that could have earned higher profits.
- *Productivity*: There is also loss of productivity with inconsistency in service due to unavailability of the network. If a manufacturing organisation practising "just-in-time" production has a network failure, its inventory would not be updated at real time, which would create a bottleneck and hamper the entire production process.
- *Intangibles*: There are always some losses that are difficult to measure simply because they do not seem apparent. These, for instance could be in the case of online shopping marts that may lose valuable business because the website was slow and the network was down.

Ensuring High Performance

If the organisation aims for growth in business as well as stature, it has to ensure that all the integral parts of business work in strong cohesion with each other. Network performance is one such area and needs thorough monitoring to ensure high standards. There are a few points that should be remembered while monitoring a network performance. They are:

- Restoring service as quickly as possible and having as minimum a downtime as possible.
- Identify degradations in the network before they become obvious and replace or repair as demanded.
- Conserve bandwidth to ensure fast connectivity with the customers as well as other clients on the same network.

Answer: [d] All of the above.

Module:3 Reference No:M3027

Question: Network Capacity Planning comprises the following three activities:

- 1) Predicting future utilisation
- 2) Gathering data over time
- 3) Establishing baseline

Arrange the above in the order in which they are performed:

- [a] 1,2,3
- [b] 3,2,1
- [c] 1,3,2
- [d] 2,1,3

Module 3 – Network Capacity Planning

Capacity planning is the process of determining current usage of server or network resources, and tracking utilisation over time to predict future usage and the additional hardware that will be required to meet projected levels of utilisation. Capacity planning can be performed on a single computer, such as a network server, or it can be performed on an entire network.

Methodology

Two methods are commonly used to perform capacity planning. One method involves determining current server/network utilisation to predict future utilisation. The second method involves simulating the expected future utilisation using various tools. These tools, which are sometimes called stress test tools, can simulate specified levels of server utilisation and/or network traffic to determine how current hardware responds to the expected future levels of use. In this discussion on network capacity planning we will study closely the first method.

The basic steps involved in capacity planning as per the first method are:

- *Establishing a baseline:* Establishing a baseline is equivalent to determining current server or network utilisation and performance that is the first step in predicting what the future environment might be like. Data gathered in such a manner establishes an initial baseline about the server or network. Gathering of data should be uniformly spread over a period of time to obtain an overall picture of utilisation. For example, data should be collected during business hours when network usage is at its peak and production is heavy. Similarly, data should also be collected during non-business hours when network utilisation levels are relatively lower. Also, data should be gathered on different days of a week to account for cyclical business highs and lows.
- *Gathering data over time:* Once a baseline has been established, the next step in capacity planning is to continue gathering data over time to obtain additional statistics that can be later used for trend analysis. A reasonable period of time for gathering data depends on many factors, like:
 - o The amount of time that can be dedicated to capacity planning tasks.
 - o The changing skill levels of users in the organisation.
 - o The nature of organisation, particularly if the company experiences seasonal peaks and lows during the course of its operating cycle.

The most important factor is that, data should be gathered frequently enough so that reliable trend analysis can be performed.

- *Predicting Future Utilisation:* Once the baseline has been established and data gathered over a period of time, the next step is its analysis to predict future utilisation. Often, raw data isn't extremely useful for trend analysis. It is usually beneficial to export the gathered data in a suitable format like spreadsheets, graphs and the like. These graphs can then be extended to predict future server or network utilisation.

Answer: [b] 3,2,1.

Question: In context of expert systems, moving down to the symptoms from a fault is called as

- [a] Forward chaining
- [b] Forward integration
- [c] Backward chaining
- [d] Backward integration

Module 3 – Expert Systems

An expert system is the highest form of management computing. While office automation allows the communication and manipulation of documents, experts systems go a step further and allow the experts to teach computers about a specific field and so that they may support in decision making process. Expert systems represent one of the most advanced features of information technology.

Components of Expert Systems

Expert Systems use knowledge and interface to solve problems that crop up time to time. They do this by storing large amount of factual information on a subject area. Let us now see the different components of an expert system.

User Interface: This allows the user to interact with the system. The user presents the problem and has the solutions presented to him. There are different ways in which a dialogue takes place between the user and the system. The most common instance is the one in which the system runs a session in which a set of questions are fired to the user. The user in turn has to reply with relevant information. Here all the initiative lies with the system because it runs the whole show. The ultimate interface would be one allowing the user to take all the initiative.

Interface engine: The interface engine is that part of the program which reasons and determines the application of knowledge in the knowledge base to the facts presented in the user interface. Interface engine is the active component of an expert system and its main job is to mimic human reasoning so that the user can understand why the system has chosen the step it has. It applies two basic methodologies:

- Backward chaining: Here we start with an error and then reason backwards to arrive at possible symptoms.
 - Forward chaining: Here the reverse action is taken. The system starts with what it has to offer and then reasons forward to determine what it can perform.
- Techniques for reasoning with uncertain data input are integral to the interface engine.

Knowledge base: This is the most important element of an expert system since it holds the expert problem solving knowledge. The key to the knowledge base is the way knowledge is represented. The knowledge acquired from the expert has to be represented formally. Knowledge representation deals with structuring of information and ways to manipulate it to infer additional data.

Difference between conventional and expert systems

Although most computers today perform the tasks according to the decision logic of conventional programs, these programs do not accommodate significant amounts of knowledge. A program consists of two distinct parts: algorithms and data. Knowledge systems on the other hand collect knowledge in a knowledge base and have no fixed set of algorithms to go by.

Answer: [c] Backward chaining

Question: Network-based Intrusion Detection Systems cannot do which of the following:

- [a] Filter and analyse packets over a network
- [b] Operate in Real-Time
- [c] Match against database of known "attack signatures"
- [d] Recognise new types of attacks

Module 3 - Intrusion Detection Systems I

Many organisations have an online presence that is slowly rivalling the physical one in terms of complexity and functionality. Through the Internet, a person has access to the organisation's important and often confidential data. This makes it more interesting for criminal activities or unauthorised access attempts. Intrusion detection systems (IDSs) can provide protection against unauthorised access.

Firewalls are the first line of defence measures required to protect the network. However, they can only filter incoming traffic from the Internet and hence can be bypassed. For example, through an unauthorised and undetected modem, external users can connect to the internal, bypassing the firewall. An IDS monitors computer systems and the network traffic, and analyses that data for possible attacks from outside the organisation. It also monitors any system misuse or attacks from inside the enterprise and alerts administrators of such unauthorised activity.

There are mainly two primary types of IDS software: host-based and network-based.

Host-based system

In Host-based IDS, the software is installed on the server. It monitors the server and some application logs for unauthorised access attempts and unusual behaviour patterns. The administrator writes the host-based rules or "signatures" that the IDS tries to match when it analyses the traffic through the server.

For example, it may issue an alert if a sales clerk attempts to access payroll data. It may also analyse information for abnormal activities, such as a malicious user trying to repeatedly login attempts.

However, host based IDS software has its own restrictions. Since the systems use event logs, they cannot operate in real time, but work only after the event has occurred. Consequently, these systems are not fully able to minimise false positives, while effectively detecting intrusions.

False positives are alarms raised by the system even though no actual intrusion has taken place.

Network-based system

This type of IDS runs on LAN servers and acts as a sensor. It filters and analyses network packets in real time. It also compares them against a database of known "attack signatures" or patterns. The attack signatures are known exploits that have occurred previously to penetrate a network.

The four techniques used to recognise attack signatures are:

- Pattern or byte-code matching
- Threshold crossing
- Correlation of lesser events and
- Statistical anomaly detection

If the packet contents match an attack signature, the IDS detects and takes appropriate measures. These can include issue of alerts to an administrator, creating a log or record a network session. More aggressively, it can terminate a connection or automatically reconfigure the firewall to block the source IP of the offending packets.

Protocol analysis signatures can also be designed to overcome attempts by attackers to hide their real intentions. For example, hex encoding can be used to slightly modify URLs so that they appear different to us but have the same meaning to Web servers.

This signature type of analysis produces a low rate of false positive alarms, but cannot recognise new types of attacks. Therefore, these types of systems must be periodically updated to remain current.

Answer: [d] Recognise new types of attacks

Module:3 **Reference No:M3060**

Question: Which of the following is true with regard to a good Intrusion Detection System Software?

- [a] It can investigate intrusions without human intervention
- [b] It can compensate for exploits based on errors in network protocols
- [c] It is able to resist unauthorised modifications to itself
- [d] It is able to analyse all of the traffic on a busy network

Module 3 - Intrusion Detection Systems II

An IDS monitors computer systems and the network traffic, and analyses that data for possible attacks from outside the organisation. It also monitors any system misuse or attacks from inside the enterprise and alerts administrators of such unauthorised activity.

Some of the various activities that an IDS can perform are:

- Monitoring and analysis of user and system activity
- Auditing of system configurations and vulnerabilities
- Assessing the integrity of critical system and data files
- Recognition of activity patterns reflecting known attacks
- Statistical analysis for abnormal activity patterns

An example of how an IDS catches malicious intrusion attempts or malicious code is checking for Email containing a particular virus. The IDS compares the subject of each email to the subject usually used by the virus, or it can look for an attachment with a particular name.

As with other measures, it should be recognised that an IDS by itself doesn't assure complete security. Despite having effective signature analysis mechanisms, an IDS cannot do all the security work itself. Some areas where an IDS has shortfalls:

- The IDS requires complementary support of strong authentication mechanisms. Passwords, smart cards or biometric devices can serve the purpose.
- It cannot investigate intrusions without human intervention
- It cannot compensate for exploits based on errors in network protocols
- Due to resource constraints, an IDS may not analyze all of the traffic on a busy network
- It cannot deal with modern network hardware and features

Further, an IDS is not a replacement for a good security policy. It is an element that functions along with other security products as per the corporate security policy.

How to select a good IDS

An IDS should be able to do the following, irrespective of what category it belongs to:

- It must run continuously without human supervision
- It must be fault tolerant in the sense that it must be able to withstand a system crash. If the system crashes, its knowledge-base must be intact so that it doesn't start from scratch again
- The IDS should be able to resist unauthorised modifications to itself
- It must not consume lot of system resources and slow down traffic
- Deviations from expected behaviour must be logged
- The IDS should be adaptable to the system, since every platform and network has its own traffic patterns

Some network IDS products do not provide much customising ability to modify existing signatures or write new ones, while other IDS products gives users the ability to adapt the signatures to the specific needs of the organisation and also write almost any new signature. Further, some IDS products can only check certain header or payload values, while other products can give you the data from any portion of any packet.

Economic issues

Financial institutions such as banks and other financial services companies and those having high-availability networks are the major users of IDSs. As IDS technology evolves, IDS vendors have begun incorporating intrusion detection management into a centralised network management system. This will help administrators detect intrusions and manage the network from a single computer.

Best Security practices suggest using a layered approach to computer security. With companies facing an increasing number of external and internal attacks, IDS is gradually gaining wider application. As a result, it simplifies the promotion and sale of IDS to the top management.

An IDS can help develop security policies. Many vendors provide IDSs with a full suite of security protection. A company devoid of fully developed policies can take up the guidelines included in many IDSs.

The standards for IDSs are still in the process of development as it is an emerging technology. The Internet Engineering Task Force (IETF), the Intrusion Detection Working Group (IDWG) and the Common Intrusion Detection Framework (CIDF) are working towards establishing standards.

Answer: [c] It is able to resist unauthorised modifications to itself

Module:3 Reference No:M3062

Question: Banking organisations make use of which form of data processing?

- [a] Batch processing
- [b] Online processing
- [c] Time sharing
- [d] Remote job entry

Module 3 - Data Processing System

Technology has produced many forms of data processing. Today, a company can select a type that is perfectly suited to its needs. The management must decide which hardware and data processing approach to adopt- a decision that will dictate the day-to-day functions of the data processing department, and how users will receive their computer-prepared information. Let us take a look at the various forms of data processing methodologies available to an organisation.

- **Batch processing:** It is a widely used technique that involves regular processing of huge amounts of data. In batch processing, data is collected for a predetermined period of time, after which it is processed. This kind of processing is used when reports have to be generated on a periodic basis and the system does not require up-to-date information at any given point in time. This can be better understood with the help of an inventory management system.
An inventory clerk collects data over a period of time. This includes invoices, receipts and total count of all items sold. The clerk then verifies all the data and transfers it to a form. After an entire week's forms are collected, a data entry operator feeds it into the organisation's database. The updated inventory file appears in the inventory report which is produced after batch processing of data for each week.
- **Online processing:** Batch processing requires data to be accumulated before it is processed by the computer, creating a delay between the transaction and its processing. Current technology can shorten this delay and process data almost immediately by making use of special hardware. These online devices allow direct communication with the computer and an uninterrupted flow of input data. When a customer deposits an amount into his saving bank account it is processed online and shown immediately in his balance so that he can use the amount when he wants.
- **Time sharing:** This form of online processing allows the concurrent use of a computer by a group of individuals and is called time-sharing. Many users share the resources of a computer at the same time and time-sharing allows many users to concurrently access the same computer. The users can create a link to the central computer using a device called a terminal having a keyboard for inputting data and a monitor for display of data. This link could be established using network cables (for a LAN) or leased/ telephone lines (for a WAN). Once the link is created the user can access a particular program while another user works on a different program on another system. The computer's speed of operation lets it jump from one program to another, and process each task in the order in which it was received.
- **Remote job entry:** Time-shared processing represents a type of telecommunications operation in which a remote job entry (RJE) station (a device permitting transfer of data from a remote location to a distant computer via telecommunications) is used. An RJE may use a keyboard for online processing. As processing occurs information may be transmitted back to the RJE as a printed report. RJE stations often have a terminal to expand a device's ability to handle input and output operations.

Answer: [b] Online processing

Question: Which of the following is not necessary in the policies and procedures related to computer incident, intrusion and emergency response?

- [a] Procedure for risk assessment
- [b] Person to be in charge for handling the publicity
- [c] Person to be contacted in case of emergency
- [d] Audit procedure to be followed by the auditor

Module 3 – Computer Incident, Intrusion and Emergency Response Audit Program

As a part of the audit program, an auditor may have to audit incident, intrusion and emergency response. The auditor during the audit has to ensure that a team is formed, is functioning as desired and is effective.

Policies and procedures: The auditor before commencing the audit should first review all the policies and procedures. He must ensure that the policies, procedures and relevant documents include the following at least.

- Procedure for risk assessment
- Basis for classification of information
- Procedure for identification of the incidents, intrusion and emergencies
- Persons to be contacted in case of emergencies
- Person in charge for handling the publicity/ information to stake holders
- Person to contact the law enforcement
- Recovery procedure

The auditor should evaluate the policy and ensure that it is consistent with the industry standards and best practices.

Distribution: The policies should be distributed to the concerned individuals in the company. The auditor must review such a distribution.

Updates to the policy: It is necessary to ensure that the updates to the policies are as per the prescribed procedures. The auditor must take a sample during the audit period and evaluate whether the prescribed procedure has been followed. He may interview a few individuals to confirm the receipt of policy and that, they are aware of its contents.

Policies are current: The policies should be current and it has to be ensured that the management carries out a periodical review (say quarterly or half yearly) to ensure that they are current and in accordance with the business functions. The auditor should select a sample of the policies to ensure the same.

Risk assessment

Management has the primary responsibility towards risk assessment. The auditor should ensure that the risk assessment process is defined in order to identify the assets that should be protected, the threat that the company is vulnerable to and risks that the company will face if the assets are not protected.

Projects: Whenever a new project is undertaken the risk assessment process should be performed. The auditor should select a sample of new projects to review whether risk assessment was performed on the new projects and it identifies all the threats, incidents and vulnerabilities that the project may be exposed to.

Current environment: The current environment needs periodical review to determine if any new threats and vulnerabilities have arisen after the last assessment. The auditor should evaluate last reassessment of the current environment. He should confirm that the process includes the reassessment of initial assumptions, identifying the chances since last assessment and the future plans.

Answer: [d] Audit procedure to be followed by the auditor

Module:3 **Reference No:M3080**

Question: Which of the following is TRUE with regard to audit of computer incident, intrusion and emergency response audit?

- [a] Auditor should ensure that proper procedure is followed for purchase of tools
- [b] The tools are given to all the employees of the company
- [c] IT auditor should not form part of the response team
- [d] The employees should be trained in all the tools that are available in the market to deal with the incidents

Module 3 – Computer Incident, Intrusion and Emergency Response Audit Program – Part 2

This is concluding part of the series on computer incident, intrusion and emergency response audit program. The earlier article covered the evaluation of policies and procedures and risk assessment. This article covers review of

- Inventory Tools
- Training of employees
- Roles and responsibilities of key personnel
- Escalation process

Inventory of tools

The management needs certain tools for handling the incident, intrusions and emergencies. The tools should help in network monitoring, authentication, scanning for known vulnerabilities, reporting, integrity checking and the like. The auditor should obtain the inventory of the tools that have been purchased. The inventory details should include the name of the tool, date of purchase, manufacturer, duration of maintenance contract, the date of replacement, if any, and other relevant details.

Purchase: While procuring new tools, the auditor should ensure that a proper procedure is followed for purchasing them. These tools, whose purchase is approved by the appropriate authority, must be advanced.

Replacement: Whenever the tools are replaced the auditor should ensure that they are replaced with more sophisticated ones or at least the tools with same performance standards as those being replaced. Proper authority must sanction the replacement of tools.

Updates and patches: The auditor should ensure that there is a procedure defined for updates and patches for the current inventory. The tools should be the current release or a latest version.

The tools that are used should be consistent with the industry standards and best practices.

Training of employees

The employees should be trained to use the tools that the management has purchased for tackling incidents, intrusions and handling emergencies. The auditor should ensure that the management has provided the requisite training to the concerned employees. He should obtain a list of employees trained, and the tools they are entitled to use. The tools that are being used by the employees should correspond to their training. He should also evaluate the procedure followed for assigning the tools to employees when they are promoted, resign or retire.

Roles and responsibilities of key personnel

The incident, intrusion and emergency team should include personnel from security team, network team, law department to deal with frauds and legal cases, IT auditor. The auditor should ensure the inclusion of representatives from every team. He should also interview few of the personnel to ensure that they understand their role and responsibility.

Escalation process

The auditor should evaluate the escalation process and whether the same was followed during previous incident, intrusion and emergency. The escalation process should include the occurrence of the incident, intrusion or emergency, securing the lines of communication, notifying the concerned employees, recovery, appropriate legal action, publicity and the like.

Answer: [a] Auditor should ensure that proper procedure is followed for purchase of tools

Module:3

Reference No:M3014

Question: A successful project management practice involves training a project team to achieve desired goals. Under which process does this fall?

- [a] Planning
- [b] Organising
- [c] Controlling
- [d] Leading

Module 3 - Project Management Process

Project management involves planning, organising, staffing, directing, and controlling some parts of the organisation for a relatively short period of time. All these activities revolve around a few basic processes which when performed synchronously form the basis of project management. Project management consists of five basic activities. They are:

Planning

Planning takes place before the commencement of the project. It revolves around reviewing, confirming, and refining the feasibility study. The principal object of planning is to ensure that the project gets off to a good start. It involves a few tasks:

- A feasibility study, which is a report that details the cost, benefits, schedule, and budget for the project.
- The project manager should review and refine initial assumptions and estimates and update the feasibility study as the project progresses. There should be checkpoints at regular intervals to determine if the project should be changed according to updated estimates and assumptions or if it should continue as planned.
- The final step in project planning is to obtain the approval of the management before proceeding with the project. The approval process should ensure that the management, users, and team members understand and accept the approach and the scope of the project.

Organising

Organising the project includes developing a detailed project work plan, defining project standards, establishing project initiation, and training the team. Proper organisation will contribute significantly to the smooth functioning of the team and to the overall success of the project. Additional criteria for successful project organisation are detailed as follows:

- The project's organisational structure should be well defined with responsibilities and lines of authority clearly stated.
- People having the necessary programming knowledge and technical skills should be assigned to the project team.
- Training of the team should be conducted during the organisational phase.

Controlling

Controlling a project is the most challenging responsibility in project management. It is also time-consuming and often difficult. The process itself involves capturing progress data, preparing project control reports, developing an action plan, and managing project scope changes.

- Project control should be an iterative process. It should continue throughout as the plan and organisation of the project may be adjusted.
- The project manager should have timely and accurate information in order to control the project schedule, budget, performance, and direction.

Leading

Although less tangible than planning, organising, and controlling, leading is the primary role of the project manager. In fact, it can be the most significant management function. The way a project manager deals with team members involved can create a spirit of cooperation that is essential to the project's success. Effective people management for a project should include the following:

- Motivating team members
- Delegating and assigning work
- Recognising good work

Concluding

Concluding a project is the most important milestone: all segments of the system are completed and frozen, and the transition from the current project to the next projects begins. Criteria for successful project conclusion should include the following:

- All open issues should be resolved or deferred
- Acceptance tests should be successfully completed, verifying that the management and the users accept the system
- A transition plan should be implemented
- Post-implementation evaluation should be conducted.

Answer: [b] Organising.

Module: 4 Reference No: M4001

Question: Which one of the following is not an essential feature of LAN?

- [a] Range
- [b] Transmission Technology
- [c] Topology
- [d] Routing

Module 4 - Local Area Network

Local Area Network or LAN is an arrangement of computers and peripherals in a limited space. It is used extensively to share resources and exchange information. A network has a central computer that is known as the "server". The server has software that helps in controlling and operating the entire network. There are different types of LANs for example AppleTalk from Apple, Windows NT from Microsoft and the like. Here are a few characteristics that differentiate LAN from other networks.

Range of the network

Since LANs are owned mostly by private entities, they are generally confined to a single building or a few kilometres in area. The advantage is that the transmission time under the worst scenario is known in advance simplifying the task of network management.

Transmission technology

Most LANs often use a single cable to transmit data to all other systems that are connected to the backbone (as in bus topology). Earlier LANs used to operate at a speed of around 10 -100 Mbps (Mega bits per second) and had very low delay time i.e. time difference between the data sent and data received. But nowadays LANs operate at very high speeds, up to a few hundred Mbps.

Topology

LANs may differ on the topology they implement i.e. the way terminals are arranged in a network. Different mechanisms are in place to monitor and control the flow of data across the network. Let us consider an example wherein terminals are connected in a bus topology. In such an arrangement, only one terminal is the master at a given point of time and is allowed to transmit.

Routing

Routing is a technique used to connect two or more LANs. If a LAN has to connect to a network outside, it requires a router. Router does not form an essential part of a LAN because there may be networks that do not need to connect to other LANs outside.

Advantages

1. Presence of a LAN improves communication within the organisation. Various services like messaging and mailing help in creating a fully automated environment.
2. Standard software like virus-protection, word processors, spreadsheets database programs are stored on the central server and can be accessed by all users. It is cost-effective, as separate copies of the software do not have to be installed on each terminal.
3. With the help of LAN, terminals can be arranged to form a learning site. One of the terminals is assigned to be the master while the rest are considered students. A program that is run on the master is visible to all students.

Disadvantages

1. For a LAN to run smoothly, it requires a competent network administrator who understands its operations. Any negligence on his part can prove to be disastrous.
2. Installing a LAN is a costly affair and depends on various factors like the number of terminals to be linked, required bandwidth and the like.
3. Special security features have to be integrated into the network to ensure that the data is not misused.

Answer: [d] Routing

Module:4 Reference No:M4002

Question: Expansion of a network is easiest if the topology employed is:

- [a] Bus
- [b] Ring
- [c] Star
- [d] Mesh

Module 4- Network Topology-TypesNetwork Topology

Topology is a mathematical concept that deals with different types of geometric shapes. In networking, topology refers to different ways in which computers can be connected. Topology can be considered as the "shape" of the network, but this shape does not adhere to the physical layout of systems in a network. Topology is not merely a pattern of connecting nodes, but also a contributing factor to the cost and performance of a network.

Types of Network Topologies

We have four basic kinds of topologies. They are:

Bus Topology

This is the most basic kind of network topology that is implemented in most LANs. Bus networks use a common cable called the backbone or the trunk. It has a single communication medium that is shared by all terminals connected on the network. Systems are connected to the backbone using "drop" cables that branch out from the backbone. A system seeking to communicate with another system on the network will transmit its message through the medium with the address of the intended system. This message will travel through the entire network and will be available for all systems to see. The terminal matching the address that the message is carrying will accept it, while the rest will let it pass without any interference. One of the drawbacks of this topology is that it is difficult to increase the number of terminals because as the traffic increases, the speed of data transmission decreases. The bus topology is passive which means that the systems on the bus merely 'listen' the incoming signal and are not responsible for movement of signals between terminals.

Ring Topology

Ring topology is a very popular method of configuring the network. Every terminal in this kind of framework has exactly two neighbours for the purpose of communication, one on either side. Under normal circumstances, dataflow is unidirectional, either clockwise or anticlockwise. The terminals are connected to each other in the form of a ring. Data to be transmitted is sent to the neighbouring terminal that will pass it on to the next terminal in the chain. Every system on the ring has equal access to all the other systems, but only one of them is allowed to 'talk' at a given moment. The drawback of this architecture is that if one of the systems forming the ring fails, the entire network comes to a halt. Ring topology overcomes the passive nature of bus topology in the sense that it not only transmits data to the next terminal, but also 'boosts' the signal before transmitting.

Star Topology

Star topology features a central connection unit called the hub. All terminals are connected to the central hub via cables, which means that there is a higher requirement of cable, increasing the cost of implementing a star topology. But the advantage is that even if one system breaks down, it will not affect the entire network. Since hubs have expansion slots, expanding the network is quite easy because all that has to be done is to plug-in a terminal into the central hub. Like others, this too has its disadvantages. If there is a problem with the central hub, the entire network comes to a grinding halt.

Mesh Topology

This is a combination of all the topologies that have been mentioned, and is thus referred to as hybrid topology. In this, almost all terminals are connected directly to each other and hence several routes of communication are possible. Since it does not have a central hub, and there are alternate routes available, it is not bogged down by bottlenecks that are created in other topologies. This is extremely expensive when compared to other topologies. It is suitable for large networks because it is very reliable. Typically, WANs like the Internet employ mesh routing.

Answer: [c] Star

Module:4 Reference No:M4004

Question: In WAP, the actual transfer of data is done by the _____

[a] Bearers

[b] Session Layer

- [c] Transport Layer
- [d] Transaction Layer

Module 4- Wireless Application Protocol (WAP)

Wireless stands for any communication that does not use the conventional wire connection, but uses electromagnetic waves as a medium. WAP as a technology bridges the gap between the mobile world and the Internet, and provides users with appropriate information whenever and wherever they want.

The term "WAP" in itself is misleading for it is not a protocol, but comprises multiple protocols and network architecture that provide value-added services along with a wide range of information. A WAP Forum was set up in 1997. It was backed by several firms that were either using WAP or planning to implement it. This forum officially described WAP as "an open, global specification that empowers mobile users with wireless devices to easily access and interact with information and services instantly". It specifies a method to communicate across wireless networks quickly, efficiently and securely. Such communication can take place using mobile telephones, pagers, personal digital assistants and other mobile digital devices. WAP specifies a layer-based architecture that is commonly called the stack.

The WAP Model

WAP has five different layers stacked one over another. These are:

1. Application Layer

The Wireless Application Environment (WAE) functions as the user interface for WAP enabled devices. Just as the World Wide Web uses HTML, WAP uses WML or Wireless Markup Language for application development. Its scope is limited due to the constraints of memory and display on hand-held devices.

2. Session Layer

The Wireless Session Protocol (WSP) provides a means for organised exchange of content between cooperating client/ server applications. Just as HTTP [1] is for the WWW, WSP is for WAP browsers. HTTP cannot be used for WAP because it operates mainly on data, while WSP works on compact binary data.

3. Transaction Layer

The Wireless Transaction Protocol (WTP) has been defined to provide services necessary for interactive "browsing" (request/response) of applications. During a browsing session, the client requests information from the server, which may be fixed point or mobile, and the server responds with the relevant information.

4. Security Layer

This layer implements the Wireless Transaction Layer Security (WTLS), a security protocol similar to the Secure Socket Layer (SSL) on the Web.

5. Transport Layer

The transport layer implements the Wireless Datagram Protocol (WDP). It is quite like the User Datagram Protocol (UDP)[2] and performs the task of transporting the information packets between the client and the server.

Bearer

Actual transfer of data packets requires physical interconnection or a low level connectivity. This is achieved by bearers that actually carry the data between networks. Since the WDP layer provides the interface between the bearer service and the rest of the WAP stack, the WDP specification lists bearers that are supported by the above protocols.

[1] HTTP stands for Hypertext Transfer Protocol. It gives the specification for transfer of text over the Internet

[2] UDP or User Datagram Protocol that also performs the task of transferring data packets across the Internet. It does not guarantee the delivery of packets.

Answer: [a] Bearers

Module:4

Reference No:M4005

Question: Which of these is not a benefit of data warehousing?

[a] Data creation

[b] Immediate information delivery

[c] Data integration

[d] Business analysis

Module 4- Data warehousing - Concept

Introduction

The growth of a business enterprise demands large volumes of data to be handled on a day-to-day basis. Information systems have to access critical and valuable information resources in a more flexible, effective and efficient manner. In order to do so, companies have adopted a new concept of information storage and retrieval termed 'data warehousing'.

What is a data warehouse?

A computer system developed to give decision makers instant access to information within an organisation is termed as data warehouse. Data available in a central database can be viewed in a comprehensive manner for business and market analysis. The architecture of the database depends on the business model followed by the company.

Data warehousing

Data warehousing integrates hardware and software components to analyse information that organisations store in their database to make better business decisions. Its primary objective is to maximise utilisation of available data within an organisation. It also includes activities that are carried out to maintain a data warehouse.

Any organisation has two kinds of information systems. They are:

- Operational systems
- Informational systems

Operational systems are essential for the daily functioning of an organisation. They comprise critical systems of functions like accounting, manufacturing, inventory and order entry, payroll and the like. These systems require functional data specific to each application. Information pertaining to other functions has little relevance in such systems.

Informational systems are essential to ensure that an organisation can keep pace with the rapidly changing business environment. These include planning, forecasting and analysis of information related to finance, marketing, engineering, business data and the like. These systems require data across functions.

Informational data often span different areas and include large amounts of related functional data.

Information of various departments must be integrated into a single database. Informational systems are essential for data warehousing.

Separate operational and business data

Data analysis in an operational system results in low performance. Here low performance means slow down in a number of parameters including processing speed. The reason is these are essential for mission critical applications. They follow a predefined sequence of operations. Moreover, operational systems require high performance and quick response time. Business analysis processes in a data warehouse are not predefined and don't have rigid response time requirements. For this reason, they need to be separated from operational data.

Data Warehouse Architecture

Data Warehouse Architecture (DWA) gives the framework for the overall structure of the data and its processing within an organisation. Two different mechanisms that are used in data warehouse architecture are:

- Physical management of flow of data, so that large amounts of information can be provided easily and quickly.
- A large archive of data is stored in an information repository. This is termed metadata. Metadata forms the basis for data flow processing which is a high-level data flow language.

A centralised database serves the purpose of these two architecture mechanisms. Here batches of data that are essential for the daily operations are stored in addition to the physical flow mechanism.

Answer: [a] Data creation.

Data warehousing helps to gather and report information that is already stored in the database. It cannot support the function of creating more data. A data warehouse performs other functions like data integration across various departments, business analysis and immediate information delivery. It also helps in reducing the cost of information search and analysis of existing data.

Module:4 Reference No:M4006

Question: ISDN's Basic Rate Interface (BRI) is also known as?

- [a] 23B+D
- [b] 23D+B
- [c] 2B+D
- [d] 2D+B

Module 4- ISDN Concept

Introduction

In the past years, the idea of integrating fax machines, telephones, video conferencing and LAN modems in a single network would have sent shudder down the spine of even the largest of corporate houses. The problem was the lack of bandwidth to support such a high rate of data transfer that would take place if the system were in place. This drove the demand for having architecture to enable multiple services to run simultaneously on a single communication medium. That is how ISDN or Integrated Services Digital Network came into existence.

Integrated Services Digital Network is a suite of standards that have been adopted internationally for digital communication over the ever-existing telephone network. While the modems receive/transfer data at a rate of 56kbps, ISDN being an all-digital network is capable of transferring data at a rate of 64kbps.

ISDN is the ideal technology for the ICE age (Information Communication and Entertainment) when not only the quality, but also the speed at which it is delivered is important. It supports all kind of data transfers including voice, text, graphics, video and the like.

How ISDN works?

To understand clearly the basic functionality of ISDN, we should familiarise ourselves with a few basic concepts

Channels

Channel is that part of the bandwidth that can be used for data transmission. There are three basic types of channels:

A bearer channel (B channel) is defined at 64Kbps. It is the basic user channel and can carry any kind of data to and from at the same time.

A data channel (D channel) can either be 16 or 64Kbps, depending on the need of the user. This carries the control signals for the B channel i.e. signals to set up or end a connection.

A hybrid channel (H channel) transfers data in the range of 384Kbps to 1920Kbps. It is used for transferring high data-rate applications like videos and the like.

Interfaces

Interfaces are the methods to access various ISDN channels and include one D channel and some number of B or H channels. There are two kinds of interfaces:

Basic Rate Interface (BRI) consists of two B channels and one 16Kbps D channel. It is also known as 2B+D interface.

Primary Rate Interface (PRI) consists of twenty-three B channels and one 64Kbps D channel in North America and is also known as 23B+D interface. In Europe, it is 30B+D.

We as a user connect to the ISDN lines using these interfaces. Once connected, large amount of data can be transferred or received within seconds.

Benefits

1. Clarity

Since ISDN is digital, there are less errors when compared to analog transmission. Also, voice and video files are transferred and received with crystal-clarity without any distortion.

2. Compatibility

ISDN is compatible with the traditional analog mode and no problems are experienced while transmitting or receiving data. ISDN service can be carried over on the existing telephone line that saves vast amount of investment towards setting up the infrastructure.

3. Higher Productivity

ISDN enables us to perform two communication tasks at a time. For example, we can simultaneously transfer a file and receive a phone call without any disruption, while both use the same communication medium.

4. Dynamic Bandwidth Allocation

The two B channels can be used for different types of data, say voice and text. If only one kind of data is to be transferred, then both the channels can be used that doubles the transmission speed.

Answer: [c] 2B+D

Module:4 **Reference No:**M4007

Question: Which of the following features is not a part of DSL but of ADSL?

- [a] Use of Plain Old Telephone Service (POTS)
- [b] Use of copper wire as transmission medium
- [c] Facilitates more downstream rather than upstream transfer
- [d] Provides more bandwidth for voice.

Module 4- Digital Subscriber Link

Technology is growing at the speed of light. And, existing infrastructure has to cater to change cost effectively. The plain old telephone network is the basic infrastructure for the telephone system. This network is widely used for LANs, WANs, Internet and the like. A connection that can use this infrastructure to provide high-speed and high bandwidth access to the Internet is DSL (Digital Subscriber Link).

What is DSL?

A technology that provides secure, high speed, reliable Internet access using existing copper telephone lines is termed as DSL. Dedicated access to the Internet is available through this technology, without disturbing normal telephone usage. POTS refers to the normal telephone connection that uses a pair of twisted copper wires as the medium of transmission. Telephone lines are primarily used for voice transmission. These lines can be used to accommodate more bandwidth than is required for voice. DSL uses this extra capacity for carrying information over telephone lines.

Working

Information transmission is in an analog mode in a telephone line and is limited to 3400 Hertz. Analog transmission uses only a small portion of the available frequency range that a copper wire line can provide. Due to this, an ordinary modem can receive only 56 Kbps (Kilo bits per second) of data. With the ISDN (Integrated Services Digital Network) it can extend up to a maximum of 128 Kbps. By removing the limitation of 3400 Hertz, DSL utilises the full potential of the copper wires, and achieves a transfer rate of millions of bits per second. Using DSL, information is transferred in digital form to and from the computer over the telephone lines. Hence, more bandwidth can be utilised for data transfer. Further, analog and digital data can be divided in equal bandwidths to simultaneously use telephone and the Internet. Connections using DSL can provide 1.544 Mbps downstream (to receive data) to 128 Kbps upstream (to send data) speed. One drawback in using DSL is the signal loss and cross talk. This increases with the increased distance. DSLs perform better at short distances from ILECs (Incumbent Local Exchange Carriers).

ADSL

Asymmetric Digital Subscriber Line (ADSL) uses more of its bandwidth for downstream rather than upstream data transfer. (i.e. the user can /receive more data than send data to another destination). A small

part of the bandwidth is allotted for upstream or user-interaction messages. Data up to 6.1 megabits per second downstream, and up to 640 Kbps upstream can be sent, using ADSL. It can cover a maximum distance of 18,000 feet. This is more appropriate for receiving video, audio, animation and the like from the Internet to computers. A small portion of the bandwidth in the downstream is utilised for voice, so that the telephone line functions normally while using the Internet.

Answer: [c] More downstream transfer than upstream.

ADSL has been devised under the assumption that more downloading rather than uploading takes place from the Internet. Bandwidth allocation for voice features is done in DSL also. Both DSL and ADSL use existing copper wires and the POTS as infrastructure.

Module:4 Reference No:M4008

Question: Which of the following is not an aspect of data mining?

- [a] Data collection
- [b] Powerful multiprocessor computers
- [c] Data mining algorithms
- [d] Decision trees

Module 4-Data Mining

Introduction

Data mining can be defined as the use of automated data analysis techniques on large data sets to establish significant facts, relationships, trends, patterns, exceptions and anomalies that might otherwise pass undetected. Data mining tools help in predicting behaviours and future trends, and therefore allow businesses to make proactive, knowledge-driven decisions. It is an automated process of identifying patterns in the database. Let us consider the example of an automobile manufacturer. By studying patterns and trends in sales, the company can predict the reaction of customers to new changes in the design; the customer segment that is most receptive to the new product; and the type of product that best suits the target group.

Working

Data Mining uses data modelling for forecasting. Data modelling creates a model from a known data source and then applies it to unknown situations. For example, an airline may seek to focus its marketing strategy on customers who travel long distances. The airline may have a lot of information about its customers, but may find it difficult to determine common characteristics, since there are many variables that have to be considered. It can use data mining tools, such as neural networks on its existing customer database, which contains information such as age, sex, credit history, income, zip code, occupation, and the like, to identify characteristics of customers who travel long distances. For instance, it might find that an extra income of Rs5,00,000/- comes from frequent travellers ,who are bachelors between 34 -40.This would therefore be its model high value customers, and the airline can target its marketing efforts accordingly.

The most **commonly used techniques** in data mining are:

Artificial neural networks: These are non-linear predictive models that resemble biological neural networks in structure.

Decision trees: These are tree-shaped structures representing sets of decisions, which generate rules for classification of a dataset. Specific decision tree methods include Classification And Regression Trees (CART) and Chi Square Automatic Interaction Detection (CHAID).

Genetic algorithms: These are optimisation techniques that use processes such as genetic combination, mutation and natural selection in a design, based on the concepts of evolution.

Data mining is **popularly used** in:

- Trend analysis: Often analysis is used to determine the product that is likely to be in demand.
- Establishing customer loyalty: Sometimes a study can be conducted to assess whether the customer is likely to switch loyalty to the competitor's product.
- Market-basket analysis: Such an analysis determines items that are likely to be purchased.
- Segmentation: It includes activities that seek to identify groups with common characteristics.
- Estimation and prediction. Estimation helps in guessing an unknown value such as income, when other aspects, such as job profile and the like are known. Prediction seeks to establish an approximate value, such as the probability of buying a car.
- Decision Tree: It is a flow chart of questions or data points that prompts a decision to be made. For example, a motorcycle-buying decision tree would begin by asking the model of the bike that you favour, then find out whether you want power or economy, and so on, until it determines what would be the best bike for you.
- Rule induction: If the database contains data of statistical significance, then "if-then" rule could be applied.

The business community is already supported by extensive technologies in data collection, and data mining algorithms. Hence data mining techniques could be implemented in existing hardware/software, as well as, integrated with new products. When combined with high-speed client/server or parallel process environment, these techniques help to analyse large chunks of data within a short span of time.

Answer: [a] Data collection.

Data collection is done by database software.

Module:4 Reference No:M4009

Question: Which is the component not found in a data dictionary?

- [a] Table definition
- [b] ER model of data
- [c] Actual data
- [d] Data element definition.

Module 4- Data dictionary Concept

Data as such is not of much use unless defined and structured properly. In a database language, an object is an abstract entity with certain characteristics. End users interact with these objects. Objects and their relationships have characteristics or attributes (such as name, date, salary, etc.) that define specific dimensions of "colour" or "character". This distinguishes their current state or status from that of other objects or relationships. During, interaction it is necessary to know the nature of objects and their relationship with other objects. A process called data modelling does this. Documented details of this process are stored in a reference book termed data dictionary.

It consists of a group of data element definitions. These definitions include the nature and kind of relationships between objects, specific name, data type, and the list of allowed values. The primary purpose of a data dictionary is to make users understand the structure of the data, and to assess its suitability for a particular application.

Data dictionary contains information about structures and objects of the database such as tables, columns, users, and data files.

The different components of a data dictionary are:

- Data element definitions
- Table definitions
- Database schema
- Entity-relationship model of data
- Database security model.

Data element definitions contain data element number, data element name, field names, default value, database table references, source of data in the element, history references, date of the data element document, quality control references and data elements notes.

Table definitions are done through SQL (Structured Query Language) commands. They include naming the table and security classification of the table.

The graphical view of the database is known as database schema. Schema enables the joining of data elements from different tables.

The analysis and design of the database is accomplished with the ER (Entity -relationship) model. This model represents entities, attributes and their relationships.

- Database access rights are assigned through this model.

Data dictionary consists of two levels:

1. Internal level
2. External level

The internal level contains all the base tables of the DBMS software components to which users are not granted access.

The external level consists of several dimensional features of the base tables. This gives information about objects and their structure at different levels in detail.

Answer: [c] Actual Data.

Data dictionaries do not contain any actual data from the database, except for bookkeeping information. But, a database management system cannot access data from the database without the data dictionary.

Module:4 Reference No:M4010

Question: Which one of the following databases supports programming languages?

- [a] Hierarchical model
- [b] Network model
- [c] Relational model
- [d] Object-oriented models

Module 4-Database Models

A database model depicts a container of data and a methodology for storing and retrieving data from that container. Such models are just mathematical algorithms and concepts, and cannot be felt or touched. Various forms of database models are:

- Hierarchical Model
- Network Model
- Relational Model
- Object-oriented models
- Object/Relational Model

Hierarchical Model

The hierarchical database model arranges data in a hierarchical manner that seems like an upside down tree. Relationships in this model are like that between a parent and child. They are represented as links physically in the file system and termed as "pointers". Every parent has a list of pointers to the children. This assures systematic accessibility of data. It collects all instances of a specific record together as a record type. In a relational model, this is treated as a table and the individual record type as a row. In a hierarchical database, the parent-child relationship is one to many. The user should be aware of the whole tree structure to go to any point in the table. A major drawback with this model is that a new record cannot be added to the child's table, if it has not been included in the parent table. Another drawback is redundancy, since it cannot handle many to many relationships.

Network Model

The network model considers data as sets. A set consists of an owner/parent record type, a set name and a member/child record type. It is similar to the hierarchical model except that children are allowed to have more than one parent to support many to many relationships. This model is difficult to implement and maintain, and was used mostly by computer programmers.

Relational Model

E.F Codd developed the relational database model. This database uses tables to organise data, and establishes relationships between them. It is widely known as the Relational Database Model (RDBMS). It allows the definition of data structures, storage and retrieval operations, and integrity constraints. It designates certain fields as keys to facilitate easy search for any value in that field. More than one table can be combined for operations using select key fields.

Object-Oriented Model

The main purpose of the Object Oriented Model is to provide database support to object oriented programming languages such as C++, Smalltalk and Java. This model effectively uses both persistent data as in databases, and transient data as in executing programs. The main advantage of using this model is its excellent ability to manage objects complex interrelationships between them.

Object/Relational Model

This new model provides better object storage capabilities to relational systems. It integrates the management of traditionally fielded data, with complex objects such as time-series and geospatial data and diverse binary media such as audio, video, images, and applets. Using encapsulating methods, an ORDBMS server can execute complex analytical and data manipulation operations.

Answer: [d] Object-oriented models

The hierarchical database model arranges data in an upside down tree form. The network model deals with data as sets; while the relational model uses tables to organise the data and relationships between them.

Question: Which of these options is not a feature of VPN?

- [a] Uses Internet
- [b] Uses intranet
- [c] Uses extranet
- [d] Uses common standards.

Module 4- Virtual Private Networks Link Concept

Introduction

The focus of today's business enterprises is on increasing the scope of communications with reduced cost of infrastructure. WAN (Wide Area Network) is based on connectivity between the head office of an enterprise and different regional offices within a large geographical area (more than a LAN-Local Area Network). Thus, the need arises for a corporate network that can be accessed through intranets and extranets.

What is a Virtual Private Network (VPN)?

A private connection between two machines or networks at different locations covering a long distance, using the infrastructure of an existing public or shared network like the Internet is a VPN. It is similar to a WAN as it covers a long physical distance. However, it differs from other computer networks because it makes use of public networks like the Internet instead of leased private lines. Hence, restricted-access networks with good security features should be developed.

VPN Vis a Vis other networks

VPN differs from other corporate networks in three ways:

1. Remote users can access the corporate network using the same network scheme and addressing methods as regular users of the central network.
2. The central network of the corporate can validate its own users though it uses a public network.
3. A unique dial-up tone can be provided by the ISP (Internet Solution Provider) to differentiate corporate users from the public network users. However, this has to be synchronised with the software of the remote user.

Implementation

It can be implemented through:

1. Remote access VPNs
2. Intranet VPN
3. Extranet VPN

Remote access VPNs provide remote users and mobile commuters access to the corporate network through the Internet or any shared network. Two ways of realising remote access VPNs are:

1. Client side tunnelling (where a software installed at the client end ensures encryption of information and establishes a tunnel)
2. Service provider tunnelling (Here the security and communication infrastructure is outsourced to a service provider.)

Intranet VPNs use dedicated connections besides the Internet to connect corporate headquarters, regional offices and home offices.

Access restrictions incorporated into the VPN in the case of Remote access and Intranets pave the way for the construction of Extranet VPNs, which establishes connection with other stakeholders like suppliers, customers, partners and the like.

How does it work?

A user in a remote location should first log on to the ISP network. He can then send a 'tunnel' request for a connection to the corporate network. After the request is sent, the corporate security server authenticates the user. The user can then send the message to the corporate security server, which will be encrypted by the VPN software. Similarly, the message sent by the corporate server will reach the remote user in encrypted form.

Advantages

1. Branch offices and telecommuters are networked in a corporate network through the Internet, eliminating long distance charges.
2. Scalability is an important advantage of VPNs. As the number of networks to be interconnected increases, the communication infrastructure also increases. VPNs resolve the issue by using public shared networks.
3. Since the ISP does the maintenance of dialup services, such costs are lesser.

Disadvantages

1. There is no common standard for VPN technologies. Different vendors provide their own technology, which are not compatible with each other.
2. An in-depth understanding of public network security issues and proper deployment of precautions is essential.
3. VPNs have to cater to several protocols other than IP and the existing internal network technology.
4. In case of ISP tunnelling, the encryption takes place after the message reaches the ISP. Hence, these messages are vulnerable to attacks from the time it leaves the corporate network till it reaches the ISP.

Answer: [d] Uses common standards.

There is no standard for VPN solutions as vendors use different technologies.

Question: Circuit switching technology is used for:

- [a] Sending data in small packets as in emails.
- [b] Sending data continuously in an order as in voice or video messages.
- [c] Switching on and off circuits in the telecommunications network.
- [d] Storing messages and then transmitting them to the next node depending on the address.

Module 4-Switching Technologies

Packet switching

This protocol divides the message to be transmitted into small units of data called packets. Based on the destination address, these packets are routed through a network. Packets, which may be of variable length, can go either in the same route or different routes to its destination address. The network establishes the maximum length of the packet. Each packet has a header with control information (such as priority codes and source and destination address). The packet is stored briefly at each node, and then routed over the network according to the information in its header. On reaching the destination address, packets are recompiled into the original message. Since the data is broken down into packets, different users in the network can use the same path. This is very useful for transmission of data, which can withstand some delays in transmission, like emails, web pages and the like. A network using this type of communication is termed as a connectionless network. Two technologies used in packet switching are:

Datagram packet switching: Each packet in this technology is treated independent of others in spite of being a part of multipacket transmission. Packets in this technology are referred to as datagrams. The header of each datagram has information about the destination. Intermediate nodes examine the header and decide which node to send the datagram has to be sent to, so that it will reach its destination.

Virtual Circuit packet switching: Before transmitting all packets related to a single message or data, a route is determined for the session. Packets are then sent one by one on the route.

Circuit switching

This uses a dedicated channel/circuit for transmission of data. When data is being transmitted, resources on the network are not available to other users, for the duration. Circuit switching has been designed for voice communication. It creates a temporary (dialled) or permanent (leased) dedicated links. Circuit switching systems are generally used when data is to be transmitted quickly and must arrive in the same order. Real Time data transmission, (audio and video) makes use of this technology. In circuit switching, the number of inputs need not match the number of outputs. Two commonly used technologies are:

Space division switches: Originally designed for analog networks, paths in this circuit are separated from each other spatially.

Time division switches: This involves partitioning of a lower speed bit stream into pieces that share a higher speed stream with others. It primarily depends on two points. One is time sharing of transmission medium (also known as multiplexing), and the other is time switching, which means multiplexed information carried on the transmission medium must be transferred from input points to the desired output points.

Message switching

This is a protocol where messages are handled through a switching centre, which could be either from local users or from other switching centres, whereby the message traffic is stored and forwarded through the system. The message is stored in a secondary device like a disk and forwarded.

Answer: [b] Sending data continuously in an order as in voice or video messages.

In packet switching, the data is transmitted in small packets. Message storing and transmission is done in message switching. Circuit switching is therefore used for continuously sending real time data (video and audio).

Module:4 Reference No:M4013

Question: Which of the following technique/feature does ATM not integrate?

- [a] Multiplexing
- [b] Switching
- [c] Data/voice/video transmission
- [d] Encryption.

Module 4- Asynchronous Transfer Mode Concept

Evolution

The path breaking convergence of computers and telecommunications requires an efficient technology to transfer voice and video over networks, in addition to data. Fibre optic cables have the potential for higher bandwidths but are very costly and do not transmit voice. This led to the usage of high-speed voice optimised WANs but soon the problem of efficiency cropped up. ISDN (Integrated Services Digital Network) evolved a broadband solution to transmit information in synchronous and asynchronous modes. This allows the utilisation of bandwidth for a particular application in an efficient manner. The allocation of bandwidth for specific requirements on demand led to the evolution of a new standard called Asynchronous Transfer Mode.

What is ATM?

Asynchronous Transfer Mode (ATM) is a mode of transferring data where information is organised into cells in an asynchronous format. The recurrence of cells containing information from an individual user is not necessarily periodic. ATM is a high speed, low delay (the time taken by the system to process a request for data transfer), multiplexing (the concept of sending multiple information packets through a single channel) switching technology. Information in many forms like voice, data, and video applications are transmitted through ATMs. They are suitable for bursty (where processes of different speeds are transmitted over the networks resulting in frequent mismatch between the sender and the receiver) traffic.

ATM technology

Information is broken into data units called data cells/bytes, 53 being the fixed number. Of these, 5 cells are reserved for storing header information. The fixed size of these 48 cells ensures that critical elements like voice and video are transmitted without interference by other long packets of data. The transmission medium is fibre optic cables that support high speeds. Information is moved into standard-sized cells. As data/voice/video are organised in small fixed length cells, it is easy to implement a switching mechanism in hardware. It is also easy to allocate resources in the network suitable for each cell. This enables switching in the hardware of these networks at a fast pace when compared with software switching. ATM is connection oriented. The organisation of different streams of data in separate cells allows the user to specify resources required and allows the network to allocate resources accordingly.

Before data is transmitted, a logical connection is established with the destination. These connections are known as virtual paths or virtual channels. Depending on the requirements of the user these connections can be made and released dynamically.

ATM applications

They find wide spread applications in the following areas:

- **ATM work group** (a group of individuals working towards a common goal) and **campus networks**: Dedicated campus networks can be built with the help of ATMs that provide enormous speed and enhanced desktop computing features. This can be done with the help of ATM emulation standards.
- **Multimedia virtual private networks**: Applications that require high bandwidth for voice and high resolution including integrated multimedia features are built with the help of ATM networks. This is useful for building VPNs (Virtual Private Networks).
- **Internet backbones**: Virtual private intranet facilities use the high-speed capabilities of ATMs, since this infrastructure can be effectively used for the supporting the internet.
- **Carrier infrastructure for telephones**: Using the existing fibre infrastructure/ cables, ATM networks are deployed as telephone carriers to increase speed and scalability.
- **ATM WANs and MANs**: Wide area networks and Metropolitan area networks can be implemented with ATM technology to give higher performance and speed.

Answer: [d] Encryption.

ATMs can support any type of data traffic including voice, text, images and video. It is a broadband multiplexing switching technology. Hence, it has found wide applications in Multimedia, Videoconferencing and Video on demand. There is no encryption involved in the adoption of ATMs

Module:4 Reference No:M4014

Question: Which of the following is used to append a digital signature?

- [a] Public Key
- [b] Private key
- [c] Trusted Key or Third party key
- [d] Any digital Key

Module 4- Digital Signature

The Digital Signature can be defined as the electronic code embedded to a document, a message or a file that gives it a unique identity. The digital signature is a way to authenticate that the document originated from the sender. Authentic means that user knows who created the document and that it has not been altered in any way since the sender created it.

Digital signatures rely on encryption to ensure authentication. Authentication is the process of verifying that information is coming from a trusted source. These two processes work hand in hand for digital signatures. The digital signature requires a pair of keys. One public key to be kept in the public key server and the other private key to be kept with the user. The private key is used to sign the document, which is then sent to the recipient. And the public key is used to verify the signature.

To start with, a message digest of the documented is first created. This is concatenated with information about the sender, a date stamp, timestamp etc. The resulting code value is then encrypted using the private key of the sender using a suitable algorithm. The resulting encrypted block of bits is the signature.

Suppose Kiran wants to send Kumar a document electronically, and Kumar needs an electronic signature to verify authenticity, Kiran first computes a message digest of the document. He adds his personal information to it. The resulting string is then encrypted with his private key, using a complex mathematical algorithm. He then sends the encrypted value to Kumar. This is Kiran's digital signature. Kumar decrypts the code value he received from Kiran using Kiran's public key. If the two values match, then Kumar not only knows that he received an authentic document, but he also knows that Kiran's signature is real. Conducting transactions in this manner is more secure than signatures in ink, since they can be forged.

The digital signatures can be used to Certify that a public key belongs to a certain individual. A trusted key (third party) signs the documents, thus authenticating the digital signature.

Requirements of digital signatures:

- Both the sender and the recipient must be able to activate the keys, sign the documents properly, and verify the documents received in very less time and at a nominal cost.
- The digital signature should be secure.
- The digital signature mechanism should be well defined. Which means a document created by user after verifying transformation, should accept that the signed message is genuine.

Spam mails: Unsolicited mails

Answer: [b] Private Key

Module:4Reference No:M4015

Question: _____ ensures an undisturbed connection between two nodes during data exchange:

- [a] Application layer
- [b] Data link layer
- [c] Session layer
- [d] Presentation layer

Module 4- Network Standards

The International Standards Organisation designed a networking frame known as the Open System Interconnection Reference Model, which explains the transfer of control from one layer to another, as if in stack. Each layer has its own functionality and interacts only with the layer immediately beneath it. The main advantage of the OSI reference model is that it solves the problem of interconnecting two systems by dividing the networking system into layers. This means that a product from a vendor who implements layer 2 can easily operate on another vendor's product, which operates on layer 3, if both follow the same model. Another advantage is new protocols and network services can be easily added to a layered structure rather than a monolithic model. The application, presentation, and session layers are referred to as "upper layers". They deal with data formatting, encryption, and connection management. Transport, Network, Data link, Physical layers are known as "lower layers" and deal with more primitive network-specific functions like routing, addressing and flow control.

1.Physical Layer: The role of the physical layer is to transmit raw bits over a communication channel. The design should make sure that when one side sends a 0 bit, the other side receives it as a 0 bit and not as a 1 bit. Specifications of this layer include signal voltages, bit duration and channel definition. It primarily deals with mechanical and electrical characteristics to activate, maintain and de-activate the physical connection. Example: Ethernet cable

2.Data link Layer: It transforms the raw bit stream supplied by layer1 into data. This is done by breaking input into frames, transmitting the frames sequentially, and then processing the acknowledgement frames

sent back by the receiver. This ensures an error free transmission of data. In this process, a frame could be duplicated or lost and layer2 wouldn't be aware of it.

3. Network Layer :It deals with routing decisions taken in the network, which has a large number of nodes and routes. It has specifications for the transmission and switching technologies required to build circuits through a network of nodes. For example, it sets up the circuit for the transmission of each packet of data and then de-allocates and re-allocates the nodes to other services.

4. Transport Layer :It ensures data reliability and integrity. If a packet fails to arrive, in this layer, it is retransmitted by the sending system when it does not receive an acknowledgement from the device with which it is communicating.

5. Session Layer :It establishes a connection between two nodes, and allows data exchange between them. But releases the contact in an order when not required.

6. Presentation Layer: It provides data to the application layer in a standardised format. Some of the services provided are protocol conversions, encryption and decryption, text reformatting, compression and decompression and the like.

7. Application Layer: This is the layer where the user actually works. Applications such as FTP, TELNET, Electronic Mail and the like are done here.

Answer: [c] Session Layer

The application layer is concerned with user related applications such as email, FTP. The data link layer deals with transforming raw bit streams into data; the presentation layer deals with presenting data to the application layer in a standard format; and the session layer oversees the connection between two nodes to ensure uninterrupted data exchange

Module:4

Reference No:M4016

Question: Which of the following is considered the greatest threat to the corporate network, as far as cyber theft is concerned -

- [a] Business partners who have authorized access to the network
- [b] External parties not having authorized access to the network
- [c] Suppliers and customers who have authorized access to the network
- [d] Employees who are connected to the corporate network

Module 4-Building Secure LAN

Building a Secure LAN

One of the priorities of every business is to "get connected". In this process, they risk their most important asset - "Information". Companies that have enabled online transactions with employees, customers and business partners are allowing a lot of sensitive information to be accessible through intranets, extranets and even through the Internet. With an increase in e-business activities, intellectual capital is gaining importance, and safeguards are required against the "cyber thief".

Today, the LAN is no longer restricted to a single site, isolated and protected from the outside world. **Virtual LANs (VLANs)**, which connect different workgroups across distributed geographical locations in a network are emerging. This kind of network extends beyond the corporate premises and provides access to workers in remote locations. Even business partners, customers and suppliers can be connected to the existing VLAN through an extranet. Though the intranet and extranet offers increased productivity and efficiency, it also increases the risks. Today corporate networks are exposed to the following types of risks-

- When business partners jointly create a network where they exchange information or share their knowledge. Now this information can be accessed by anyone on the LAN and information that is meant to be confidential becomes public.
- In case of extranets, customers and suppliers are connected to back-office servers and databases through authorised access. This is achieved by, "**punching a hole**" through the corporate firewall and other perimeter defences. But such access also creates an opportunity for cyber thieves to enter through the back door.
- Even in cases where a corporate network does not permit public access, it is vulnerable to cyber theft. Employees (permanent or temporary) have access to private LAN. Thus network administration should take care to prevent access of employees to private information. Employees who often leave companies walk away with privileged information such as login IDs, passwords, customer list and other relevant information. Thus a special security measure should be employed as insider theft is very difficult to detect and can take place easily.

Steps to secure the corporate network

Companies should follow two basic rules -

- Protect data at the source
- No shared links should be considered secure

LAN and VLAN should not be considered trustworthy though they are secured by traditional measures. Enterprises usually adopt following security measures -

- Physical security - Restrict access to servers and systems by use of locked doors, keypads and access codes. This prevents physical theft and damage of computer assets.
- Network security - Physical security does not mean that systems are safe from network threats. Traditional firewalls act as a perimeter defence that blocks access from outside to internal resources. Firewalls enable packet inspection, filtering and proxy services to provide access only to authorised users, hosts and networks. Any other traffic outside the firewall is prevented access to internal servers and desktops.

In some cases, companies are using the public Internet to establish connectivity to remote sites. Emerging Virtual Private Networks (VPNs) protect packets of information that leaves the LAN.

Though these measures are essential, it still ignores the most essential part of the network - private LAN. A large part of the communication takes place between servers and desktops or among servers that are connected with LAN based workgroups. As stated above "insider theft" is the greatest threat to networks. IPSec (Internet Protocol Security) provides some flexible options that help in securing networks and in meeting performance expectations.

A 1999 FBI/CSI study on computer crime found that most security breaches occurred due to unauthorised access by employees.

Answer: [d] Employees who are connected to the corporate network

Question: _____ are self replicating malicious code that bring down the speed of the processor on entering a network, and are not dependent on the action of the user

- [a] Viruses
- [b] Worms
- [c] Trojan Horse
- [d] Spoofing

Module 4- LAN Malicious Code

LAN - Threats from malicious codes

One of the threats that LAN faces is the exposure to different types of malicious code that may affect the network. Hence it is important to have an understanding of different types of malicious codes and how they affect the network -

- **Viruses** - They are a series of commands that start self-replicating, as soon as the file to which they are attached is opened. They are not always destructive. But sometimes they may cause serious damages to data files resulting in possible data loss and disrupting operations. There is also a threat of the virus spreading to other users through the network. Viruses usually enter the network through two modes -
 - a. By email attachments
 - b. By use of virus infected floppies and other storage devices

Good anti-virus software protects the network from virus attacks. . All incoming e-mail attachments, floppies and other storage devices should be scanned before opening.

- **Worms** - They are very often confused with viruses because of their self-replicating characteristic. The only difference between the two is that worms do not require any kind of action from the user, all they need is an insecure connection to the Internet. They do not affect the network by deleting or damaging files; instead they use the processor to install, replicate and transfer themselves to other computers in the network. They bring down the processor's speed dramatically. Use an anti-virus (which should be updated periodically say monthly) to protect against worms. In addition it is important to have stringent access controls.
- **Trojan Horses** -It is a program that appears to do a useful job, but is actually destructive. Through an insecure network it somehow gets downloaded to install itself on computers that are connected to the network. These programs enter the network through e-mail attachments; therefore infected file attachments should not be opened.
- **Spoofing** - It generally works like this -
 - a. An unauthorized person misleads an authorized user to perform a particular function or activity.
 - b. The authorized user performs the function and in the process discloses some valuable information
 - c. Later on, the unauthorized person misuses the information that the authorized person provides

For instance, an unauthorized person may write a program to resemble the login screen. When the authorized user enters the login ID and password, a message "system is temporary out of service" appears. The

unauthorized person may then misuse this information. Now-a-days it is a very common, and most scams and misdeeds online are because of spoofing.

Answer: [b] Worms

Module:4 Reference No:M4018

Question: Security problem(s) that a PC can create in a Local Area Network are:

- [a] Multiplication Factor
- [b] Channel Factor
- [c] Both (a) and (b)
- [d] Division Factor

Module 4- LAN Security Issues

Local Area Networks (LANs) are groups of PCs that are connected together so that data and devices can be shared. Personal computers as stand alone machines are exposed to many security threats. When they are connected in a network security concerns increase. This is referred to as the 'multiplication factor'.

Reduce the multiplication factor

Ensure that individual systems are secure before they are connected in a network. Unauthorised access to a terminal provides access to the entire network. To tackle individual terminal security issues local storage and processing devices could be removed, but then the PC would be a dumb terminal. Many operating systems provide stringent security measures to the network but these do not work when individual terminals are not secure.

Multiplication factor can be kept under control by -

- Securing each computer in a network with the help of a site system and file access control
- Taking care of suitable power and data back up facilities
- Having the operator/administrator constantly monitor the network

Channel Factor

When two or more computers communicate with each other through a port in a network, a new security issue emerges, which is referred to as the "Channel Factor". It creates a possibility for the attacker to steal, delete and corrupt the information by exploiting these channels. Thus it becomes important to protect the channel, which can be done in three steps - channel control, channel verification and channel support.

Channel Control refers to limiting access to channels by keeping a check on individuals, who can open, use and close a channel.

Channel Verification involves checking the identity of users, identity of data and the integrity of the channel. On LAN, the identity of a user can be verified by giving every user a unique ID number (name) and password to log in. This makes it easy for the administrator to identify the user.

Channel Support involves co-ordination of communication hardware and software. Another security issue in a LAN is the authenticity of data.

Thus LAN security should also ensure -

- Confidentiality of stored, processed and transmitted data in the network

- Integrity of stored, processed and transmitted data in the network
- Availability of stored data
- Identity of the sender and receiver of information

Answer: [c] Both (a) and (b)

Module:4Reference No:M4019

Question: Which of the following is not a characteristic of a modem?

- [a] Transmission Speed
- [b] Data Accuracy
- [c] Error Detection and Correction
- [d] Data Compression

Module 4- Modems Concept

What is a modem?

Transfer of data between two networks takes place through physical communication channels like coaxial cables or twisted pair wires. These media are capable of sending only analog signals whereas the information flow within a computer system takes place in the form of digital signals i.e. zeros and ones. A modem is a device that converts the outgoing digital signals from a computer into "medium-compatible" analog signals, which are then transferred through the physical media to the required destination. At the other end, they are received and reconverted to the digital format, which is understood by the computer. So, a modem is a device that *modulates* digital signals into analog signals and then *demodulates* them back into digital signals.

Types of Modems

Internal Modem

As the name suggests, an internal modem is placed inside the computer and is connected directly to the I/O BUS. Internal modems are electronic cards which neither requires a separate power connection nor a separate serial port. These cards are a bit difficult to install and have to be mounted on existing ISA slots, present on the motherboard. But, they are relatively cheaper than external modems

External Modem

An external modem is a fully functional external hardware device that is placed outside the computer and is connected to the serial port through connecting cables. Such modems require a separate power connection to function so that they can be reset without affecting the system. Moreover, they can be moved between computers and any problem that occurs can be diagnosed with the help of the lights on the modem.

Characteristics of Modem

Transmission Speed

The transmission speed for a modem is measured in **BPS** (Bits per second) or **Baud rate**. While baud is a measure of how frequently sound changes on the phone line, the BPS indicates the number of bits transferred in a second. Standard transmission speeds are 9,600 baud, 14,400baud, 24,400 baud, 33,600 baud, and 56,800 baud

Error Detection and Correction

Over the phone, there are chances that communication may be incomplete or inaccurate. As data transmission takes place, there are chances that communicating modems may miss a beep or two and hence compromise on the integrity of the data. To overcome this problem, parity checks are added to the outgoing data. The

communicating parties decide on whether they want to have an even or odd communication and accordingly a parity bit (1 or 0) is added to maintain the standard established earlier. Let us consider an example. Two parties agree on an even communication i.e. sum of all the bits should be even. Now if the data being sent is 111111, adding up to an odd figure, a parity bit of 1 is added at the end to make it even. Similarly, if the data being sent is already an even figure, say 111111, a parity bit of 0 is added.

Even after taking such precautions, there may still be instances of error occurring. Protocols are designed to overcome such problems. A modem, while sending data will calculate a checksum (a mathematical algorithm) on a block of data. The checksum is again calculated during the flow of data and also when it reaches its destination. The results are then compared and in case of a mismatch, a request is made to re-send the data. This may take time but guarantees authenticity of the data being sent.

Data Compression

Since the transmission speed achieved by modems was relatively low, a need was felt to compress data so that communication could be faster. Various protocols were used to compress the data that increased its throughput by a remarkable 50%. These protocols perform the dual job of error correction as well as data compression. Data, compressed at one end, is sent over the line to be received and decompressed at the other end, before being fed into the computer.

Data Accuracy

One of the drawbacks with the modem is that it does not ensure accuracy of data that is being transmitted. If a message has to be transferred informing the schedule of a meeting on Tuesday, March 20, 2002, a modem has no feature in place to check whether the March 20 is a Tuesday or not. It works on the concept of GIGO (Garbage-In-Garbage-Out) i.e. what is provided at one end is delivered as it is, without checking for its correctness.

[b] Data Accuracy.

Module:4 Reference No:M4020

Question: When three or more nodes are linked together through a single communication medium it is termed as,

- [a] Ring Logical Topology
- [b] Point-to-Point Topology
- [c] Multipoint Topology
- [d] Bus Logical Topology

Module 4- Network Topology- Arrangement

Network topologies are broadly categorised into four main types i.e. bus, ring, star and mesh. But they can also be defined based on physical topology and logical topology. The way a topology functions can be entirely different from the way it is set up. The cabling might suggest one thing, but the actual flow of electrical pulses may indicate otherwise.

Physical Topology

The physical topology of a network refers to the configuration of cables, computers and other peripherals. It is the layout of the cabling scheme for the network. This can be further sub-divided into two types.

Point-to-Point Topology

As the name suggests, in a point-to-point topology two nodes are connected directly to each other. In a point-to-point connection, the two communicating links monopolise the medium they are communicating on and hence

the medium is not shared. We can have three different types of point-to-point links i.e. simplex, half-duplex and full-duplex.

In simplex communication, only one of the two communicating parties is allowed to send data. This means that the information can flow in one direction only e.g. telex, faxes and the like.

In half-duplex, both communicating parties are allowed to send data but not at the same time e.g. wireless communication

Full-duplex communication means that data can be transferred on a single carrier in both directions at the same time e.g. telephonic conversations

Multipoint Topology

In multipoint topology, we can have three or more nodes linked together through a single communication medium. This suggests that all devices that are connected share the medium, and hence there has to be a mechanism for addressing the specific node to which the data has to be sent. Four main types of multipoint topologies are bus, ring, star and mesh.

Logical Topology

Physical topology highlights the network that is visible; and, logical topology deals with the network vis-à-vis the data that travels on the network. So, even if computers in a LAN are arranged in the form of a circle, the topology employed might not necessarily be ring. Logical topology describes the way information is passed between computers based on a set of rules that govern the way computers communicate in a network. These rules are also known as Network Protocols. There are two types of logical topologies that share their name with physical topologies but are entirely different in function.

Ring Logical Topology

This type of topology functions by transmitting data from one node to another i.e. the data passes to each node. In this kind of topology, each node has different receive and transmit circuits. The receive circuits take the information irrespective of whether it is meant for them or not. If it is meant for that particular node, the node accepts it, otherwise it is loaded back on the communicating medium with the help of the transmit circuits.

Bus Logical Topology

In bus topology, data transmitted on the network passes by each node connected to that network. All data transmitted is broadcast to the entire span of the network, and the nodes use an addressing mechanism to identify whether the data is meant for them or not. The nodes on such networks have the same circuits to transmit and receive because they do not accept data unless it is meant for them, and carries the address of that node.

Answer: [c] Multipoint Topology

Module:4 Reference No:M4021

Question: _____ are Wireless LAN devices that act like the "hubs" in traditional LANs and provide connectivity to the user irrespective of his location.

- [a] Data carriers
- [b] Access Points
- [c] Receivers
- [d] Transmitters

Module 4- Wireless LAN

Wireless Local Area Network (WLAN)

A WLAN is a communication system that is developed as an effective extension and attractive alternative to the traditional LANs. WLANs counter the drawbacks of LAN like cabling, accessibility and the like because they transmit and receive data through electromagnetic waves. It provides the user mobility as well as data connectivity. The basic idea is to take the network to the user rather than bring the user to the network. This has made WLANs quite popular within a short time span, with increasing number of industries taking to this technology. Wireless LANs confirms to the IEEE 802.11 standards.

Functioning

WLANs use the concept of electromagnetic waves to transfer data. These electromagnetic waves could be infrared, radio or microwaves depending on the distance the data has to travel. Hence, they are known as data carriers. The data that has to be transmitted is "superimposed" on the carriers and is transmitted to the receiver with the help of the transmitter. This is called as modulation of the data. To receive the data at the other end, the receiver has to be tuned to the frequency of the wave on which the data is mounted. The receiver then performs the task of extracting the data from the carrier waves. This is referred to as demodulation of data. Typically, WLANs have a combination of the transmitters/receivers (transceiver) that are called access points. These access points act like hubs in traditional wired LANs that perform the job of connecting a LAN to the outside network. These access points are mounted at some height for clarity of reception and are connected to the network through a cable

Benefits

Mobility

WLANs provide their users the privilege of accessing data in real-time i.e. as and when required. The network is no longer confined to a single geographical location like a building, but can be accessed even from far-flung areas. This not only provides ad hoc networking but also increases the productivity of the user and the business on the whole.

Simplicity in Installation

Setting up a wireless LAN is far easier when compared to implementing a wired LAN. WLANs eliminate the need to have cables around the network and hence speed up the task of setting up a network. Besides, the wireless technology can take the network to every nook-and-corner of the building it is set up in.

Low Cost

Although the initial cost of setting up a WLAN is more than a LAN, the overall cost of installation and maintenance is significantly lower. The effect of increased cost is also alleviated by the increase in the efficiency and the effectiveness of the end-user.

Scalability

WLANs can be configured according to different topologies to cater to the needs of different users and applications. These configurations can be easily changed with the changing requirements of the business. WLANs can support a point-to-point network for a small organisation, as well as, a state-of-the-art set up that caters to the requirements of a large corporate house.

Answer: [b] Access Points

Module:4 Reference No:M4022

Question: Which of the following feature is attributed to UDP?

- [a] Data reliability
- [b] Stable connection
- [c] Maximum protocol mechanisms
- [d] Use of checksum to check whether the data transferred has reached destination without being corrupted.

Module 4-User Datagram Protocol

The User Datagram Protocol (UDP) is used in applications, which need to transport data between computers. Built over Network Layer and using Internet Protocol as its underlying protocol, the UDP provides a datagram mode of packet-switched connection for data transmission between computers in a network. The UDP is transaction oriented and provides procedure for application programs to send data to other programs with minimum protocol mechanism. The data transfer in this protocol is not reliable, as delivery and duplicate protection are not guaranteed.

UDP Structure:

Source Port	Destination Port
Length	Checksum
Data ...	

The data to be transferred by the application program occupies the data field of the UDP datagram. The source port indicates the port of the sending application, which is zero by default.

The **destination port** indicates the port to which the data is to be sent. The **Length** is the length of the user datagram including its header and the data. The **Checksum** is the encoded datagram data that is calculated by the sender and then by the receiver. If the datagram gets tampered or corrupted during transmission, the checksum value of the sender and the receiver will not match and the UDP protocol detects this error.

Working:

When the application program chooses UDP over TCP, then the application is connected directly to the IP. The UDP attaches source and destination port numbers to the data for multiplexing/demultiplexing transmission service. It then adds the Length and checksum value and passes the resulting segment to the network layer. The network layer then sends it to the receiving host, which checks whether it is corrupted, or not with the help of checksum. Since there is no real time connection between the sender and receiver, the UDP is also called as connectionless.

Reasons for using UDP:

1. **Connectionless Data Transfer:** Unlike TCP the UDP doesn't establish any connection between two computers and is therefore very quick in data transfer.
2. **Connectionless state:** The UDP neither maintains connection state nor keeps track of its parameters such as receive and send buffers, congestion control parameters, sequence and acknowledgement number parameters which is generally done by the TCP. Due to this reason a server devoted to a particular application can support more applications when run over UDP than TCP.
3. **Smaller Segment head:** The UDP has only 8 bytes of header as against 20 in TCP.
4. **Unregulated Send Rate:** The UDP sends the data depending on the data generated by the application program and the access to bandwidth of the internet. So it is possible that data transmitted is lost due

to router buffer overflow. Thus, the data transmitted could not be guaranteed to the receiver even though the data sent is not constrained.

UDP is generally used for multi-media applications, like video conferencing, streaming of audio and video, Internet phone, since data reliability is not very important in such applications.

However, the main problem with UDP is that it does not have a congestion control, which means that if all the users were to send large bit-rate videos, the huge traffic would overflow the router resulting in very poor delivery of the videos or some times nothing at all.

Answer: [d] Use of checksum to check whether the data transferred has reached destination without being corrupted.

Module:4 Reference No: M4023

Question: Which of the following is true with regard to fibre optics?

- [a] It consists of outer cladding and an inner core.
- [b] It consists of an inner core and outer cladding.
- [c] Even though thinner and lighter than metal wires, they are more susceptible to interference.
- [d] They are less susceptible to interference than metal wires but carry analog signals that slow down transfer of data.

Module 4-Fibre Optics

Fibre optic technology uses glass threads (or fibres) to transmit data or carry signals in the form of pulses of light. It can carry signals up to 50km without the help of repeaters.

Structure:

It consists of a glass core that is approximately 50 micrometers, and is embedded with "optical cladding" of glass. This usually makes it 120micrometers in diameter. The glass core has a refractive index that is higher than the cladding. The cladding by itself does not carry light but helps in maintaining the critical angle constant, along the length of the fibre. Optical fibres confine the light within the inner core. Wherever the wire bends the light also bends accordingly. For this reason they are also known as waveguides.

Cladding

Fibre core

Propagation of light:

Light travels at maximum speed in vacuum and slows down in any other medium. The speed of light changes when moving from one medium to another causing deflection of light. This is termed Refraction. The Refractive Index N indicates the amount of deflection.

$$N = \frac{(\text{speed of light in vacuum})}{(\text{speed of light in the medium})}$$

Angle of Incidence Normal Angle of refraction

medium 1

medium 2

The figure shows Total Internal Reflection

When light passes from one medium into another that has a higher refractive index, it is refracted back towards the normal. But when it travels from a medium with high refractive index to one with low refractive index, it is refracted away from the normal.

If light enters in at an angle, then q_i , refers to the angle of incidence in medium 1 and q_r refers to the angle of reflection. As the angle of incidence increases the angle of refraction moves closer to 90 degrees. When the angle of refraction is 90 degrees, it is referred to as the critical angle. When the angle of incidence becomes more than the critical angle, then the light is totally is reflected back. This is referred to as **Total Internal Reflection (TIR)**.

In the fibre optic, when light is passed in to the fibre it meets the glass core-optical cladding interface. Since the refractive index of glass is higher than the refractive index of the optical cladding, it is reflected back into the core, which again gets reflected due to TIR. This process continues until it reaches the end of the fibre.

Areas Of Applications:

Fibre optic technology has a wide range of applications.

Sensors: Research is being conducted so that it can be used in gas concentration, chemical concentration, pressure, temperature, rate of rotation and the like

Telecommunications: Fibre optic cables now link telephone substations supporting transmission with reduced loss of signals.

Cable TV: It can also be used in cable TV networks because power consumption is considerably lower.

Closed Circuit Television: It is also used for closed circuit television security for monitoring.

Advantages:

- It is free from external interferences and hence immune to electrical distortions.
- It carries signals with far less energy loss than copper cable. Its higher bandwidth can also carry more signals to far off distances.
- Fibre optic cables have a lifespan of more than 20 years.
- It is very light and thin compared to copper cables, and requires less space and energy for installation.
- Information taping is much more difficult, therefore it is more secure than the copper wire.

Notes:

Micrometre : One millionth of a metre

Answer: [b] It consists of inner core and outer cladding.

Module:4 Reference No:M4024

Question: Which of the following requires two different keys for encryption and decryption:

- [a] Symmetric Cryptography
- [b] Asymmetric Cryptography
- [c] Cryptanalysis
- [d] Cryptology

Module 4- Encryption

Cryptography is the science of storing information in a modified form. The information will be revealed only to those who are authorised; and, hidden from all others. The original information is termed "**plaintext**", while the hidden information is termed "**ciphertext**". **Encryption** is the process of transforming plaintext into ciphertext, so that it cannot be read and understood by anyone, except the intended recipient/s. **Decryption** is the process of transforming ciphertext into plaintext. **Cryptosystem** is a method of encrypting and decrypting information. **Cryptography** is the art of creating and using cryptosystems. **Cryptanalysis** is the art of breaking into cryptosystems. **Cryptology** includes both cryptography and cryptanalysis.

As encryption modifies the original message, a key is necessary to decode and understand the message. For example, let us substitute each alphabet in a message with the next letter. If the key=1, the algorithm considers A=B, B=C and so on. If the key =2, then A =C, B=D and so on. If the original message is " INFORMATION SYSTEM " then the encrypted version depending on the key is as follows:

Key=1: JOGPSNBUJPO TZTUFN

Key=2: KPHQTOCVKRP UAUVGO

Types of Cryptography

- 1.Symmetric (or secret-key)
- 2.Asymmetric (or public-key).

Symmetric cryptography uses a single key for encryption and decryption (the decryption key can be easily derived from the encryption key). This means, both the sender and receiver must be aware of the key. Symmetric cryptography can be divided further into:

- Stream ciphers which encrypt a single bit of plaintext at a time
- Block ciphers which take a number of bits (typically 64 bits in modern ciphers), and encrypt them as a single unit. The most widely known instance of a symmetric cryptosystem is DES (Data Encryption Standard)

Asymmetric cryptography uses two keys, one for encryption (public key) and another for decryption (private key). A widely used instance of asymmetric key cryptosystem is Pretty Good Privacy (PGP). Two keys, one public and the other private are generated together as a pair, for this purpose. The software keeps the public key in the key-server for public access and protects the private key for decrypting the information received. For generating keys, the following issues should be considered

- 1.Size of the key: Longer key size makes keys more secure.
- 2.User ID: It consists of name and email address. E.g.: Kumar<Kumar11@yahoo.com>. The user is known to the PGP and the world with this ID.
- 3.Passphrase: The purpose of the passphrase is to protect the secret key from unauthorised use. Without a passphrase, it is not possible to sign or decrypt a message. It is called a passphrase (as opposed to a password) because it accepts several words and special characters including white space. The longer the passphrase and the more unusual characters it includes, the harder it will be to crack the key.
- 4.Sequence of keystrokes: Random keystrokes (akwoi423^&576hgcvklasdf9) make the generated key unique. The larger the key, the more keystrokes it requires.

When a person has to send an encrypted message to Kumar, he first goes to the key-server and extracts his public key with the help of his User ID in the key-server. The message is then encrypted using the public key and sent to Kumar. Kumar decrypts the message with his private key, which he extracts by using his Passphrase.

Answer: [b] Asymmetric Cryptography

Question: A Bluetooth "piconet" can have a maximum of _____ slaves.

- [a] One
- [b] Three
- [c] Five
- [d] Seven

Module 4- Bluetooth Concept

Bluetooth got its name after Harald I Bluetooth who ruled over Denmark. He was the son of King Grom who had a dream of conquering Norway and unifying it with Denmark. But it was Harald who realised his father's dream. Just as Old Harald Bluetooth united Denmark and Norway, the technology Bluetooth aims at uniting the world of computer and telecom.

Bluetooth is a computing and telecommunications industry specification that describes how mobile phones, computers, and personal digital assistants (PDAs) can easily interconnect with each other and with home and business phones and computers using a short-range wireless connection. Developed by the members of the Special Interest Group (SIG), Bluetooth has become a global de facto standard for wireless connectivity. Based on a low-cost, short-range radio link to carry data, Bluetooth eliminates the cords that are otherwise used to connect digital devices. These devices are then called Bluetooth-enabled devices.

How it works

Let us first equip ourselves with a few basic concepts that would help us understand better the functionality of Bluetooth:

Piconet

Bluetooth has been designed to incorporate many users simultaneously. A maximum of eight users or devices can communicate with each other in a small network provided they are within the range of 10 meters from each other. This is known as a piconet. A simplest arrangement would comprise two users/devices wherein one acts as a master and the other as a slave. This is also referred to as point-to-point topology. In case of multiple slaves the topology is point-to-multipoint and can have a maximum of seven slaves but only one single master wherein each slave is identified by a 3-bit address Active Member Address (AM_ADDR). Hence, piconet is a Bluetooth network that can have only one master.

Scatternet

Bluetooth specification caters to a scenario wherein two piconets are very close and as a result overlap with each other. This is known as scatternet. Slaves in one piconet can act as either a master or slave in the other piconet. This is done by sharing time between the different piconets in a manner that all the piconets get a chance to access that device at some point of time or the other. We can have a maximum of ten piconets in one single scatternet suggesting that a maximum of eighty devices can be connected to each other with a combination of piconet and scatternet.

Let us consider an example of how Bluetooth works. You might be travelling in your car with only a mobile phone and your PDA and can still receive emails. Your PDA and mobile will come under the range of 10 meters and hence form a piconet. The mobile phone is linked to the outside world using WAP [1] technology that receives your mails and transfers it to your PDA.

Bluetooth could play a major role in setting up Wireless Private Area Networks. Such networks are set up by low-end users and can be installed at our homes without disturbing its decorum because there is no cabling required. The cable-replacement technology transparently synchronises data across devices and creates access to network.

Challenges

If an organisation has a wireless LAN (WLAN)[2] in place, the placement of a piconet within a wireless LAN may crop up problems and pose a challenge for the administrators. Moreover, with wireless LAN available for the same cost and addressing to wider needs, Bluetooth might soon be extinct.

[1] WAP stands for Wireless Access Protocol and uses wireless communication media like radio waves and others to transfer data.

[2] Wireless LANs are networks that transmit and receive data through electromagnetic waves and hence counter the problems of cabling and accessibility.

Answer: [d] Seven

Module:4 Reference No:M4026

Question: The voice data is transformed from analog to digital mode or vice-versa by:

- [a] Internet Service Provider
- [b] Gateway Server
- [c] VoIP Service Provider
- [d] PSTN Station

Module 4- VoIP Concept

VoIP stands for Voice over Internet Protocol. As the name suggests, it includes delivery of voice with the help of the "omnipresent" Internet Protocol. We refer it as omnipresent because Internet Protocol or IP has become the standard for any kind of communication and forms the backbone of the Internet. To understand clearly the concept of VoIP we should first know what is an IP and how can it be used to transfer voice data.

Internet Protocol (IP)

Internet Protocol or IP forms a part of the family of communication protocols called TCP/IP [1] and has become the de facto standards for the communication of data. In an IP network, each computer is assigned an IP address such as 174.20.1.6. Information travels between computers in the form of packets where each packet has the IP address of the destination but one important fact is that IP does not guarantee the delivery of the packets. All it does is to send the packets across the network without worrying about the fact that they reach their destination or not. These packets have no fixed route or order in which they move. They are received at the destination and assembled back in the right order.

Voice over Internet Protocol

When a telephone call is made using the conventional telephone network there is an actual physical connection being established between the two telephones. Such a network is called a "circuit-switched" network and the telephone network using this technology is called Public Switched Telephone Network (PSTN). On the other hand, when voice is sent using an IP, there is no physical connection between the sender and the receiver. Voice is digitised at one end and converted to packets wherein each packet contains about 1/100th of a

second of speech. Such a network is called a "packet-switched" network. Since the transmission of voice data is done using the Internet, VoIP is also referred to as Internet Telephony.

How it Works

Just as ISPs (Internet Service Providers) we have VoIP Service Providers or VSPs. Mostly we have ISPs taking over the role of VSPs because they already have an established infrastructure and both the services mainly use the same kind of technology. When we pick up the phone and make a call it first goes over to the PSTN station which in turn transfers to the VoIP. A gateway server in place at the VoIP's end compresses it into IP packets and moves it onto the Internet for transfer to another gateway sever at the receiving end. This server converts the digital IP packets back into the analog form and transfers it to the local PSTN station that completes the call locally.

Advantages

Reduced Costs

Telephone calls made using VoIP costs much less as compared to the traditional PSTN calls. Users can now by-pass the per-minute usage rates and instead go for a flat rate as in monthly Internet access fee.

Unified Messaging

With the advent of VoIP, unified messaging can be made possible. Unified messaging gives us access to all kind of messages be it voice, fax or email using the same communication medium.

Disadvantages

Latency

This refers to the delay in transmitting the packets. There are three main reasons for the delay.

First, there can be a delay in receiving sufficient amount of data to be compressed in one packet.

Second, there can be a delay in transmitting the packets across the Internet.

Third, delay can be caused in converting the IP packets back into the analog form. Also, the quality of speech goes down because of higher level of compressions.

[1] TCP/IP stands for Transmission Control Protocol/Internet Protocol. It is the standard that is followed for all the communication that takes place on the Internet.

Answer: [b] Gateway Server.

Question: SET transaction is initiated by the:

- [a] E-wallet
- [b] Merchant Server
- [c] Acquirer
- [d] Certificate Authority

Module 4- SET Concept

Secure Electronic Transactions (SET)

Even though Secured Socket Layer (SSL) transactions ensure authenticity of the communicating parties and integrity of data transferred over the Internet, credit card security leaks still cropped up from time to time. These were not caused by hackers picking up credit card numbers 'of the wire', but were caused by poor security at the merchant's website, who had details of the customer's credit card account.

SET is a set of standards that makes it safe for an individual or business to use the payment card to pay for goods, even when the transaction occurs in a completely insecure environment like the Internet. SET can be used with any type of payment card including credit and debit cards.

SET Components

Even though encryption and other high-end technologies have hardware requirements, SET is a piece of software deployed by all the communicating parties. A simple SET transaction involves four parties- customer, merchant, acquirer and the card-issuing bank, and four types of SET components. Without these, such a transaction would not be possible. They are:

- *A cardholder application* also referred to, as an **e-wallet** is software run at the customer's end. This application generates a SET protocol that can be accepted by the SET merchant, payment gateway and certificate Authority component.
- *A merchant server component* run by the online merchant processes payment card transactions. It communicates with the cardholder application, payment gateway and the certificate authority component.
- *A payment gateway* is a product installed at the acquirer's end. Acquirer is a neutral party that processes merchant authorisation and payment requests with financial institutions.
- *A certificate authority* component is run by financial institutions to verify digital certificates as requested by the other three parties, and also to process financial requests.

How it works

Let us consider an example to understand the working of SET.

The customer having made a purchase will initiate a transaction for payment. The client's browser and the merchant's server decide on a private session key. Using his "e-wallet", the customer places an order information, credit card data and his digital certificate into an electronic "envelope". This envelope is encrypted using the session key decided earlier and is sent over to the merchant who decrypts and opens it to extract the order information. The merchant now places the consumer's card number and digital certificate along with his digital certificate into an electronic envelope and sends it to the acquirer. After verifying the consumer and merchant's digital certificates, the acquirer validates the credit card information

with the card-issuing bank. After the card information is verified, the acquirer gives an authorisation response to the merchant, who in turn completes the transaction by releasing goods for shipping. The merchant then requests the acquirer for a settlement of funds with the credit card institution, which then releases funds to the merchant's bank account.

SET-Better than SSL

Even though most websites opt for SSL transactions, it has a significant drawback. SSL ensures safety of data during transmission by way of encryption, but the merchant obtains the customer's credit card number and may misuse it. SET works around this problem by barring the merchant's access to the customer's credit card. He receives only a confirmation of the authenticity of the customer's card. Another advantage with SET is that it can handle multiple parties at a time. While SSL is only between the customer and the merchant, SET handles four different parties at a time. This does reduce the speed of transaction but then, it's the price we have to pay for the security of data.

Answer: [a] e-wallet

Module:4 Reference No:M4028

Question: The most important process in an SSL session is:

- [a] Client authentication
- [b] Server authentication
- [c] Encryption of data
- [d] Symmetric key creation

Module 4- SSL Concept

Secure Socket Layer

In the e-commerce era, a majority of the business is done on the Web; hence, providing foolproof security for online transactions is a priority. The ideal solution would be to have checks that ensure message privacy, shielding confidential documents not only on your network but also across all networks through which the data travels.

Secure Socket Layer (SSL) is one such solution. It is a security protocol developed by Netscape Communications to compensate for the lack of data protection on the Internet. SSL can be used for any type of Internet service -whether it be FTP (File Transfer Protocol) or the Web, but currently it is popularly used by traffic on the Web. This protocol allows you to send and receive information to customers on the Web in an encrypted manner. Any information that is transmitted will be completely encrypted. Thus, though the data may travel across 20 or 30 networks, nobody will be able to read it en route.

How SSL works

When data is communicated between a client and the server, SSL ensures that the connection established is secure. This is done by authentication and encryption of both the client and the server. While authentication confirms the identity of both the client and the server, encryption creates a 'tunnel' to transfer data so that unauthorised users or systems cannot gain access to it.

SSL consists of two protocols: One is the SSL Handshake Protocol, while the other is the SSL Record Protocol. Both protocols work in tandem to ensure a secure electronic transaction. Let us consider the two protocols separately.

SSL Handshake Protocol

A session begins with an SSL handshake. This allows the server to authenticate itself to the client, after which the client and the server cooperate in creating a symmetric key that will be used for encrypting the data. SSL-enabled browsers and servers authenticate themselves using digital certificates that are issued by a third party called the Certificate Authorities or CAs. The SSL may also require the client to authenticate itself depending on the kind of transaction.

SSL Record Protocol

This handles data transfer during the SSL session initiated by the handshake protocol. This protocol uses the session key created earlier to encrypt all data that has to be transferred.

Let us consider an example. If a user wants to make an online purchase, he will first make a request for an SSL session to the Web server. The server then introduces and identifies itself using a digital certificate comprising the server's public key. After the client's browser validates the server, it generates a master key using the public key of the server, sends it back to the server, and holds a copy of it for itself. The web server receives and decrypts the master key, using its private key. So, both the client and the server have the master key that they use for encryption of the data and then send it across to each other. Even though seems a rather long process, it takes less than a second.

Answer: [b] Server Authentication.

Although client authentication, encryption and symmetric key creation are integral aspects of an SSL session, server authentication is the most important feature because it initiates an SSL session.

Module:4 Reference No:M4029

Question: SMTP resides on port_____ of the client/server.

- [a] 80
- [b] 25
- [c] 120
- [d] 1010

Module 4-SMTP Concept

Simple Mail Transfer Protocol (SMTP)

Simple Mail Transfer Protocol is the standard for sending email messages over the Internet. With the increasing use of the Internet for communication, there arose a need to develop a standard that would govern the movement of messages between networks. This prompted experts to specify RFC 821 and RFC 822. RFC 821 provides the specification of the protocol itself i.e. SMTP; while RFC 822 sets standards regarding the format of messages.

How SMTP works

Let us consider the case of a user sending an email:

The sender creates a message using an application running on the client system known as User Agent (UA). When the user sends the message, it is transmitted to his Internet mail server. After the message reaches the Internet mail server, it enters the Message Transfer System (MTS). The MTS relies on other Internet mail servers to act as Message Transfer Agents (MTAs) to transport the message to the receiving UA. After an MTA passes the message to the recipient's Internet mail server, the recipient sees a new mail in his "inbox" and can access the message. Although it seems very simple, there are a lot of technicalities involved.

Communication between two systems is possible only when they have established a connection between the respective ports. When an email has to be transferred from one system to another, a connection is established between the ports (25) of the two machines. Listening to this port is an email daemon that speaks SMTP. After the connection has been established, the sending machine or the **client** waits for the receiving machine or the **server** to begin the conversation by sending a piece of text, giving the identity and indicating its willingness to receive the email. If the server is not willing, the client frees the connection to try later. If the server is ready to accept the email, then the client announces the sender and receiver of the email. If such a recipient exists, the server allows the client to send the message, and on receiving the message acknowledges it. When the message has been delivered, the connection is released.

E-mail format

RFC 822 defines the standard format for e-mail messages as having two parts: an envelope and the content enclosed. According to RFC 822, the envelope contains information required to transmit and deliver an e-mail message to its destination. The content is the message that the sender wants delivered to the recipient. The envelope contains the e-mail address of the sender, the e-mail address of the receiver and a delivery mode, which states that the message is to be sent to the recipient's mailbox. We can divide the content into two parts, a header and a body. The header is automatically included by the sending UA at the top of the message.

Answer: [b] 25

Module:4 Reference No:M4030

Question: Which of the following is an application level firewall?

- [a] Packet filtering routers
- [b] Proxy systems
- [c] Stateful inspection
- [d] Circuit layer gateways.

Module 4- Firewalls Concept

Introduction

With the increase in networks both within the organization and outside, its vulnerability to intrusion has also increased. In order to protect the networks of individuals or organizations, several safety measures are adopted. Firewalls are one such measure. It creates barriers that prevent unauthorized access to a network.

What are firewalls?

A firewall in a network is a filter that checks information reaching the network both from within and from outside. It can be a program or a hardware device that enhances the security of the network by filtering the data packets that enter or leave a network. In addition, firewalls may also check for restrictions and perform 'accept' or 'reject' operations.

Types of firewalls

Firewalls are broadly classified into:

1. Network Level Firewalls
2. Application Level Firewalls.

This classification is based on the arrangement of the firewall in the protocol layer.

1. Network level firewalls

The OSI (Open Systems Interconnection) model has seven layers. Layer three is the network layer, layer four is the transport layer and layer seven is the application layer. Among these, network level firewalls function either in layer three or four. The information that passes as packets through the firewalls is scanned and routed accordingly. Such firewalls are extremely suitable for high-speed networks. Routers and switches are used as network firewalls. Network firewalls are further categorized as:

- Packet filters
- Circuit level gateways

In packet filtering, the data is allowed to pass through a filter after verifying the Internet Protocol (IP) header. The IP header contains the following identifiers:

- Packet's source address
- Destination address
- Application/protocol
- Source port number
- Destination port number

The administrator maintains a table of data that can be allowed to enter the network. The table contains a list of sources and destinations of IP packets. The filter, then checks the data with this table. If the details match, it permits the packets into the network. All other data is discarded.

Circuit level gateways operate in the transport layer. It uses the Transmission Control Protocol (TCP), which is a higher layer protocol than the one used for packet filtering. It provides more security than packet filters. It generates a session for each screening process of a data stream. Once the required parameters are met at the end of the session, the firewall closes the connection.

2. Application level firewalls

It occupies the application layer of the OSI model. Here information is broken into data streams rather than a series of packets. These firewalls are essentially hosts running on proxy servers. The proxy server applies protocol-specific access rules and performs access control based on user identities. Stronger user authentication in the form of logons is available.

3. Stateful Multi-layer inspection

To mitigate problems related to firewalls that are specific to a single layer, a hybrid system was devised. Here the software can function in different layers. Here certain parts of the packet of data are examined and not the entire contents of each packet of data. Information that passes from inside the firewall to outside is monitored for specific characteristics. If a match exists, the data is allowed, else it is discarded.

Answer: [c] Proxy Systems.

A proxy server is a software agent that acts on behalf of a user. Typical proxies accept a connection from a user, make a decision about whether or not the user or client IP address is permitted to use the proxy, does additional authentication, and then completes a connection on behalf of the user to a remote destination.

A proxy server (sometimes referred to as an application gateway or forwarder) is an application that mediates traffic between a protected network and the Internet. Proxies are often used instead of router-based traffic controls to prevent traffic from passing directly between networks. Many proxies contain extra logging or support for user authentication.

Module:4 Reference No:M4031

Question: _____ **do not have an address table when they are first installed.**

- [a] Simple bridges
- [b] Multiport bridges
- [c] Transparent bridges
- [d] None of the above

Module 4- Bridges Concept

Bridges

The physical distance that Local Area Networks can cover, and the number of hosts that can be attached are limited. To overcome this limitation, bridges are introduced to connect two or more LANs. Bridges allow hosts attached to different LANs to communicate, as if they were located on the same LAN. They are capable of distinguishing between local and remote data; hence data transferred from one terminal to another on the same LAN doesn't have to cross the bridge. Unlike routers [1], they do not perform the job of selecting the path that the data packet should take, to reach its destination.

How bridges work

Bridges divide a LAN into segments. For example, a building spanning many floors may have numerous terminals connected in a LAN. Each floor may form a different segment, and many such segments can co-exist on a single LAN. Bridges operate at the Data-Link Layer [2] of the OSI Model [3], which provides them with an address list, with the physical address of all terminals attached to it. When a data packet enters a bridge, it compares the address on the packet with the address list. If there is a match, it figures out the segment to which that terminal belongs, and relays the packet only to that segment. If the data transfer is between two terminals in the same segment, it is blocked from entering another segment; instead, it is relayed to all systems on the same segment.

Types of bridges

Simple bridges are the most primitive and the least expensive of all kinds of bridges. Such a bridge connects two segments, and has an address table that contains the physical addresses of all terminals included in each of them. It is rather primitive because it requires an operator to manually feed in the address of all terminals that are connected to it. In case a terminal is removed, its address has to be deleted from the address list.

Multiport bridges are used to connect more than two LANs. Such bridges have address tables corresponding to each LAN, with addresses of terminals that are attached.

Transparent bridges build their address table as they perform bridging functions, and are also referred to as learning bridges. At the time of installation the address table remains empty. With each bridging function, source addresses are included and the table is built. As soon as, the bridge receives a data packet, it reads both destination and source address. If it does not find a match between the address in the table and the address associated with the packet, it floats the packet on the LAN for the relevant terminal to pick it up. Once the data is picked up, it identifies the segment that the terminal belongs to. Thereafter, data is sent directly to this terminal.

- [1] Routers are devices that transmit data packets across networks. They are sophisticated devices that also perform the task of routing the information to its destination with the help of various algorithms.
- [2] Data Link Layer is the Layer in the OSI model that transfers data in frames.
- [3] Open System Interconnection (OSI) is a specification that describes how a data packet is transferred between two nodes

Answer: [c] Transparent Bridge.

Module:4 Reference No:M4032

Question: MIME essentially acts as:

- [a] A transport agent for e-mail
- [b] An interface between the mail client and the web server
- [c] A compressor that packages different formats into SMTP compatible type
- [d] None of the above

Module 4- MIME Concept

Initially, the Internet e-mail system was limited to simple text messages because SMTP [1], the protocol used to transport mail over the Internet, could carry only ASCII [2] text. However, the use of data has moved beyond mere text, with different kinds of word processing programs coming into the picture. These programs support rich text format such as italicised or boldfaced that are not supported by the 128-character set as specified by ASCII. This limitation looms large when you realise that the Internet e-mail system is perfectly suited to act as a data delivery vehicle i.e. there is a pipeline linking users, from desktop to desktop. If e-mail could handle diverse data - such as word processing documents and image files - users could share all types of data, without having to ship disks or make any actual real-time network connections to copy or download files. To work around this limitation MIME was introduced.

MIME

Multipurpose Internet Mail Extensions (MIME) refers to an official Internet standard that specifies how messages must be formatted, so that they can be exchanged between different email systems. It was defined in 1992 by the Internet Engineering Task Force (IETF) in an Internet standard paper, the RFC [3] 1521. MIME is very flexible, and permits the inclusion of virtually any type of file or document in an e-mail message. Messages can contain text, images, audio, video or other application-specific data.

How it works

Since SMTP does not support any other format other than the 7-bit ASCII format, MIME packages different data formats that are compatible with SMTP. Hence, all e-mail, regardless of the data it contains, appears as standard e-mail messages to the Internet's SMTP servers. To top it all, SMTP didn't have to change to handle such data. The solution also did not require Internet mail servers be upgraded (to a new version of SMTP), which would have been an uphill task.

Supported Media Types

RFC 2045 defines seven types of e-mail content that MIME can package and send over the Internet. They are:

- [1] SMTP stands for Simple Mail Internet Protocol and is a standard for sending e-mails over the Internet
- [2] ASCII stands for American Standard Code for Information Interchange that is a 128 character set comprising numbers, alphabets and special symbols.

[3] RFC stands for Request for Comments. RFC is maintained by the Internet Society and contains documents on the Internet Protocol Suite as designed by the Internet Engineering Task Force.m.

Answer: [c] A compressor that packages different formats into SMTP compatible type.

Module:4 Reference No:M4033

Question: Which one of these options allows multicasting and broadcasting in an ATM LAN?

- [a] Ethernet
- [b] Token ring
- [c] LES
- [d] BUS

Module 4- ATM LANs Concept

Local Area Networks (LANs) when connected with routers and gateways evolve into wide area networks. Services involving simple data transfers and high-end multimedia applications demand a better technology than a LAN, which uses shared media connections. Broadband multiplexing and switching networks remove bottlenecks. Features of ATM like larger bandwidth, increased scalability and manageability can be utilised to emulate a LAN.

Why ATM-based LANs?

- Traditional LANs deploy IEEE 802 standards like ethernet, token ring and buses, which are shared media interconnects. They use connectionless data gram packets of Internet protocol for transmission of data. Since these shared media interconnects are used in LANs, all communication is broadcast.

On the other hand, Asynchronous Transfer Mode (ATM) is not a broadcast medium. Two ATM hosts have to establish a connection between them before data is transferred. This connection is termed a virtual channel. Data is then transferred in fixed-size ATM cells. ATM being a switch-based network provides for optimum use of bandwidth.
- QOS (Quality Of Service) is a contract/agreement between the customer (user) and the network to ensure efficient use of the connection. QOS is guaranteed in ATM networks.
- Transparent support for common protocols. ATMs share the IP protocol stack (a group of protocols constitute a Protocol stack), which makes it compatible with existing networks. In addition, an ATM adaptation layer is incorporated into the data link layer protocol or an MAC (Message Access Control) layer is incorporated over the LLC (Logical Link control) layer of the protocol stack.
- ATM is designed to support simultaneous transfer of data, audio, and video at speeds ranging from 5.1 Mbps (Mega bits per second) to 1.2 Gbps (Giga bits per second). This enables full-motion video, CD-quality audio, and high-speed data communications to work flawlessly.

Local Area Network Emulation

ATM switches implement virtual channels for ATM cells to be transmitted in a network. This necessitates a virtual path/virtual circuit identifier. These virtual circuits have to be implemented in a connectionless LAN that possesses traditional addresses (as found in IP datagram packets). The approach to make an ATM switch behave/work like a LAN switch is called as Local Area Network Emulation (LANE).

With the help of LANE, broadcast delivery can be achieved. Hence, LAN emulation means the point-to-point ATM switch requires a shared virtual medium. It works on the client/server model. A LANE client (LEC) software and two servers use two different softwares (the LANE Server (LES) and the Broadcast/Unknown Server (BUS)) to comply with this two-tier architecture. LES is used when a frame is sent to particular destination. BUS is used when a frame has to be sent to multiple destinations.

Types of ATM LANs

Gateway to ATM WANs

An ATM switch acts as a router to connect the ATM network with other networks. This acts as an end point for setting up a virtual connection.

Backbone ATM switch

A single ATM switch is used to connect LANs. A group of ATM switches connects different LANs.

Work group ATM

Systems that require high-end applications like integrated multimedia computing utilise the ATM switch directly, through dedicated connections and serve as Work group ATMs

Answer: [d] BUS

BUS (Broadcast/Unknown server) supports multicasting and broadcasting in an ATM LAN. LES is another server software that works on the client/server model. Ethernet and Token ring are LAN standards that are not used in ATM applications.

Module:4 Reference No:M4034

Question: Which of the following elements is unique to a Smart Card?

- [a] Magnetic stripe
- [b] Microchip
- [c] Signature
- [d] Photograph

Module4-Smart Cards

A single card that can hold variety of information, simplify many day-to-day tasks and replace the currencies would be of immense boon to consumers. The decline in the usage of magnetic stripe cards due to its inherent security lapses has led to the new concept of smart cards.

What is a smart card?

A Credit card sized plastic card with an embedded computer chip that can hold data used in a variety of applications is termed as a smart card. The chip used in the card is a microprocessor with internal memory or a chip with non-programmable memory. Microprocessor cards can perform complex calculations, store information, and carry out local processing using the stored data. The chip is attached to the card through a direct physical connection or a contact less electromagnetic interface.

How does it work?

Smart cards have an inbuilt 8-bit micro controller that can hold 16KB or more of data. The communication between the card and the computer is achieved by the use of smart card readers that can read the information from the microcomputer chip. This card reader in turn is connected to a computer or remote office where processing takes place. A smart card is called a contact smart card when it requires insertion

into a smart card reader. The reader has a direct connection to a conductive micro module (a device that processes the transaction carried with the card). The surface of the card is gold plated. It is through these physical contact points, that transmission of commands, data, and card status takes place.

Another category called contact less card requires only close proximity to a card reader. Both the card reader and the card have antenna and it is via such contact 'less' link that the two communicate. Contact less cards derive the internal chip power source from electromagnetic signals. Microprocessor chip can add, delete and manipulate information in its memory. Industry standards for interface between programming and the computer hardware in smart card have been established.

Categories:

The are primarily three types of smart cards:

1. Integrated Circuit (IC) Microprocessor Cards
2. Integrated Circuit (IC) Memory Cards
3. Optical Memory Cards

Microprocessor cards or chip cards are the ones that have more memory storage capacity, security of data and process capability than the magnetic stripe cards. They use an eight-bit microprocessor with 16KB (Kilo bytes) of read only memory and 512 bytes of random access memory. They are suitable for high end cryptographic number processing.

IC memory cards have no processor inside the cards but have memory space of 1-4 kilobytes. They are more suitable for specific applications with more dependence on a card reader.

Optical memory cards are similar to a compact disc with a memory of 4MB (Mega Bytes). They are read only cards and are mostly used for large data storage.

Security

The data stored inside the card is hard to be read without proper authorisation. This makes the card more secure than the magnetic stripe based cards. Software is incorporated to ensure both authentication and authorisation. Authentication is done through traditional practices like PINs (Personal Identification Numbers) or passwords. Authorisation of the cardholder is through digital certificates where authenticated card holder is entitled to view the required information.

Applications

Financial Applications

- Electronic Purse
- Credit or Debit card with more security.
- Secure payment across the Internet.

Communications Applications

- Secure caller identification (for billing purposes) on any Global System for Mobile Communications (GSM) phone.

Government Programs

- Electronic Benefits Transfer in lieu of paper coupons and vouchers.
- Agricultural producer's smart marketing card to track quotas.

Information Security

- Employee access card with secured passwords and biometrics to restrict access to computer systems.

Transportation

- Drivers Licenses.
- Electronic Toll Collection Systems.

Health Card

- Consumer health card containing insurance eligibility and emergency medical data.

Identification

- All-purpose student ID card, containing a variety of applications such as electronic purse, library card, meal card and the like.

Answer: [d] Microchip

A smart card has a microprocessor embedded into it, which does a variety of functions ranging from storing data to processing them. Magnetic stripes are used in traditional credit/debit cards. These also have signatures/photographs embossed on them as per the requirement.

Module:4 Reference No:M4035

Question: SONET is a standard for which of the following networks?

- [a] Twisted-pair cable
- [b] Fiber-optic cable
- [c] Coaxial cable
- [d] Ethernet

Module 4-SONET

As business applications require more consistent and dedicated access to networks, bandwidth requirements have increased. Apart from this, corporate networks demand high speed, flexibility in bandwidth, and fail-safe and secure operations. Due to its inherent properties of high bandwidth data applications, an optical fibre network would be the appropriate one. If SONET is implemented, communication carriers throughout the world can interconnect their existing digital carrier and fiber optic systems.

What is SONET?

SONET stands for Synchronous Optical Network. It is an ANSI (American National Standards Institute) standard for high capacity optical telecommunication. SDH (Synchronous Digital Hierarchy) is the equivalent standard adopted in Europe/ by ITU (International Telecommunication Union), which refers to the fibre optic transmission rates that can transport digital data of different capacities. SONET defines interface standards at the physical layer of the OSI (Open Systems Interconnection) seven-layer model. The standard defines a hierarchy of interface rates that allow data streams at different rates to be multiplexed (the process of sending multiple signals through a single channel). It is a multiplexing scheme for optical signalling. It has higher preventive monitoring capabilities and help speedy restoration of fiber when there is a breakdown.

How does SONET work?

Data is sent over an optical fiber by turning the light off and on in the fiber. Using "1" for the presence of light and "0" for the absence of light, one can send and receive bits across an optical link. The mechanism to extract the information from these bits is provided by SONET/SDH. It defines the low level framing protocol used on these optical links.

"Framing", means a block of bits (or octets) which have a structure, and which utilise some technique, to find the boundaries of the frame structure. A part of the frame stores overhead information for the network provider to use to manage the network. Other parts are dedicated to carry payload or information to communicate. SONET establishes Optical Carrier levels (used to specify the speed for fiber optic networks conforming to the SONET standard) from 51.8 Mbps to 2.48 Gbps.

Architecture

SONET works in two operational mode architectures.

1. Path switched ring
2. Line switched ring

Path switched ring uses two fibers to switch an individual path. Here signals are sent both ways (clockwise and anti-clockwise) around the two fiber rings that are arranged parallel to each other. Both signals reach the receiving end and the best among them is selected. This places a limitation on the data transfer rate of the network.

Line switched ring uses four bi-directional fibers to send the data in the required direction. A working fiber and a protect fiber is present in each direction. A protect fiber is one that acts as a protective shield over the working fiber (the fiber through which data is transmitted). In case of interruptions in signal line, switching can restore service and change direction of signal flow in less than 50 milliseconds in a ring distance range of 1,200 Kms.

SONET occupies the lowest level of the OSI protocol stack i.e, the Physical layer. By this it provides a roadway or path for a variety of other standards and protocols to share the network.

Further, it is neutral to the higher layers of the protocol stack enabling seamless compatibility with other standards.

Answer: [b] Fiber optic cable

SONET uses optical fibers as transmission media. Ethernet, coaxial cables and twisted pair are used in LANs and telephone networks.

Module:4 Reference No:M4036

Question: What are the categories under which X.25 devices fall?

- [a] DCE only
- [b] DTE and PSEs
- [c] DTE and DCE only
- [d] DTE, DCE and PSNs

Module 4-X.25

An interface standard between Data Terminal Equipment, DTE and Data circuit-terminating equipment, DCE for a packet switched network is called X.25 protocol. It is an International Telecommunication Union-Telecommunication Standardisation Sector (ITU-T) protocol for WAN communications that defines how connections between user devices and network devices are established and maintained. It is typically used in the packet-switched networks (PSNs) of common carriers, such as the telephone companies. Subscribers are charged depending on their use of network.

X.25 layers

X.25 protocol specifies three layers; the physical layer, the frame layer and the packet layer. These layers function in the physical layer, data link and network layers of the OSI (Open Systems Interconnection) layers.

The X.25 specification defines a point-to-point interaction between data terminal equipment (DTE) and data circuit-terminating equipment (DCE). DTEs (terminals and hosts in the user's facilities) connect to DCEs (modems, packet switches, and other ports into the PDN, generally located in the carrier's facilities). These DCEs then connect to packet switching exchanges (PSEs, or switches) and other DCEs inside a PSN and, ultimately, to another DTE.

Working

X.25 establishes virtual circuits that make it connection oriented. The connection is established, the data is transferred, and then the connection is terminated. End-to-end communication between DTEs is accomplished through a bi-directional association called a virtual circuit. Virtual circuits permit communication between distinct network elements through any number of intermediate nodes. There is no need for the portions of the physical medium that characterises physical circuits to be involved in this connection. Virtual circuits can either be permanent or switched (temporary). Permanent virtual circuits are commonly called PVCs, switched virtual circuits are commonly called SVCs. PVCs are used for data transfers, while SVCs are used for sporadic/irregular data transfers. Layer 3 of X.25 is concerned with end-to-end communication involving both PVCs and SVCs.

Once a virtual circuit is established, the DTE sends a packet to the other end of the connection by sending it to the DCE using the proper virtual circuit. The DCE looks at the virtual circuit number to determine how to route the packet through the X.25 network. The layer 3(Network layer) X.25 protocol multiplexes (Send multiple packets of data through a single channel) between all the DTEs served by the DCE on the destination side of the network and the packet is delivered to the destination DTE.

Packet Assembler/ Disassembler

A device that is used in a X.25 network when a DTE is not able to perform all the functions of the X.25 protocol is the Packet Assembler/ Disassembler (PAD). PAD is located between a DTE device and a DCE device, and it performs three primary functions: buffering (storing data until a device is ready to process it), packet assembly, and packet disassembly. The PAD stores data sent to the DTE device and also the data going out from the DTE device. It also assembles out going data into packets and forwards them to the DCE device (Adding an X.25 header is also done). PAD disassembles incoming packets before forwarding the data to the DTE. (This includes removing the X.25 header).

Answer: [d] DTE, DCE and PSNs.

X.25 network devices fall into three general categories: data terminal equipment (DTE), data circuit-terminating equipment (DCE), and packet-switching exchange (PSE). Data terminal equipment devices are end systems that communicate across the X.25 network. They are usually terminals, personal computers, or network hosts, and are located on the premises of individual subscribers. DCE devices are communications devices, such as modems and packet switches that provide the interface between DTE devices and a PSE, and are generally located in the carrier's facilities. PSEs are switches that compose the bulk of the carrier's network. They transfer data from one DTE device to another through the X.25 PSN.

Question: A class-B GPRS terminal can support _____ service at a time.

- [a] GSM and GPRS
- [b] GSM or GPRS
- [c] TDMA
- [d] TDMA and GSM.

Module 4-GPRS

What is GPRS?

A standard for wireless communication with an enhancement over GSM (Global System for Mobile Communications) with speed upto 115 kilobits per second is GPRS (Global Packet Radio Service). This standard provides all time dedicated mobile access in the form of email, Internet and the like. Packet-mode of transmission is used to transfer both high speeds and low speeds over GSM networks. GPRS supports a wide range of bandwidths and makes efficient use of limited bandwidth.

Features

- **Packet switching**

In an existing GSM network, which uses circuit switching, GPRS is added as a packet based air interface. Network operators include new infrastructure nodes and upgrade the software of some existing network elements. The information is split into separate packets before being transmitted and reassembled at the receiving end. All these packets are related and fit together, but the way they are transported and assembled varies.

- **Spectrum efficiency**

Spectrum refers to the frequency range within which a signal can be transmitted. GPRS radio is utilised only when users are actually sending or receiving data. There is no dedicated radio connection to a mobile data user for any fixed period of time. The available radio resource can be shared between several users and can be served from a single cell. This enables network operators to maximise the use of their network resources in a dynamic and flexible way, along with user access to information.

- **Supports TDMA and GSM**

General Packet Radio Service is designed on mobile networks that are based on the GSM digital mobile phone standard and the Time Division Multiple Access (TDMA) standard. This feature allows compatibility with the existing networks with few upgrades.

GPRS terminals

The variety of mobile phones and mobile stations that can function in a GPRS environment are called as Terminal equipment. Equipments come under terminal classes and types.

A GPRS terminal can be of the classes A, B, or C. Class- A terminal supports GPRS and other GSM services (such as Short Message Service and voice) simultaneously. This terminal can make or receive calls on two services (GSM and GPRS) simultaneously. Class B terminal can monitor GSM and GPRS channels simultaneously, but can support only one of these services at a time. Class C terminal supports only non-simultaneous connection. The user must select the service to get connected. . Therefore, a Class C terminal can make or receive calls from only the manually (or default) selected service.

PC Cards are credit card-sized hardware devices that connect through a serial cable to a mobile phone. Data cards for GPRS phones allow laptops and other devices with PC card slots to connect to mobile GPRS-capable phones. Smart phones are mobile phones with built-in voice, and Web-browsing services. Personal digital

assistants (PDAs) such as the Palm Pilot series and handheld communications are data-centric devices that are adding mobile wireless access.

Applications

Some of the applications both in corporate and consumer segment include Chat, Textual and visual information, Web browsing, Audio, Corporate email, Internet email, Vehicle positioning, Remote LAN access, File transfer and Home automation.

Answer: [b] GSM or GPRS.

Class B terminal equipments support simultaneous service but one at a time. Class A terminals are capable of working simultaneously. i.e. they allow simultaneous use of GSM and GPRS.

Module:4 Reference No:M4038

Question: Which feature makes an intranet similar to the Internet?

- [a] Corporate network
- [b] TCP/IP
- [c] LAN technology
- [d] Token ring

Module 4- Intranet

Storing and sharing of information is key to the success of any company. Information sharing and processing has to span all functional aspects of an enterprise. Seamless networking is essential. Corporate activities in a distributed decision-making environment can be effectively co-ordinated through intranets.

What are intranets?

Company wide networks or information distribution systems that use Internet technologies and a variety of hardware and software platforms through a web browser are referred to as intranets. An intranet ranges from being a HTML file on a LAN to a fully developed system with server hardware.

Features

- Uses TCP/IP (Transmission Control Protocol/Internet Protocol) for both wide-area and local-area transport of information
- Uses HTML (Hypertext Markup Language), SMTP (Simple Mail Transport Protocol) and other open Internet-based standards for moving information from clients to servers Is completely owned by the corporation and cannot be accessed via the Internet-at-large by the general public.

Benefits

- Improved access to corporate databases enhances efficiency and productivity.
- Improves internal flow of information, breaking down the boundaries between functions.
- Removal of paper based documentation results in cost savings.
- Supports work groups located in different offices across different cities/countries.

Steps to build a corporate intranet

- Make a board level initiative: To initiate change in a company briefing of the whole enterprise including the top brass has to take place to adapt to the electronic form of transactions. It means that a policy decision at the board level has to be enunciated.
- Build the communications infrastructure: Web architecture with browsers and mobile computing facilities has to be implemented.

- Opt for open systems: Adopt Internet standards like TCP/IP while making provision for accommodating other protocols so that the intranet is compatible as changes are made in the network architecture.
- Make it secure: Define privileges for individuals to access of information along with authorisation and authentication standards.
- Keep it simple: Implement in simple phases- first by introducing intra organisation mails, then browser and the like. This will ensure that employees can slowly adapt to the changing work culture.
- Support publishing: Encourage intraorganisational publishing that will increase the usage of intranets and supports teamwork.
- Redevelop the business: The intranet helps in reorienting the business set up .It allows employees to update their personal files It should also facilitate remote processing of sales orders and transactions. An intranet with specific customers will also be useful, to reduce transactional costs.

Answer: [b] TCP/IP.

Intranets use the same Internet standards. The other choices are LAN standards.

Module:4Reference No:M4039

Question: What is the similarity between a multiplexer and a hub?

- [a] Both of them use TDM
- [b] Both use FDM and STDM
- [c] Both are hardware
- [d] Both route multiple connections.

Module 4- Multiplexers and Hubs

Transfer of data in a network has to take place efficiently without compromising on speed. To transmit data signals in an efficient manner, multiplexing is used. The technique to combine multiple signals to be transmitted in a network into a single line or media or channel is called as multiplexing.

What is a multiplexer?

The hardware device that combines various signals for transmission over a single channel is a multiplexer. A similar circuitry at the receiving end of a communication channel where the multiple signals are separated into the original single form is called as a Demultiplexer.

What it does?

It accepts the signal from individual end user and breaks them into segments. These, segments are assigned to the composite signal in a particular sequence. The composite signal is then converted into parameters viz. time, frequency and the like, for efficient transmission over the network.

Multiplexing methods

The various methods of multiplexing forms the basis for its working. Some of the frequently used multiplexing methods include Frequency Division Multiplexing (FDM), Time Division Multiplexing (TDM), Statistical Time Division Multiplexing and Wavelength Division Multiplexing (WDM).

FDM: The mechanism of allocation of data signals in channels of different frequency slots for transmission is known as Frequency Division Multiplexing.

TDM: Accommodating the transmission signals in different time slots is termed as Time Division Multiplexing.

STDM: A variant of TDM where time slots are allocated to signals based as per the specific requirement of the application to make better use of bandwidth is called as Statistical TDM.

WDM: Wavelength is the number of cycles per second that a signal travels in any medium. By assigning different wavelengths, signals can be transmitted in the form of Wave Division multiplexing.

What is a Hub?

A network component that joins multiple nodes/computers together in any kind of a network is called as a hub. It is a physical component made of plastic that interconnects a series of ports/junctions of computers in a network. Ethernet and USB (Universal Serial Bus) are the two widely used hubs.

Features

Hub forms an interface at the lowest Layer 1(physical) of the OSI, Open Systems Interconnection model. It functions as a simple circuit for receiving and routing multiple signals. Three types of hubs are:

1. **Passive hubs:** Hubs that do not amplify the signals that enters it, before being routed for further transmission are termed as passive hubs. They are also known as concentrators.
2. **Active hubs:** Hubs that amplify the signals that enter it are also called as Repeaters.
3. **Intelligent hubs:** Active devices that can perform extra functions like remote management support (SNMP-Simple Network Management Protocol and VLAN-Virtual LAN) come under intelligent hubs.

Answer: [c] Both are hardware.

TDM, FDM and STDM are the different forms of multiplexing schemes used in Multiplexers. Hubs form as junction for interfacing two or more nodes. Multiplexers route the signal into a single channel and they are operationally different from one another.

Module:4 Reference No:M4040

Question: In which of the following services is Public Key Infrastructure (PKI) and Digital certification not a useful feature.

- [a] Virtual Private Networks
- [b] Web Authentication
- [c] File Encryption
- [d] Circuit Switching

Module 4- Public Key Infrastructure

Services offered by Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is a collection of components and procedures that uses Digital Certificates to manage cryptographic keys. The basic component of PKI is digital certificate that is issued to entities that can identify themselves, be they people, web server or any application. This certificate identifies the entities involved in any online transactions. In addition it ensures integrity, confidentiality and non-repudiation of data. The features of PKI are done through cryptography. A pair of public/private key associated with the certificate performs the cryptographic functions. The certificated and associated key pairs offer following services -

- **Web Authentication** - Web makes possible the transfer of any kind of information to any part of the world. However web is not a secure environment, any information that is transferred may be intercepted, changed and stolen. Thus there is a need for authentication of transacting parties. A

certificate is needed to establish authentication. After authentication encryption keys are provided which ensure confidentiality and message integrity.

- **Securing messages** - E-mail is another area prone to attack. Organisations should ensure maintenance of integrity of information while sending messages. Certificates and associated keys are used to encrypt and sign the messages digitally.
- **Digital signature of Forms and Transactions** - A digital signature in an electronic world is much like a signature on the paper. Digital signature binds the signer to the transactions that are initiated or content written in a contract. However, the contracting parties should agree upon the PKI policies.
- **User and Network Authentication** - PKI enables multiple systems to use certificates for authentication of end users. This solves the problems of different user IDs/passwords for different servers and users may access any applications by just authenticating once. This also helps in case of remote access where certain employees are at different locations. In this case also, certificates are more reliable to access the LAN from other locations rather than using user id and password.
- **Virtual Private Networks** - VPN facilitates communication between two parties by using a public network. Head office and branches located at different location use Internet in order to save the cost of leasing WAN lines for each office. In such cases certificates authenticate the end points in VPN.
- **File Encryption** - Many files are shared over a LAN. This exposes sensitive information to risks. Generally most LANs run Transmission Control Protocol (TCP)/ Internet Protocols (IP), but do not take care of encryption. Many network administration develop the list of permission granted to different users, but this system of making and processing lists often break. This may lead to exposure of sensitive information to anybody connected to LAN. PKI helps in issuing certificates of attestation to the keys that were used in encryption of such sensitive data.
- **Software Code Signing** - Many companies in the business of developing software distribute updates on software via web. This poses certain security issues since it is easy to intercept the update and alter the code with a virus. Software code signing enables developers to digitally sign the code. Receiver comes to know in case the code is intercepted and altered.

Answer: [d] Circuit Switching

Module:4 Reference No:M4041

Question: Which of the following is not a PKI Component -

- [a] Certificate Authority
- [b] Merchant Server
- [c] Time Server
- [d] Signing Server

Module 4- Components of Public Key Infrastructure (PKI)

PKI enables issuing, distributing and managing the use of digital certificates. To accomplish this task, PKI needs many components. They are -

1. **Certificate Authority** - CA is the trusted authority that certifies identities and creates digital certificates. This digital certificate links an identity to public/private key pair. To issue a certificate we need a set of software and hardware components. The personnel, process flow and policies that define rules to establish identity should be in place to issue a proper certificate. By reading the rules, subscribers and certificate users should satisfy themselves that the identities certified by CA are

useful for them. Rules that describe the constraints and various operations are defined in a document called the Certification Practices Statement (CPS). This statement issued by CA should be available with the certificate user otherwise identities may be doubted. CA has certain sub-components which are discussed below -

- a. **Registration Authority (RA)** - Internet Public Key Infrastructure Certificate Management Protocols state that functions of RA includes "personnel authentication, token distribution, revocation reporting, name assignment, key generation, archival of key pairs, etc". It takes care of registration and initial authorisation of subscribers. Subscribers are users who get certificates after their registration request is approved. The most important responsibility of RA is to ensure submission of certificated request and validation of identity.
 - b. **Certificate Server** - It refers to the machine and service that issue certificates based on the information provided at the time of registration request. The user's public key is used, and is combined with other identifying information to produce a certificate structure, which is signed using the CA's private key.
 - c. **Certificate Repository** - It is a place where all the certificates and corresponding public keys are stored which can be accessed. It is important to make the public keys available before they can be used and can be accessed by all end entities and CAs. In case certificates are to be distributed, then repository is a place where the certificates are published. These repositories are directories, occasionally X.500 directories, but most of the time LDAP (Lightweight Directory Access Protocol) directories. This is a protocol, which is used to interact and access the information in directories.
2. **Certificate Validation** - Once the certificate users receive certificates, they are required to validate them. It involves the following -
 - o Verifying the signature
 - o Check validity period to ensure that the certificate is current
 - o Check the compliance of the intended use of certificate against any policy constraints specified by the CA
 - o Verify for revocation (cancellation) of the certificate issued by the CA
 3. **Key Recovery Service** - It is important to have a mechanism to access archive keys so that they can be recovered in case they are lost. This ensures that information can be decrypted even if the key is lost due to unforeseen circumstances. For instance, an employee encrypts some information and due to some reason public/private key pair is lost. Then in that case organisation where the employee works may use the facilities of Key Recovery Service to recover the information.
 4. **Time Server**: Certain time sensitive transactions require time stamp services. Suppose A directs B to carry out a financial transaction in an hour, B may deny receiving the information on time. If there is no way to ascertain the time of receiving the information then A will have no legal grounds against B in case he loses money. Timeserver helps in providing digital time stamps. Using a Time Stamp Protocol (TSP), A sends the message hash and digital signature via e-mail to Time Stamping Authority (TSA). TSA digitally signs the request of A and sends it back. This is the proof; A has to support his claim.
 5. **Signing Server** - Signing server acts as a central signing and verification service of documents and transactions to which digital signatures are applied.

Answer: [b] Merchant Server

Question: ----- is a security protocol that can be used with Multipurpose Internet Mail Extension (MIME) to send messages through mixed transport systems, because of object-based features.

- [a] PGP (Privacy Good Policy)
- [b] S/MIME (Secure/Multipurpose Internet Mail Extension)
- [c] PEP (Privacy Enhance Mail)
- [d] MIME Object Security Services

Module 4- MIME- Security Issues

MIME-Security Issues

Every Internet message has two parts -

- Header - It is the collection of field/value pairs that are structured according to STD 11(RFC 822)[1].
- Body - It is structured as specified by MIME specifications.

However, the structure as defined by MIME does not provide security for information, sent through e-mails.

RFC 1847[2] provides a framework where security can be provided, if protocols are used along with MIME in a complementary manner. This framework provides two types of multipart security -

- Multipart/Signed Content type - It involves authentication and integrity of content through the use of digital signatures.
- Multipart/Encrypted Content type - It ensures confidentiality by encrypting the content

MIME Object Security Services (MOSS) protocol uses Multipart/Signed and Multipart/Encrypted framework, described in RFC 1848[3]. MOSS is based on Privacy Enhanced Mail (PEM) protocol; this protocol uses a certificate-based key management mechanism to encrypt and authenticate text messages. The usage of PEM is described in detail in RFC 1421[4], RFC 1422[5], RFC 1423[6]. PEM is compatible with many Internet Mail systems.

Another protocol that can be used along with the MIME to provide content type security as specified in RFC 1847 is Pretty Good Privacy (PGP). When a PGP is installed, a "public key" and a "private key" are generated. A public key is sent to the PGP, who publishes the public key, and stores it in a PGP key server that can be accessed by anyone who wants to send e-mail. The sender encrypts the e-mail using the public key. The receiver uses his private key to decrypt, ensuring that only the person having a valid private key can decrypt and read the message.

Secure/Multipurpose Internet Mail Extension (S/MIME) is an advanced version of MIME that enables a user to send and receive secure MIME content, over the Internet. MIME protocol provides the following cryptography security services -

Authentication

- Ensuring Message Integrity
- Non repudiation of origin through digital signature

- Providing privacy and data security through encryption

An important benefit of S/MIME is that its use is not restricted only to mail, but it can be used with any mechanism that transports MIME data such as HTTP. Since S/MIME has object-based features, it allows the transportation of secure messages over mixed transport systems. S/MIME also extends its security features to messages that are sent by fax over the Internet through encryption.

[1] STD 11 (RFC 822) Standard for the format of ARPA Internet Text Messages. RFC stands for Request for Comments. RFC is maintained by the Internet Society and contains documents on the Internet Protocol Suite as designed by the Internet Engineering Task Force.

[2] RFC 1847: Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted

[3] RFC 1848: MIME Object Security Services

[4] RFC 1421: Privacy Enhancement for Internet Electronic Mail, Part 1 - Message Encryption and Authentication Procedures

[5] RFC 1422: Privacy Enhancement for Internet Electronic Mail Part 2 - Certificate Key based Management

[6] RFC 1423: Privacy Enhancement for Internet Electronic Mail Part 3 - Algorithms, Modes and Identifiers

Answer: [b] CS/MIME (Secure/Multipurpose Internet Mail Extension)

Explanation: S/MIME is not only restricted to mail, it can transfer secure messages through other mechanisms that transports MIME data.

Module:4 Reference No:M4043

Question: Which one of the following risks is unique to wireless communication?

- [a] Lack of physical security
- [b] Denial of service
- [c] Spoofing attack
- [d] Disabling of network.

Module 4- Security issues in wireless communication

1. Security issues in wireless communication often depend on the type of information that is sent. Bluetooth transmits data in two ways: It acts as a cable replacement for short distances. Since the range is limited, it usually carries a single flow of information. For example, data that is received by a single voice channel or a single printer.
2. It acts as a network access link. In this case, there is multiple flow of information, which may overlap with the single flow of information. In case of a security breach, information (which is not meant for wireless connection) available on the entire corporate or home network is affected. Thus, while in the first case only single information flow is affected, here the entire network may be affected.

Threats faced by a wireless network

1. **Denial of Service:** In this case, an authorised user is denied access to a device or network.
2. **Spoofing attack:** Here, an unauthorised person may place his own device in place of the device of a valid user, and seek to gain access into the network.
3. **Disabling the network :** In extreme cases of a DOS (Denial of Service) attack, an intruder may disable the entire network, and render it useless.

Limitations of wireless links

Shortcomings in wireless communication links expose the network to security breaches, such as -

- Wireless links cannot have physical security, as the transmission can be intercepted from anywhere.
- It is difficult to track down an intruder, as there are no wire connections.
- It is difficult to differentiate between a real intrusion and one that is unintentional.
- Wireless links are not of good quality, hence it is important to exercise caution with regard to link errors.

Another major area, which requires attention, is information leakage through insiders. Accessing confidential information through an insider seems easier than taking a risk and incurring heavy costs on accessing the network. This problem can be resolved in two ways -

By establishing security procedures such that information leak from one person will not disrupt the functioning of the entire network.

By ensuring that a security breach can be easily detected. The greater the chances of getting caught, the more reluctant the person will be to divulge sensitive information. The price to be paid for revealing information is more, and this often deters intruders from attempting to breach security.

"All that matters is the weakest link". In wireless communication, it is essential to prevent the air link from becoming a weak link.

Answer: [a] Lack of physical security

Module:4

Reference No:M4044

Question: Which one of the following is a feature of Bluetooth security provisions?

- [a] Device authentication
- [b] Compulsory pairing and bonding between two devices
- [c] Constant authentication of device and user
- [d] Use of a single key for device authentication and link encryption

Module 4- Security provisions for Bluetooth

Active provisions for Bluetooth security include device authentication and link encryption.

Device Authentication

A bluetooth connection is established based on the addresses of physical devices, specified by manufacturers. While establishing a connection, the devices 'challenge' and 'respond' as a secret key is shared between the responder and authenticator. Challenge/response uses an algorithm called SAFER+, which helps in creating the secret key that ensures authentication among various physical devices that share the connection. This algorithm uses a 128-bit key, which is considered safe by the cryptography community. It helps in identifying different physical devices that are a part of the set-up.

In case an intruder tries to access information using a different physical device, authentication fails. It also prolongs period and 'key guessing' becomes tedious.

Link encryption

After devices are connected and authenticated, the next step is to encrypt the links. This is possible, only when the devices share a common secret key. Link encryption can be done using a key between 8 -128 bits, depending on the legal requirements of various countries. The encryption key is created during the authentication process; it is not the same as authentication key (which is always 128 bits).

Bluetooth provides flexibility for different encryption keys. Usually encryption keys are different for every session. However, while sharing broadcast data among multiple devices, it becomes imperative to share the same key. Thus, in this case, the encryption key is based on the 'link-key', which may be of two types depending on the usage -

- **Authenticating Devices** - The Bonded Link key -When there is no user interface, a process called 'bonding' establishes a semi-transparent link key, which can be used for an indefinite period. Bonding is done by bringing the two devices within the range, and initiating one of the devices. Devices get connected and authenticate each other, to create an encryption key that can be used in future. The next time two devices are connected, they use this link key to connect to each other, and develop another encryption key for the new session. Thus, for every session a new encryption key is created even though the devices are bonded through the link key.
- **Authenticating Users & Devices** - The Dynamic Link Key - In some cases, it is essential to authenticate not only the device, but also the user. In case a device is stolen or lost, it safeguards against unauthorised access. To ensure security, the user is asked to enter the PIN (Personal Identification Number) every time he wants to connect to the device. In case, the PIN entered is correct, a dynamic encryption key is formed with the help of the PIN. In case, the PIN entered is not correct, the link is denied.

Answer: [a] Device authentication

Module:4 Reference No:M4045

Question: Which of the following is not a part of digital certificates -

- [a] Digital signature of the issuer
- [b] Public key of the subject
- [c] Private key of the subject
- [d] Serial number

Module 4- Digital Certificates Digital certificates

In PKI (Public Key Infrastructure), after a certification authority creates an identity for the user, the next step is to create a document to verify its validity. A digital certificate is the electronic form of such a document. For instance, A sends information to B. B is sure that the message has come from A because B has decrypted the message, using A's public key. Only the corresponding private key could have encrypted the message, thus it is believed that the message has come from A. However, somebody has to certify that A is the owner of the private key. The digital certificate does so, and is given by a third party trusted by B. The certificate contains information, which satisfies the counter party about the identity, especially in the case of sensitive electronic transactions.

- Information contained within a digital certificate includes the following -
- Subject - It refers to the name of the individual/entity identified by the certificate-name@organisation.com
- Public key -It corresponds to the individual's private key.
- Issuer -It is the Certificate Authority (CA) that issues the certificate.
- Serial number - It is a unique number which differentiates two certificates that may have similar or substantially similar amount of information.
- Validity -The period for which the certificate can be used is specified.
- Key/certificate usage - The individual's private/public key pair can be used for a variety of purposes as defined here.

- Digital signature -This is the electronic signature of the issuer generated by his private key. It certifies the individual's identity.

Types of certificates

Apart from information about the identity of the certificate owner, the digital certificate also contains attributes and applications for which it can be used.

- Certificates used to identify the sender of the e-mail will have his e-mail address mentioned. This helps to verify the identity of the sender by comparing the e-mail address listed in the certificate with the e-mail address contained in the mail message.
- In case of Virtual Private Networks (VPNs) it is also important to authenticate the identity of the communicating machine. Hence, the identity mentioned in the certificate will be the TCP/IP network address of different machines connected in VPNs.

Security aspects

A digital certificate is a public structure, which contains information stated above that can be accessed publicly. Widespread access to certificates through the public structure reduces the distribution problem but may reveal confidential information. Before finalising the certificate infrastructure/policy, the scope of information that is to be provided must be carefully considered. For instance, the policy should decide whether information such as home address and social security number will be included in the certificate.

Certificates are both self-protected and secure structures, i.e. in case anybody tries to modify information or if an unauthorised person tries to use the certificate, the application software will issue a warning.

Answer: [c] Private Key

Module:4 Reference No:M4046

Question: Which one of these options is incorrect? An IPSec is an extension of IP and -

- [a] Requires no encryption
- [b] Ensures message integrity
- [c] Implements WAN and LAN security measures
- [d] Ensures data confidentiality

Module 4- Internet Protocol SecurityUsing IPSec to Secure Networks

IPSec (Internet Protocol Security) defined by the Internet Engineering Task Force (IETF) is a set of security extensions designed to enable access control, data confidentiality and protection against message modification and replay. It is an enhanced security form of standard Internet Protocol (IP). Internet Protocol is a network layer protocol, which is embedded in almost every network device today. IPSec can be used to protect IP packets from modification and unauthorised access, protecting WAN and LAN traffic.

IPSec consists of two Internet Protocol extensions -

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

These extensions help in establishing a secure network. Access to the network is controlled by a key management control called Internet Key Exchange (IKE). IPSec and IKE jointly ensure that IP packets are exchanged between authorised users in a secured way. IPSec ensures following -

Message Integrity - IPSec ensures that the packet sent from a sender to a receiver is not modified during transit. It also establishes the identity of the sender to receiver. IPSec does not allow any unauthorised personnel to access information, or to modify the message and resend it to the recipient. It also prevents an intruder from performing bogus transactions with the server. For instance, a hacker can repeat an accounting system transaction to transfer the payment to his own bank account. IPSec prevents such actions and ensures that message integrity is maintained.

This is made possible through the use of digital signatures by AH and ESP. They take the packet or part of the packet, generate a message hash, and encrypt the hash with the secret key known only to the sender and the receiver.

Data Confidentiality - ESP encrypts a part or the entire packet with a symmetric algorithm. The key to decrypt is known only to the sender and the receiver. This helps in keeping the data confidential. This helps to transport sensitive corporate data such as payrolls, customer list and the like on the intranet and the extranet, where only the intended person/s will be able to receive and read the information in the packet.

WAN and LAN security measures

When information flows through a WAN, the addresses of source and destination will enable an outsider to take a guess at the information that's within, even though he may not be able to read the information. For instance, if information is being transmitted from company A to company B, then a person may assume that mergers and acquisition activity is going on. He may seek to exploit this information that he supposedly has to make illegal profits. Addresses in some cases also reveal the network topology and may help an outsider to hack systems. In order to secure the addresses, IPSec can be used in a tunnel mode. The entire original header and the payload are hidden inside an IP packet "envelop". The tunnel mode is usually utilised by security gateways like routers, firewalls and other devices that send packets on behalf of other systems. While we can use tunnel mode for WAN, in the LAN environment, a transport mode can still be used. In transport mode, only the payload is hidden. This helps in reducing processing overheads and overall packet length.

Answer: [a] Requires no encryption

Module:4 Reference No:M4047

Question: A Packet Filter Firewall Ruleset ideally should:

- [a] Forward any packet with a source address of the local network to the external network
- [b] Allow all access from the external network to the firewall system itself
- [c] Expressly allow everything unless specifically prohibited
- [d] Expressly prohibit everything unless specifically allowed

Module 4- Firewalls

Packet filtering firewalls use routers with packet filtering rules to grant or deny access based on source address, destination address and port. They offer minimum security, but are inexpensive to implement and are an appropriate choice for a low risk environment. Packet filters use rules specified in tables configured by administrators. These tables list source and destination addresses that are acceptable and sources and

destinations that are to be blocked. For packets coming or going to other machines, default rules can be configured to handle the requests.

There are two broad types of rules concerning firewalls:

- Permit any service unless it is specifically denied.
- Deny any service unless it is specifically permitted.

A firewall implementing the first policy allows all services by default, but denies those services that the access policy has disallowed. This policy is not very secure since there might be some services which must be blocked, but are overlooked. The reason this policy is not secure is that certain Operating Systems like Unix start all services such as Telnet when booted. Also, there are nearly 65536 ports on which services may be run. It is easy for an administrator to forget blocking certain ports and then it becomes easy for a hacker to use that service to get into the network.

A firewall that implements the second policy denies all services except those that the service access policy allows. The second policy is stronger and safer, but is more difficult to implement and may impact some users more when some services need are not turned on by the access rules.

Ideally, both the policies must provide for logging of requests in all cases. Further this logging must be replicated in a more secure location simultaneously, as hackers have been known to alter the logs to hide their activities. After all logs are replicated to a central server, use of log analyzer tools can help in finding out patterns in requests. If a pattern is found and the requests come from one IP address frequently, it may be safe to assume that some is attempting to hack into the network.

Before building the rule set, there is an important point to be noted: rule order. The order in which rules are entered in the rule set is critical. Having the same rules, but placing them in a different order, can radically alter how the firewall works. Many firewalls (such as SunScreen EFS, Cisco IOS, and FW-1) work by inspecting packets in a sequential manner. When the firewall receives a packet, it compares it against the first rule, then the second, then the third, etc. When it finds a rule that matches, it stops checking and applies that rule. If the packet goes through each rule without finding a match, then that packet is denied. It is critical to understand that the first rule that matches is applied to the packet, not the rule that best matches. Based on this, it is more secure to keep the more specific rules first, the more general rules last. This prevents a general rule being matched before hitting a more specific rule. This helps protect the firewall from misconfigurations.

Answer: [d] Expressly prohibit everything unless specifically allowed.

Module:4 Reference No:M40048

Question: A firewall cannot do one of the following:

- [a] Protect against unauthorised logins from external networks
- [b] Protect the network against users connecting to the Internet by dialling to their ISP using their office telephone and a modem
- [c] Appear transparent to their users
- [d] Log traffic to and from the local network

Module 4- Firewalls

A firewall can provide the following features:

- Each packet of information contains the address of both the sender and the receiver. So a firewall can be configured to block all packets from a particular sender or allow only packets from specific senders. While it's a good policy, the problem with this approach is that the firewall has to limit most access or know the addresses of hackers in advance. This is impossible since most hackers use ISP accounts, which may be taken as trusted domains.

One solution is to look at the ACK bit in the packet header. If a user requests a page from Microsoft, packets will come to the network with a Microsoft return address and the ACK bit set to "Yes". This means that the user has requested these packets and hence they are allowed through the firewall.

In a typical computer attack, hackers send packets to the network without some user requesting them. This results in the ACK bit set to "NO". The return address is not familiar and hence a firewall could refuse to let these packets proceed into the network.

- Firewalls are typically transparent to internal network users (while they request external pages from inside the network). For traffic from outside coming into the local network the firewalls are configured to be non-transparent in the sense that all packets will be inspected before being allowed inside.
- Logging is another mechanism that allows proper examination of an attack in case the Web Server or the internal network has been attacked. Such examination is called forensics and is done to investigate the mechanism of attack and protection in the future against it.
- The main function of a firewall is to centralise access control. A firewall serves as the gatekeeper between the Internet and the trusted internal networks. If outsiders can access the internal network without going through the firewall, there is no point in having the firewall in the first place.

For example, if a travelling manager has a modem connected to his office PC that he can dial into while travelling and that PC is also part of the protected internal network, then an attacker who can dial into that PC can use it to circumvent the firewall. Similarly, if a user has a dial-up Internet account with a commercial ISP and sometimes connects to the Internet from that account, an unsecured connection is being opened to the Internet that goes right around the security mechanisms.

To summarise, a properly configured firewall can provide several types of protection:

- They can block unwanted traffic.
- They can direct incoming traffic to more trustworthy internal systems
- They hide vulnerable systems
- They can log traffic to and fro from the private network.
- They can hide user information like system names, network topology and network addresses from the Internet.
- They can provide more robust authentication than standard applications might be able to provide.

As with any tool, there are compromises between convenience and security. A more secure firewall might slow things down when traffic is high, since each packet has to be inspected before being passed. Proper and dynamic configuration as and when necessary must be done for smooth functioning of the firewall system.

Answer: [b] Protect the network against users connecting to the Internet by dialing to their ISP using their office telephone and a modem

Module:4 Reference No:M4049

Question: Which of this is not an internal access control mechanism?

- [a] Sound an audible alarm.
- [b] Block all further traffic, irrespective of whether it is authorised access or not
- [c] Correlate events, as the firewall is the gatekeeper to the entire network.
- [d] Reroute all traffic through a back up firewall.

Module 4- Firewalls

A security incident is defined as an activity in which an attempt to access the protected network takes place. This may not be a cause for concern if an employee mistakenly types a wrong password to access the system, causing an alarm. However, it does become a worrying situation when someone does get into the network and acquires the ability to destroy data integrity.

These two incidents are on the extreme sides of the scale, but often, the incident will simply be attempts by unauthorised people to get access to the system using known bugs or exploitable holes of the network, operating system and other software.

The response of the organisation to security incidents must be properly defined and implemented in the Security Policy Document. Further, all possible security threats must be decided on a level and there must be thorough investigation of intrusion attempts after a pre-defined level has been reached.

Firewall is the entry door to the organisation's network and is the basis for Event correlation. It is the analogous concept of check posts in the real world, where the single point of access is blocked, and every entity is inspected as to its authorisation and authentication before being allowed in. Hence, all Intrusion Detection Systems (IDS) must be synchronised in time so that reconstruction of security breaches can be made. Network Time Protocol (NTP) is the most commonly used protocol to achieve time synchronisation.

The following steps can help in recovering from a security threat.

- Document the incident and related matters using standard forms, since they may be used as evidence in a court of law. Answer the questions - Who, What, When, Where, How and Why
- Notify the incident to the security coordinator and managers. Record carefully what each person says. This evidence may or may not be admissible, but can provide much needed clarity to the direction of investigation.
- Restrict the details to few people so that undue advantage is not taken of. The cause of trouble may be an employee and if counter measures taken are revealed, then he may take steps to erase evidence before it is found.
- Assume that all computers connected to the compromised system or network are also breached. Use other means of communication such as telephones and faxes. Do not send information about the incident by electronic mail as the information may be intercepted by the attacker and may worsen the situation. If e-mail must be used, strong e-mail encryption software such as PGP (Pretty Good Privacy) may be used.
- Take necessary steps to keep the problem from getting out of hand. This can be done by removing the system from the network, though the management might favour keeping the connections open in an effort to catch the intruder.
- Create a mirror of the compromised systems. This can help in analysing the intrusion method at a later date. If possible, make a binary or bit-by-bit backup. Security or Computer Forensic experts can find this data valuable in reconstructing the entire attack step-by-step.
- Take appropriate measures to improve the defences of the systems and plug the holes in the operating system and other software.

- After checking that the backups (not the backups of the compromised systems taken earlier, but the regular backups that are done regularly in all organisations) are not compromised, restore and monitor the systems closely to determine whether it can resume its tasks.
- Create a systematic report of the intrusion and incorporate into the security policy of the organisation. Educate information security personnel on how to monitor and detect intrusions in the future.

Answer: [c] Correlate events, as the firewall is the gatekeeper to the entire network.

Module:4 Reference No:M4050

Question: What does NAT mean in the context of Firewalls and Security?

- [a] NAT (Network Attack Terminator) - program used by Administrator to hunt, destroy malicious packet
- [b] NAT, Network Administration Terminal, refers to the computer on which an application-proxy firewall is installed and allows administrators to inspect packets coming in from outside the network
- [c] NAT, Network Address Translation, hides the addressing scheme of its internal servers, workstations and other machines
- [d] The primary function of NAT, Network Authentication tool, is to identify authorised users and allow them to access to the local network even when they are connecting from a remote location.

Module 4- Firewalls: Network Address Translation

For a computer to communicate with other computers and Web Servers on the Internet, it must have an IP address which is 32 bits long. Theoretically, there are 2³² unique addresses (i.e., 4,294,967,296), was thought to be enough for decades. The actual number of addresses is smaller because some addresses are set aside for multicasting, testing or other special uses.

With the explosion of the Internet and the increase in home and business networks, the number of available IP addresses is simply not enough. The obvious solution is to redesign the addressing scheme to allow more addresses. This is being developed as IP v6, but will take several years to implement because it requires modification of the entire existing infrastructure of the Internet.

This is where Network Address Translation (NAT) comes into the picture. NAT translates IP addresses on the internal network to one public address that is sent out on the Internet. A company can have a single IP address and all internal hosts can be assigned addresses in the range of private IP addresses.

For example, if the registered address assigned to a company is 180.80.1.6, then the hosts can have addresses ranging from 180.80.0.0 to 180.80.255.255. When those internal hosts send a message to an outside network, the outsider will still receive the message from 180.80.1.6 only. It also helps in tracking which internal client has made the request for which outside Server. In short, unregistered IP addresses are replaced with registered IP addresses while communicating with external networks. NAT hides the addressing scheme of its internal servers, workstations etc.

NAT can map internal IP addresses to a single IP address in three ways:

- **Static NAT**
The static address translation entails that each internal IP address is always tied to the same NAT IP address every time a request is made. A static table is created where the original IP address is mapped to the NAT IP address. The drawback is that every internal address must have a registered IP address for static NAT to work.

- **Pooled NAT**

In a pooled NAT, the internal hosts are mapped to a pool of external IP addresses. Unlike Static NAT, the IP addresses are assigned dynamically, but the same one-to-one mapping is maintained.

- **Port Address Translation (PAT)**

In PAT, the internal connections are mapped to a single registered IP address, but the port number is different and the TCP port number to be used is selected by the NAT device.

NAT and Security

NAT only resolves the conflict in IP addresses, but is not a security device. It still has to be combined with firewalls, routers etc for security purposes.

A security concern arises every time there is a change in the IP addressing. For example, firewalls use IP addressing, along with TCP port numbers, destination addresses and sometimes other information in the IP header, to decide whether or not to block traffic. Depending on the place of the NAT device, the firewall ruleset may have to be changed, since NAT changes the source or destination addresses, depending on direction.

Another drawback is that when the pool of IP addresses has been used up, new requests for connections will be refused until existing connections are terminated.

Although NAT offers a variety of benefits, such as removing the need to renumber your network, reducing costs of ISP accounts and providing better load-balancing, NAT's potential threat to some management and security functions that some caution is necessary before implementation.

Answer: [c] NAT, Network Address Translation, hides the addressing scheme of its internal servers, workstations and other machines.

Module:4 Reference No:M4052

Question: The following device is used to connect one type of IEEE 802.x LAN to another.

[a] Router

[b] Repeater

[c] Bridge

[d] No device is necessary. They are designed to be compatible with one another and are hence grouped under 802 series.

Module 4- LAN

Many organisations, universities and institutions are geographically spread over several buildings and also over cities. Since the requirements of each department may be different, they end up choosing a different LAN standard. Alternatively it may be necessary to split a single LAN into multiple ones to reduce the traffic on the network. Many such reasons can be given for the existence of multiple LANs within the same organisation. Further, numerous protocols exist in every layer.

There must be some way to connect all of these in a single network. There must some interface which can overcome these limitations to enable different networks to communicate effectively.

The devices used for interconnecting networks have different names according to the layer in which they operate as detailed below.

1. **Repeaters (Layer 1)**

Repeaters are the interface devices at the physical layer. When signals travel long distances, they become weak and the presence of noise also adds to the distortion of the signal. Repeaters are used just to amplify or regenerate the weak signals.

2. **Bridges (Layer 2)**

Repeaters just copy the bits as they arrive, but bridges are 'store and forward' devices. A bridge accepts an entire frame and passes it to the data link layer where it is checked for transmission errors. Then the frame is sent down to the physical layer for forwarding on a different network. Bridges do not examine the network layer header and can thus copy IP, IPX and OSI packets equally well.

Routers (Layer 3)

Routers are similar to bridges, but the difference is that routers operate in the network layer and hence can differentiate between different protocols, unlike bridges which cannot do so.

1. **Gateways (Layer 4 and above)**

Gateways in the transport layer are called transport gateways and are responsible for maintaining connections between computers. Application gateways function at the layers above this and connect two parts of an application. For example, mail gateways are used to send e-mail from one mail server to another.

IEEE LAN protocols operate in second layer (Data Link Layer) and are not directly compatible with each other. Hence the process of converting one of the LAN protocols to another is done by the devices which operate at this layer. It is not easy to build such a device, since each of the LAN standards use a variety of schemes in terms of speed, physical media, signalling techniques, timers and voltage levels.

With the three basic LAN standards, there are nine combinations of LAN-LAN interconnections. There are no technical barriers for the incompatibility of these standards, but were deliberately kept so due to political purposes.

There are many problems that arise when a data frame in one LAN must be passed onto another. For example, the frame formats of the three primary LAN standards are different in length and the fields. This causes a serious problem when a LAN with a smaller frame length is between two LANs with bigger frame lengths. In this situation, the frame on reaching the intermediate LAN is simply discarded. This is not because of lack of a solution, but because the 802 standard does not provide this feature.

A transparent bridge or spanning tree bridge has been developed which can be used to connect any type of the IEEE LANs to another. Source routing bridges are used by token ring LANs to connect to other LANs. The difference between them is that source routing bridges support connection-oriented networking while transparent bridges do not support it.

Answer: [c] Bridge.

Module:4 Reference No:M4053

Question: The CSMA/CD Protocol is useful in

- [a] Correcting Collisions
- [b] Preventing Collisions
- [c] Eliminating Collisions
- [d] Detecting Collisions.

Module 4- 802.3:Ethernet

CSMA and CD

When many devices are connected through a single line, all devices would try to communicate with each other. In the process, there would be signal overlap and most of the signals would be destroyed. Such overlaps are called collisions. There is a need in LANs to:

1. Coordinate traffic.
2. Minimise number of collisions.
3. Maximise number of frames.

This is done by Carrier Sense Multiple Access (CSMA) protocols.

Carrier Sense is the ability of a station to tell if the channel (transmitting medium) is in use before trying to use it. This is done by first listening for traffic. If, after sensing for a voltage, the workstation finds the line to be idle, then it transmits. If the channel is busy, no station will attempt to use it until the channel becomes idle.

If a station does not have Carrier Sense, then it does not know whether the channel is being used by some other station or not. A station having data to send simply transmits data and only after transmission, can it determine if no collisions have taken place and the transmission has been successful.

The channel throughput is defined as the ratio of successful transmissions to the total number of transmission attempts. This throughput can be improved further if stations with CSMA can also abort their transmissions if they detect a collision. Instead of continuing transmission, where the frames have been destroyed anyway, the stations must abort their transmissions. After listening for some time, the message can again be transmitted. This saves time and bandwidth and also frees the channel faster. This feature of detecting collisions is called Collision Detection (CD) is widely used in conjunction with CSMA and called CSMA/CD.

CSMA/CD facilitates transmission by a single device at a time. This puts a limitation on the number of devices that can be connected to the channel. Also, the length of the cable limits this number. When the electrical signals travel through the cable, it is prone to interference from neighbouring stations and also they are weakened as they travel. This factor has to be kept in mind when implementing Ethernet protocol.

The physical layer is of more importance in Ethernet than in other standards, since the standard provides for different speeds on various media. Five types of cabling are used as detailed below.

1. 10Base5 or thick Ethernet uses a thick coaxial cable and has a maximum segment length of 500 m. The maximum segment length is the length of the cable for which the signal does not get degraded.
2. 10Base2 or thin Ethernet, in which a thin coaxial cable is used and where the maximum segment length is 200 m.
3. 10Base-T uses twisted pair cables, which are the common telephone wires and hence are inexpensive. The segment length is only 100 m, but the cost of using repeaters to increase signal strength is offset by the decreased cable cost.
4. 10Base-F uses fibre optic cables, which are more expensive, but provide high immunity from noise. Fibre optic cables can be used for 2 km without using repeaters to boost the signal strength.

In the above, 10 stands for the speed of the LAN in Mega bits per second (Mbps) and Base represents the signalling scheme used (Base band).

Frames in Ethernet use 6-byte addresses to identify source and destination. A frame can be sent to one individual computer, a group of stations or to all stations on the network. Sending to a group of stations is called multicasting and sending to all stations on the network by putting all 1s in the destination address field is called broadcasting.

Answer: [d] Detecting Collisions.

Module:4

Reference No:M4054

Question: In 802.5 Token Ring LAN, when a data frame is in circulation, where is the token?

- [a] At the receiving station
- [b] At the sending station
- [c] With a special station called Monitor station
- [d] Both the sending and receiving stations have a copy of the tokens.

Module 4- 802.5:Token Ring

IBM developed the Token Ring standard in the 1970s for its primary local-area network (LAN) technology. The IEEE 802.5 specification was modeled after the IBM Token Ring. A ring actually is a collection of ring interfaces connected by point-to-point lines. Each bit of data arriving at the interface is copied into a buffer and then copied onto the ring again. This copying step introduces a 1-bit delay at each interface.

Token-passing networks move a small frame, called a token, around the network. The token is a special bit pattern that circulates through the ring when all computers on the network are idle.

If a station does have information to transmit, it must seize the token. The station must then alter 1 bit in the 3-byte token, which turns the token into a start-of-frame sequence. It then appends the information that it wants to transmit, and send this information to the next station on the ring. Each station sees the address on the token and if the message is meant for the station, it copies the message, adds a receipt and sends it again to the ring. When the frame reaches the sending station, the receipt is read and the token is replaced.

While the information frame is circling the ring, no token is on the network, which means that other stations wanting to transmit must wait. Since only one token is present in the network and only the station that has the token transmits, there are no collisions, which solves the channel allocation problem. Therefore it may be considered that the sending station has captured the token before transmission. Since the entire data frame does not appear on the ring completely at any instant, there is no limit on the size of the frames.

Token ring connectivity requires three separate physical entities: a Multistation Access Unit (MAU), a token ring lobe cable, and a token ring adapter card. A Multistation Access Unit (MAU or MSAU) is a hub-like device that connects to all token ring stations. Although the token ring stations are attached to the MAU in a physical star configuration, a true ring is maintained inside the MAU.

The advantages of using a token ring are:

1. They have been around for many years and have long been used for both local and wide area networks.
2. The ring is not really a broadcast medium, but a collection of point-to-point links that form a circle.

3. Point-to-Point links use a well known and field proven technology and can run on a variety of physical media including twisted pair, coaxial cable or fibre optics.
4. Ring engineering is a digital technology while some other standards like Ethernet have a substantial analog component. The analog component must be converted into digital signals and vice versa for transmission along networks that use other standards. Such conversions involve the use of expensive devices and cause weakening or even loss of signals.
5. The ring is fair, in that it does not discriminate against stations that are placed inconveniently in a geographical sense.

The main disadvantage is that the token ring favours the higher priority frames over the lower priority frames. The protocol has elaborate rules on handling priority frames and sees to it that lower priority frames also get transmitted. Still, a higher priority frame has a better chance of getting through, than a low priority one which can make a busy network look standstill for a low priority user.

Answer: [b] At the sending station.

Module:4

Reference No:M4055

Question: In a DeMilitarized Zone (DMZ) Network

- [a] There are no firewalls and hence the network is called DeMilitarized
- [b] There is one firewall before the boundary router connected to the Internet and one firewall after the router, but before the external Web Server
- [c] Both the firewalls lie between the external Web Server and the internal (local) Server
- [d] One firewall lies between the router and the external Web Server and another firewall is placed between this Server and the local Server.

Module 4- DMZ

A DMZ network is often used when organisations have an intranet or local network and publicly accessible servers such as Web Servers in the same environment.

If the Web Server is compromised, the company loses only publicly available data and probably losses in transaction. But if the compromised Web Server is in turn used to get into the internal network, the consequences could be disastrous for the organisation.

To maximise protection of the local network from external attacks, the public server is placed in the first DMZ network and the internal server is placed in the second DMZ network as shown below.

The DMZ is used to separate a private network inside an organisation from services that are offered across the Internet. Firewalls and Bastion hosts are used to separate the DMZ from the rest of the network. The DMZ usually contains Web Servers, Internet e-mail servers and Domain Name Service (DNS) servers. These servers are considered expendable and can be easily restored from backups.

The boundary router filters packets according to the rules specified and provides a certain amount of protection for the servers. The external or first firewall is used to control access to the external Web

Servers. The second firewall guards against attacks on the internal servers and the network in case the external server is compromised.

Answer: [d] One firewall lies between the router and the external Web Server and another firewall is placed between this Server and the local Server.

Explanation: Option d is therefore the correct answer. Answer "b" is wrong since a firewall is never installed before the router and answer "c" is wrong because a firewall is needed to prevent unauthorised access to the external Web Server.

Module:4

Reference No:M4056

Question: Which of the following is true in relation to the "Frame Relay"?

- [a] A physical frame relay port will have a single virtual circuit
- [b] It is used to send analog information such as voice and data
- [c] It uses two OSI protocol layers as against three used in X.25
- [d] Using frame relay limits the type of resources that can be connected to a network.

Module 4- Frame relay

Frame Relay is a data transmission technique used to send digital information such as voice, and data over a LAN or WAN. It is an efficient technique to transmit information in a faster and cost effective manner from a single port or node to multiple destinations. When various applications of different speeds and bandwidth are transmitted in a network, it is termed as bursty traffic. Frame relay is more suitable for such applications. The frame relay protocol resides in the physical and datalink layers of the OSI reference model (OSI is the international standard that defines an open systems connection by standardizing the interface for each layer; this assures the compatibility of multivendor hardware and software systems). It uses packet switching technology so that the end users can share the network medium and bandwidth dynamically. Protocols ensure that the data at the receiving end is the same as the one sent by the sender. Data is grouped in frames or packets and transmitted over a network with an identifier or address. Frame Relay switches packets end to end much faster, but there is no guarantee of data integrity at all.

How does it work?

Frame relay uses the concept of

1. Permanent virtual circuits (PVCs)
2. Committed Information Rate (CIR).

Permanent virtual circuits are those used to establish dedicated fulltime connection between DTE (Data Terminal Equipments) devices in a frame relay network. PVCs operate in either Data transfer or Idle operational state. Data is transmitted between the DTE devices over the virtual circuit in data transfer state. Data transfer does not take place in idle state but connection is active. Connection is available fulltime without termination. Frame relay uses statistical multiplexing, where virtual circuits belonging to the same physical port share all the available bandwidth. This gives flexibility to the connection to use the bandwidth. Committed information rate is the contract with the carrier service provider that guarantees a communication rate (bandwidth) at a minimum speed all the time. Congestion management techniques are described in the frame relay standards. Standards-compliant congestion management is adapted whereby each end user device has guaranteed access to a defined amount of bandwidth in accordance with CIR. Frame relay uses only the bottom two OSI (open systems interconnection) protocol layers.

Frame relay devices

The networks adapting frame relay standards use two categories of devices.
Data terminal equipments (DTE)

Data circuit-terminating equipments (DCE)

Devices like routers, bridges, and personal computers located at the users network station that perform the function of terminating equipments are called as Data terminal equipments.

The device that is essential for the purpose of connectivity between the user and the endpoint owned by the carrier of the service is called as Data circuit-terminating equipments. Packet switches that transmit data in a network is a best example for DCE.

Frame relay implementation

Permanent virtual circuits (PVC) are those that form a virtual circuit between two users on a continuous basis. The circuit is dedicated to specific users. It is always in place without the need for connection establishment and connection termination. Star ology is commonly used for a frame relay implementation. Here a configuration consists of one large central office acting as a hub for a number of sub offices or satellite offices. Separate PVC connects the central office, or hub, to each sub office, but none of the satellite offices are connected to another satellite office. The central office performs central switching or routing function, to forward data sent from one satellite office to another one.

The full mesh architecture has separate PVC leading from each office to every other office. This has a drawback. The number of PVCs required grows rapidly as the number of offices increases. A partial mesh structure overcomes this limitation.

Answer: [c] It uses two OSI protocol layers as against three used in X.25.

The frame relay protocol resides in the physical and datalink layers of the OSI reference model.

This enables effective digital transfer of data through these layers instead of three in X.25 where the third layer caters to congestion control.

Module:4

Reference No:M4058

Question: WAN helps in

- [a] transferring data among resources in the same building
- [b] connecting different branches of an organisation within the city or in different cities
- [c] determining the number of connections in a network
- [d] routing the data to various networks

Module 4- Wide Area Networks

Wide Area Network can be defined as a network that facilitates information exchange, within or outside an organisation. It generally covers a large geographical area. It often spans across several cities in different countries, and uses communications circuits to connect intermediate nodes.. It can also be hooked up to the Internet, to connect to the world outside the organisation . The primary purpose of WAN is to provide fast, reliable and safe communications between two or more persons or nodes at a very low price and with low delays. WANs can be used use by large networks like train reservation networks, university networks, military networks and the like . WANs are generally built by Public Telecommunication Companies in each country. So they are developed in accordance with the strategies and politics of companies .

1. In India, WAN services are generally provided by companies like VSNL. The Basic WAN service was provided for long time through a Leased Line. A Leased Line is a direct connection between nodes in two places. An organisation, whose WAN is based on such design, has to connect each of its branch to as many lines as the number of branches.

This problem was solved by using packet switched WANs. The Packet Switched WAN transfers data between nodes in small packet, the and helps in sharing resources efficiently.

Constructing a WAN can be complicated for large organisations that have businesses in different places. So an organisation needs to plan well, before doing so . It must :

1. Define its requirements
2. Decide on the WAN service
3. Determine the best router

1. Define requirements

The organisation should identify its needs , after considering questions, such as

1. Where is the organisation doing its business?
2. Is it restricted to a single location or multiple locations, within the same country or in many countries.
Where are its present and future locations?
3. What kind of communication would the WAN have to handle, such as amount of traffic load, and the like

2. Deciding on services

The organisation must decide on the type of WAN service that would best suit the organisation. Various kinds of services include:

Dial-UP (ISDN and Analogue modem): This connection supports links to many sites, but the main drawback is that only two links can be established at any given point of time. They are generally cost effective.

Dedicated point to point (Leased Line): It provides more bandwidth and is reliable . But multiple sites cannot be connected with a single line, and a separate line is required for each link. Leased lines are expensive, and charges depend on bandwidth and the distance between which the data has to be transmitted.

Mesh Networks: Such networks connect many remote sites, using a single connection to the telephone company. The telephone company then routes the destination address according to the bandwidth. It is very flexible , and can easily add a new link.

Answer: [b] connecting different branches of an organisation within the city or in different cities.

Module:4

Reference No:M4059

Question: Path length, bandwidth, load are:

- [a] Routing metrics
- [b] Routing algorithms
- [c] Routing algorithms design type
- [d] Routing activities

Module 4- Router

A router can be defined as a sophisticated device that joins multiple networks together, by moving information across a network from a source to destination. It has the ability to filter or block the message at the network boundary. Routers work at the third layer of the OSI Reference Model.

Working

Routing primarily involves determining the best path and transferring the information over the network.

Path Determination: To determine the optimal path to the destination, routing algorithms use metrics (standards of measurement) such as path bandwidth, path length, reliability, delay, load and the like . Metrics generally differ, depending on the design of the routing algorithm. Routing algorithms initialise and maintain routing tables to aid the process of path determination. The tables also contain information (used by switching software) to select the best route. The router becomes aware of the optimal path through

destination/next hop associations. When a router receives an incoming packet, it checks the destination address, and attempts to associate this address with the next hop.

To communicate and maintain the routing table, routers transmit messages. For example, the routing update message consists of whole or a part of a routing table. A router can therefore create a detailed picture of the network topology, by analysing routing updates from all other routers.

Transferring Information: For transferring the information, routers use switching algorithms. The host router first determines where the packet information is to be sent i.e., the final physical address destination. It then sends the packet to the router's physical address 1 along with its logical address 2. If the router does not know how to forward, it drops the packet. If it knows, it changes the destination physical address (to the next hop) and transmits it. This process continues until the packet reaches the destination.

Design goals

Optimality: It refers to the capability of routing algorithms to select the best route, depending on the metrics and metric values.

Robustness and stability: Routers should be able to perform even in situations such as high load conditions, hardware failures and the like. Since routers reside at network junction points, a considerable amount of damage can be inflicted, if they fail.

Flexibility: The router should be flexible, and quickly adapt to a variety of network situations.

Rapid convergence: Routers should quickly calculate the optimal path in case of a network breakdown, and share and update the routing information. This is termed as convergence. A router with slow convergence may lead to routing loops or network outstages.

Notes:

1. Physical Address: It is the address, which is generally visible and has a description, or address. Every equipment connected to a network generally has a unique address. For example, computers connected to a network have Networks Interface Cards, which have physical address cards with Media Access Control (MAC) addresses.

2. Logical Address: A logical address describes the way in which the destination can be located. A computer connected to the Internet can be identified by an address, which is part of the TCP/IP network protocol. If connected through the corporate network, then the computer would have an address that follows Novell's IPX/SPX protocol.

Header: A header is a unit of information that precedes a data object. It may contain data pertaining to the creation of the file, its last update, the file size and the like

Bandwidth: It is the available traffic capacity of a link.

Load: The degree to which a network resource is busy.

Answer: [a] Routing metrics

Module:4

Reference No:M4060

Question: Which of the following options is true (with regard to SLIP)?

- [a] It includes a protocol identifier.
- [b] It allows communication with multi protocol computers.
- [c] It has no addressing scheme for routing purposes.
- [d] It is never used in a dial up connection.

Module 4- Serial Line Internet Protocol

Serial Line Internet Protocol (SLIP) is defined as a packet framing TCP/IP used for communication between two computers that are already configured to a set of protocol. SLIP defines the manner in which IP datagrams (packets of data) can be packaged and transmitted over serial data lines. For example, when the internet is accessed from an ISP with a SLIP connection, the ISP's server responds to the user's request through the Internet. It then forwards the requested Internet response back to the user. This protocol generally uses the dial up connection to connect to the Internet. It is therefore slower than multiplex lines. It is generally used in lines with speeds between 1200bps - 19.2kbps. It helps in connecting hosts and routers with another (common SLIP configurations: host-host, router-host, router-router).

Working

Even though it's very easy to implement, SLIP does not provide any addressing, packet type identification, error detection/correction or compression mechanisms.

The SLIP protocol defines two special characters: END (which is octal [1] 300 or decimal 192) and ESC (octal 333 or decimal 219). It sends data in the form of packets. Each packet is compared with the END and ESC characters. If the data has the same code as the END character, then a two-byte sequence of ESC and octal 334 (Decimal equivalent of 220) is sent instead. If the data type is equal to the ESC character, a two-byte sequence of ESC and octal 335(decimal equivalent of 221) is sent instead. An END character is appended, when the last byte in the packet is transmitted. It means the ESC is send irrespective of whether the data type is equal to END or ESC, followed by octal 334 or octal 335.The END is sent only at the end of transmission.

Drawbacks

In spite of its simplicity, SLIP has several drawbacks: Addressing: Before computers in a network can communicate, they first need to have a mechanism to identify each other. It provides no mechanism for hosts to communicate with an address.

Type Identification: It allows only one protocol to be run over a SLIP connection, as it does not have any type field. A computer connected to Serial Line will not be able to communicate with multi protocol computers.

Error Detection/Correction: Data in SLIP gets easily corrupted due to low line speed. Although, the data damaged can be easily detected, re transmitting it would take time.

Compression: Since dial up connection lines, are very slow data compression is not of much help.

[1] Octal Numbers: The Octal numbers are base 8 numbers. To convert octal to decimal, each number is multiplied with the number of 8,depending on the digit it is placed. E.g., 123 -> $1*8^2 + 2*8 + 3*1 = 73$

Answer: [c] It has no addressing scheme for routing purposes.

Question: Rapid Application Development is not appropriate when the development cycle involves

- [a] Reusability
- [b] Short time cycle
- [c] High technical risks
- [d] Small-integrated teams

Module 4- Rapid Application Development

The Rapid Application Development (RAD) is a software development model that emphasises on a short development cycle. It is a methodology that condenses analysis, building design, and tests a series of short, iterative development cycles. RAD is generally adopted when the project has a very short time limit (generally 60 -90 days) ,and has been clearly outlined.

Traditionally, a project would require planning, analysis, designing, testing and finally deployment. A RAD project is split into modules, and after completion of their task , individuals can move out. The RAD team is generally small and integrated, consisting of IT personnel managers, developers and end users. Members have to communicate with each other effectively, to complete projects successfully, without delays and costs over runs.

Such a process adopts a different iterative approach in executing projects. Unlike the traditional process, where projects have to undergo a series of steps; this process. condenses all the steps of planning, analysis, design and the like, into small repetitive steps. It makes the process accurate, auto-corrective and thereby effective. RAD promotes the use of object-oriented methods to reduce repetitive jobs and supports reusability.

The RAD process can be carried out in the following phases:

1. Initial analysis: First, the requirements are identified then the product is designed, and possible threats are assessed. This stage also considers methodologies that have to be used ,and gives an idea of the end product
2. Data analysis: Based on the requirements and the methodology, data is grouped into objects. Each attribute of the data object is identified, and relationships between them are also established.
3. Process modelling: Data objects change to allow information flow, necessary to implement a business function. The data object processing includes adding, deleting and modifying.
4. Development of modules: RAD generally uses fourth generation techniques. It makes use of existing components or creates new reusable components.
5. Testing and fielding: By the end of the final phase, individual components are tested a number of times. New components however are tested again, before the final product is ready for the market.

Inspite of all its cost and time saving features, RAD may not always be effective.

1. Team spirit: If the team does not work in cohesion, and there is a communication gap, it may lead to overruns in time and cost
2. Technological expertise: The team should be acquainted with the technology being used. Lack of experience not only delays the project, but may also result in errors.
3. Understanding the requirements: This is one of the biggest reasons for the failure of a project. Requirements should be carefully identified and clearly understood, and should not be changed frequently.

Answer: [c] High technical risks

Module:4

Reference No:M4062

Question: While auditing the logical access control, the auditor need not review:

- [a] Authorisation of dial in access
- [b] Audit trail
- [c] Bugs in the firewall
- [d] Password management

Module 4 - Firewall Audit I

A firewall protects the network from unauthorised users and other networks, and is an important logical access control to ensure system security. This is the first of the three part series on firewall audit. In this article, we have covered evaluation of the policy, as well as, review and testing of the ruleset and logical access control.

Objective:

- To assess whether the firewall policy has been formulated, implemented, reviewed and communicated to all users in the organisation.
- To assess whether objectives of installing the firewall are met.

To assess whether the firewall is functioning as perceived.

The auditor should have a clear understanding of the following details about firewalls:

- Segment diagrams
- Software
- Hardware
- Routers
- Version levels
- Host names
- IP addresses
- Connections
- Ruleset
- Specific policy and the like

Evaluation

The guidelines enumerated in the Firewall policy have to be checked from time to time. During the course of evaluation, the auditor:

- Assesses whether the policy is versioned and dated.
- Ascertains whether instructions are clear, without any ambiguity.
- Sets out acceptable as well as unacceptable conditions of use.
- Focuses on communication to the users.
- Reviews the policy at regular intervals.
- Defines the scope of the policy with regard to other internal and external networks.

- Identifies responsibilities of each person involved in the proper functioning of the firewall.
- Authorises a person to interpret and apply the policy to a particular situation
- Sets up an authority to allow temporary waiver of the policy under certain circumstances.
- Identifies network applications and other assets that must be protected.
- Identifies information (passing through the firewall) that should be monitored.
- Identifies course of action that should be taken in case of a security breach.
- Oversees review by a legal counsel to ensure consistency with requirements and limitation imposed externally (laws, regulations etc.).
- Checks for consistency with other organisational policies and accepted practices.

While review and testing the ruleset:

- Determine if a lockdown rule is in place at the beginning. The lockdown rule protects the firewall, and ensures that those that are enforced later, will not inadvertently compromise the firewall.
- Review the connections table for time out limits. The default time should be set to minimum thus reducing the opportunity for an outsider to enter the network.
- Scan secured network segments from other network segments. This ensures that the firewall is accepting only authorised traffic.
- Determine if there is a change control process in place, and the following information is included in the rule:
 - o Name of person modifying rule
 - o Date/ time of rule change
 - o Reason for rule change

To ensure logical access control:

- Obtain a technical diagram that shows the network and the firewall with IP addresses.
- Assess whether the firewall properly separates the DMZ (Demilitarized zone) from the inside network and the outside network.
- Determine whether there is a single point at which the Internet network can be separated from the Internet.
- Determine whether the password management feature is in place for the firewall. (Refer password policy)
- Identify monitoring and control procedures used on the Internet network to enforce security.
- Review supporting documents to ensure that procedures are being followed.
- Review the dial in access to the firewall server.
- Determine if the modems are automatically disconnected by the system after a specified length of time of inactivity.
- Identify the person authorised to provide dial in access.
- Determine if a mechanism exists to control dial in or remote access.
- Determine if an audit trail of dial in access exists, and whether the reports are reviewed.

Answer: [c] Bugs in the firewall

Question: While reviewing firewall logs, the auditor does not attempt to keep track of:

- [a] Unsuccessful logins
- [b] Successful logins
- [c] Unsuccessful logins
- [d] Unsuccessful logouts

Module 4 - Firewall Audit II

A firewall protects the network from unauthorised users and other networks, and is an important logical access control to ensure system security. This is the second article in the three part series on firewall audit. In this article, we have covered physical security, configuration, logs, communication channels, hardware, software and other devices relating to firewall audit.

Physical security:

- Determine if various components of the firewall (routers, firewall software) are physically secure, and accessible only to authorised persons. Print a list of users with access to the firewall, and crosscheck with the current employee list and access authorisations. Follow up on any discrepancies.
- Review periodically the list of authorised persons provided by the security administrator. Also, keep up- to- date with the most recent review, and supporting documents.
- Obtain schematic details of the lines connected to the applicable firewall hardware.
- Discuss with staff the purpose of each line, and document the same.
- Ensure that the physical security of information and assets the firewall is expected to control is in line with the physical security of the firewall.
- Ensure that all firewall components, including devices used to manage the firewall are within the same security perimeter.

Firewall configuration:

- Obtain a copy of documented procedures for requesting, authorising, implementing and testing changes to the firewall.
- Check whether the firewall components are the latest version and security patches are correct.
- Ensure that the security administrator keeps everyone posted about the latest bugs and exploits.
- Assess whether remote administration is possible, and controls are in place to support it.
- Determine whether changes to the configuration are tested in a safe environment.
- Determine whether there is a method to easily and quickly back out from changes being made.
- Determine whether there is an independent method of comparing two configurations to identify differences, and verify them with change control information.
- Identify the frequency with which such differences are carried out.
- Determine whether configuration management is automated and simple, to prevent errors from occurring.
- Ascertain if the firewall security is reassessed whenever the firewall is significantly changed.

Firewall logs:

- Determine whether the rejection and logging of activities are tracked. Review whether the following activities are logged:

- Login (unsuccessful and successful)
- Logout (successful)
- Use of privileged commands (unsuccessful and successful)
- Application and session initiation (unsuccessful and successful)
- Use of print command (unsuccessful and successful)
- Access control permission modification for users and security parameters (unsuccessful and successful)
- Unauthorised access attempts to files (unsuccessful)
- System startup and shutdown (unsuccessful and successful)
- All dropped packets, denied connections, and rejected attempts
- Error messages from routers, bastion host and proxying programs
- Determine whether logs are summarised.
- Determine whether logging results are monitored and follow up action is performed.
- Determine how the system and firewall logs are rotated to reduce the disk space problems. Rotation should be automatic.

Communication channels:

- Determine specifications of the communication line used to access the Internet.
- Assess the vulnerabilities of the communication line to unauthorised physical access.
- Determine the procedure of 'how' and 'to whom' phone numbers and circuit Ids are disseminated.

Firewall hardware, software and other devices:

- Determine the firewall hardware, software used - vendor, version number, etc.
- Determine who is responsible for their maintenance - the organisation or the vendor.
- Determine the procedure for obtaining and installing updates and patches.
- Determine controls that exist while upgrading.

Answer: [d] Unsuccessful logouts

Module:4

Reference No:M4064

Question: Access to the firewall should be limited to:

- [a] Firewall administrators
- [b] Top management
- [c] Security administrators
- [d] IT personnel

Module 4 - Firewall Audit III

A firewall offers protection from unauthorised users and networks. It is a very important logical access control to ensure system security. This is the third and concluding part of the series on firewall audit. In this article, we have covered firewall administration and testing, as well as, the business disruption aspect of firewall audit.

Firewall administration and testing includes:

- Clearly stating the authorised administrators of firewall along with their roles and responsibilities.

- Ascertaining the segregation of duties and its effectiveness in minimising the opportunities for security incidents and problems.
- Ensuring communication of the firewall policy to all personnel responsible for administration. Discussing with them their understanding of responsibilities that they have to discharge.
- Assessing whether access to administration of firewall should be limited to a small number of qualified personnel.
- Ensuring that the IP address is not the only means by which the administrator is authenticated.
- Determining whether the firewall can be administered even when it is active.
- Determining the impact of changes in the firewall when it is active. (eg. whether ftp will be denied while the ftp session is active)
- Determining the frequency at which firewall components are backed up.
- Ensuring that the backups are stored properly.
- Identifying services that are encrypted and the encryption scheme used.
- Ensuring that firewall files are cryptographically check summed, and these checksums are regularly verified.
- Ascertaining if the URL screening is being done by the firewall, and monitoring the way the list is administered and maintained.
- Determining whether anti-virus inspection is enabled, identifying the third party application that is used, and checking whether the software is working as perceived.
- Determining if the packets are screened for the presence of prohibited works. Also, scrutinising the way in which the list of words is administered and maintained.
- Ascertaining whether intrusion detection is automated.
- Monitoring threats for which the response has been automated.
- Determining whether the effectiveness of firewall is periodically tested from both sides.
- Reviewing the processes being used on the firewall when the audit is being conducted, and assessing whether they are appropriate.
- Determining the authentication strategy that is being used and its effectiveness.
- Determining whether adequate notice is given to anyone – internal or external who tries to exploit the firewall.
- Identifying standard and non-standard protocols that are used.
- Checking the effectiveness of dynamic or static address translations are used
- Determining the controls that exist to prevent denial of service attacks.
- Determining whether the incoming Java or ActiveX code is permitted, and the screening mechanism implemented for the purpose
- Determining whether controls exist to detect spoofing
- Assessing whether the implementation of firewall effectively enforces the approved security policy.

Business disruption or disaster includes:

- Determining whether a firewall plan is developed after assessing continuity requirements.
- Assessing whether acceptable time limits have been specified for reset and recovery.
- Ascertaining whether the plan is regularly tested.
- Reviewing the results of the most recent test, and determining whether the plan has been revised accordingly.

Answer: [a] Firewall administrators

Module:4

Reference No:M4065

Question: In the audit of LAN, inventory control helps the auditor in determining the effectiveness of IS operations. Which of the following is not correct with respect to inventory control?

- [a] Identify the person responsible for disposing obsolete or badly damaged LAN equipment
- [b] Inventory control is maintained of all LAN software
- [c] Hardware components are marked with identification number which cannot be erased or removed
- [d] Virus checking software is in use

Module 4 - Audit of LAN Part 3

The auditor cannot frame one common audit program for all the LAN audits he undertakes. He may prepare a standard program, which should be modified depending on the complexity of LAN and the operating environment.

This is the third part of eight part series on LAN audit. The second part of this series covers LAN standards and data integrity of LAN audit. This part covers inventory control and backup and recovery, contingency planning of LAN audit.

Inventory control: The management spends billions of dollars on computer hardware, software, communication and the like. Technology keeps changing bringing with it improvement in quality of such assets and reduced cost. There is a need to keep track of updation/ upgradation of IT assets and version changes in software. It is likely that when companies have several branches the assets purchased and installed are of latest version and latest technology. When these are networked with branches/ headquarter with old version/ different platforms, the compatibility should exist. Proper inventory of assets would help determine the effectiveness of IS operation.

- Determine if the management has maintained a complete inventory of all LAN hardware including the file server, printer, modems and the like.
- Determine if an inventory of all LAN software - application and system is maintained.
- Identify the person responsible for maintaining the reports.
- Determine if the inventory reports are maintained in a secure place.
- Determine the date of last update of the report.
- Determine if the hardware inventory contains a unique identification number.
- Determine whether the hardware components are marked with the identification number, which cannot be erased or removed.
- Determine if the policy exists for disposal of obsolete or badly damaged LAN equipment.
- Identify the person responsible for disposing the equipment.
- Determine if the unused equipment is properly and securely stored.
- Verify on sample basis the LAN hardware inventory report with the actual hardware devices.

Backup and Recovery, Contingency planning: Without a backup and recovery plan it may be difficult for a company to survive and exist when a contingency occurs. The plan provides that all the critical activities necessary for the working of the company must have an adequate back up and standby system.

- Determine if there is a complete inventory of all files related to LAN.
- Determine if a policy exists for updating and maintaining LAN file inventory.
- Determine if the LAN facility is protected by insurance coverage.
- Determine whether a contingency plan exists.
- Determine if the anti-virus software is in use.

- Verify whether the contingency plan includes procedure for securing data files and for varying levels of emergency or processing interruptions.
- Determine if critical files are identified and backed up.
- Determine if critical backups stores off site.
- Determine if the loss of the wiring closed considered in the contingency plan.
- Determine if there is backup equipment for the server.
- Verify whether the plan includes procedure for recovery of system applications.
- Determine whether the management provides the list of documents and files to be maintained off site.
- Determine the frequency at which the plan is reviewed and whether it is current.
- Determine if the plan has been tested.

Answer: [d] Virus checking software is in use

Module:4

Reference No:M4066

Question: Logical access control consists of usage of proper access control mechanism and related security. In the audit of logical security in a LAN environment the auditor ensures that

- [a] Virus checking software is in use
- [b] LAN audit trails for login ID are maintained for a reasonable period of time
- [c] The inventory reports of the hardware are maintained
- [d] All the control files are identified

Module 4 - Audit of LAN Part 4

The primary purpose with which audit of LAN is undertaken is to ensure that the access to and use of LAN resources if appropriate and authorised.

This is the fourth of eight part series on LAN audit. The third part covered inventory control and backup and recovery, contingency planning of LAN audit. In this article we cover logical security of LAN audit.

Logical security: Logical access control consists of usage of proper access control mechanism and related security. Audit for this area consists of looking into passwords, vendor relationships, audit trails and the like. Thus the auditor must

Ascertain if segregation of duties exist between the functions of LAN administrator and LAN security administrator

Personnel:

- Determine if there exists a written authorisation for access to LAN and that the related applications and access is on a "need to know" basis.
- Determine whether the LAN software prevents access by unauthorised users to LAN services.
- Determine whether the LAN software prevents access by unauthorised users to sensitive system functions.
- Determine whether the access to disks, directories and files are restricted to unauthorised users.
- Determine if the users are able to load and run only those executables for which they are specifically authorised.

- Identify the software security controls that are not integral to the LAN system, evaluate effectiveness and verify that only authorised persons can configure control features

Log in ID/ Passwords:

- Ensure control over log in ID and password.
- Ensure that the passwords are hidden when entered.
- Determine whether passwords are encrypted when being sent to the server for verification
- Determine whether system enforces change of password.
- Determine whether log in IDs are disabled when passwords are not changed.
- Determine whether the system enforces minimum password length.
- Ascertain if passwords are stored in clear text anywhere on the LAN and at workstation.
- Determine if the group or shared passwords are permitted on the LAN.
- Ascertain whether log in ID get automatically disabled after a number of failed login attempts.
- Ascertain whether employees sign corporate system policy statement.
- Ensure that the temporary log on IDs issued to vendors contractors or temporary employees expire after the term of their contract.
- Search the general areas of the computers that utilise LAN to find written passwords.

Vendors. Contractors, temporary employees:

- Determine whether the vendors, contractors or temporary employees restricted to specific workstations.
- Determine if the vendors, contractors or temporary employees sign the non-disclosure statements.

Audit trails:

- Determine if audit trails are maintained for login and passwords with details of - location, date, time, user ID, type of access, number of invalid access attempts, logouts due to inactivity and the like.
- Determine whether the audit trails are maintained for a reasonable period of time.
- Determine if exceptional reports are produced on the basis of audit trail.
- Identify the person responsible for reviewing the report.
- Determine whether the follow up action is taken on basis of exceptional reports.

Answer: [b] LAN audit trails for login ID are maintained for a reasonable period of time

Module:4

Reference No:M4067

Question: Environmental controls include protection from water, temperature, dust and related matter. While auditing the environment controls in a LAN environment the auditor should confirm that

- [a] LAN file server facility has dust, smoke and other particulate matters
- [b] Consumption of food, beverage and tobacco is allowed
- [c] Air conditioning, humidity control system are followed as desired by the users of the LAN
- [d] Fire protection equipment are adequate and appropriate

Module 4 - Audit of LAN Part 5

The audit of LAN gives an assurance to the management that the controls are effectively implemented in LAN environment.

This is the fifth of eight part series on LAN audit. The fourth part dealt with logical security of LAN audit. In this article we cover physical security and environmental controls of LAN audit.

Physical security: Physical security is yet another important aspect for smooth day-to-day functioning of IT department. Even a small disturbance due to faulty cabling or unauthorised entry to server room may cause serious disruption to the operations.

- Verify whether the physical security provided for servers, network and communication equipment is adequate.
- Verify whether the servers are kept in a secured room.
- Determine the persons who have accessibility to server room.
- Determine the procedure for authorising access.
- Determine whether the keys are properly secured, and accessible to authorised personnel only.
- Determine whether the duplicate keys are properly stored and secured.
- Determine whether unrelated equipment and supplies are stored in the secured area.
- Verify that the major and primary distribution equipments are in controlled access area.
- Verify that secondary distribution equipment is properly protected from accidental disconnection or disturbance.
- Verify that high risk applications are protected from unauthorised physical access and unauthorised monitoring by use of appropriate sheathing, conduit or properly installed media.
- Determine whether procedures exist to detect and defeat unauthorised physical access.
- Determine the reporting capabilities of the management for monitoring security.

Environmental Controls: Environmental aspect includes protection from water, temperature, dust, uninterrupted power supply and related matters. The following aspects are within the purview of the auditor.

- Verify whether all workstation distribution cabling and connections are installed properly and secured to prevent accidental disconnection or disturbance.
- Determine whether the environmental conditions meet equipment specification - electricity supply, UPS, emergency power and conditioning equipment, static control.
- Determine whether the available fire protection equipment is adequate and appropriate.
- Determine if the LAN file server facility is being kept free of dust, smoke and other particulate matter.
- Determine if consumption of food, beverages and tobacco products is prohibited by policy in LAN file server facility.
- Determine that the online storage of all systems - server software, backup media, and workstation media is adequate.
- Determine if the backup diskettes and tapes are protected from damage due to temperature extremes, effects of magnetic fields, water damage.
- Determine whether access to printers and printed output is controlled.
- Determine whether procedure exist for managing the physical distribution of printed output.

Answer: [d] Fire protection equipment are adequate and appropriate

Module:4

Reference No:M4068

Question: Operations in a LAN environment are day to day operation, processes, activities etc. The auditor while auditing the controls over operation in a LAN confirms that

- [a] There is segregation of duties
- [b] Operation staff can change the controls over operation as desired by them
- [c] Roles are identified but the personnel performing the role define the responsibility
- [d] LAN response time is not to be considered for the operation

Module 4 - Audit of LAN Part 6

The auditor before commencing the audit takes into account the purpose of the audit and the processing environment that exists.

This is the sixth of eight part series on LAN audit. The fifth part covered physical security and environmental controls of LAN audit. In this article we cover controls over operations and equipment maintenance of LAN audit.

Controls over operations: Operations involve day-to-day operations, processes, activities and the like. Though web related servers would run 24 hours, LAN not involved in web operation have to be started and shutdown. LAN administrators are responsible for daily process, backup, change management and the like. Thus the auditor must

- Determine if the system administration and operation procedures are documented and current.
- Determine if the roles and responsibilities are clearly defined for each position.
- Determine if the segregation of duties is appropriate.
- Determine if the LAN administrator has a backup person.
- Determine if the LAN administrator is assigned the responsibility of managing trouble shootings in LAN.
- Determine if the LAN administrator monitors LAN response time, disk storage space and LAN utilisation.
- Interview LAN users and determine if they are satisfied with response time and LAN availability.
- Determine whether the procedure exist for operational staff to manage change control.
- Determine if procedures exist to inform users of system change.

Equipment maintenance: The equipments that are used by the company must regularly be maintained for the efficient and effective performance. The regular maintenance assures that the chances of failure or breakdown are less. The equipment maintenance may be carried out either by the internal staff or by purchasing an annual maintenance contract.

- Determine whether the procedures exist for problem management and resolution.
- Ascertain if the escalation procedure exist to ensure appropriate response to system problems.
- Determine whether problem resolution log is being maintained.
- Review the problem resolution log to determine if the problems are recurring.
- Review the log and determine the existence of any problem which may represent a breakdown.
- Verify whether a system maintenance log exists for network equipment and services.
- Verify whether a preventive maintenance program exists.
- Determine if the maintenance is carried out as per schedule.
- Determine if the log reflect entries for performance capacity monitoring.
- Determine if the above log is maintained by the system or manually.
- Determine if all the system generate logs.
- Identify the person responsible for scrutinising such logs.
- Determine the frequency at which such logs are reviewed.
- Determine whether the management uses the above log to track performance, capacity and transmission quality.

- Determine whether a procedure exists to respond to system identified problems or efficiency degradation.

Answer: [a] There is segregation of duties

Module:4

Reference No:M4069

Question: Different controls are required in the software whether they are re purchased, customised or developed. The auditor while auditing the LAN determines that

- [a] There exists a license agreement for purchased software
- [b] All the users have contact number of the vendor
- [c] Users can ask the vendor to customize the software as required by them
- [d] All the software used by the company is accessible by everybody on the LAN

Module 4 - Audit of LAN Part 7

During the course of audit the auditor takes into account the various aspects related to LAN such as vendor relations, change control procedures, the logical security, physical security and the like over LAN audit. This is the seventh of eight part series on LAN audit. The sixth article covered controls over operations and equipment maintenance of LAN audit. This article covers software controls of LAN audit.

Software Controls: Several softwares including operation software and application software would run in LAN. There can also be utilities and tools for software development and for security. Company may opt to buy generalised software or request customisation for specific needs. Company may also develop its own unique software. Different controls are required depending on whether they are bought, customised or developed.

Determine what software applications are run on LAN.

Verify whether they are developed inhouse or purchased from the vendor.

Vendor: When the applications are purchased

- Determine if the vendor reliability/ support has been looked into before purchasing LAN software.
- Obtain the license agreement.
- Ascertain that the actual usage of purchased package does not exceed the number of copies that are allowed by the vendor.
- Determine what modifications can be made by the company personnel.
- Determine whether the vendor provides for a user documentation or has the one developed by the company.
- Identify the person who can speak to vendors.
- Identify whether the management has laid down a policy for sharing information with the vendor.
- Determine from where the vendors can access the company's system.

Change control:

- Determine whether the LAN program change process conforms to corporate program change control procedures and standards.
- Determine whether the techniques used to monitor program change control are adequate.
- Determine whether the systems are tested before implementing the program changes.

- Determine whether the procedure for system change control takes into account the impact of the change to the business, users and system efficiency.
- Determine whether procedures exist to train and assist the users in event of change in system environment.
- Determine if procedures exists to test and implement operating system upgrades, patches, fixes and enhancements.
- Determine whether procedures exists to test and implement application upgrades, fixes and enhancements
- Determine whether procedures exist to test and implement the introduction of new productivity tools and programs.
- Determine whether procedures exist to test and implement changes in physical environment.
- Determine whether a configured test system or a logical test system exists with appropriate isolation to the production environment.
- Determine if adequate controls exist to prevent significant impact to system efficiency or availability.
- Determine if the procedures are in place to guard against the virus.

Answer: [a] There exists a license agreement for purchased software

Module:4

Reference No:M4070

Question: The relationship with vendors is important from the view of maintenance of the systems and servicing. The auditor in his review of LAN ensures that software meets the demand of the company and

- [a] The vendor reliability is not important
- [b] The license agreement exists
- [c] The vendor support for the installation, training need not exist
- [d] The software is purchased without approval of the senior officials

Module 4 - Audit of LAN Part 8

Audit is categorised into pre-audit phase, the audit phase and post audit phase and audit of LAN is no exception.. In the pre-audit phase the auditor tries to obtain the understanding of the LAN environment. In the audit phase the auditor conducts a detailed scrutiny of each area to confirm whether the controls are in place and are working as desired.

This is the eighth and concluding part of the series on LAN audit. The seventh part covered software controls of LAN audit. This article covers vendor relations, communication security, training and user education of LAN audit policy.

Vendor relations: Vendor relationship is important from the view of maintenance of systems and servicing. Different systems would have different warranty period and service life. A company many have installed systems from different vendors with different service agreement. A proper record would enable appropriate maintenance. Hence the auditor should

- Determine if vendor reliability is considered before purchasing LAN hardware and software.
- Determine if the license agreement exists and obtain a copy of it.
- Verify the maintenance agreement.
- Determine if a service log is maintained to document vendor support servicing.

- Determine if the vendor support requirement clearly defined.
- Determine if the vendor trains the staff to take care of exigencies.
- Determine if the reliability of vendor from trade periodicals, financial reporting services trade associations and MIS management.
- Scrutinise the service log for such software or hardware that have been subject to numerous problems and vendor assisted support.
- Obtain the management and the users justification on the above activity.
- Determine if responsibilities of the vendor is documented in the problem management procedure.

Communication security: The management should institute policies and procedures to protect data from being changed or intercepted. All the communication equipments must have a proper security. Controls should also exist to ensure that there is no unauthorised usage of the communication channel. This helps in maintaining the integrity of data.

- Determine whether controls are adequate and ensure that there is no
 - Misrouting
 - Unauthorised message alteration
 - Unauthorised disclosure
 - Incomplete transmission
 - Message duplication
- Determine whether communication links are properly secured which includes links to software packages, encryption devices and other processing devices
- Determine how the microcomputers are connected to each other and other processing entities - modems dial up, dial back, leased line et al.
- Determine whether effective access and implementation controls exist over
 - Network change control
 - Dial up access
 - Network activity logging
 - Data encryption
- Determine whether control exist to ensure that data integrity is maintained during data transfer from LAN to other processing entities
- Determine the procedure of how the batches are identified, screened and approved on the LAN

Training and user education:

- Determine whether policies and procedures exist for training the users, operators and staff.
- Determine whether the management provides documents and reference material for training purposes.
- Determine whether the users are educated about the security and control aspect of system.
- Determine if the users are educated about confidentiality of information and software copyright laws.
- Interview LAN users if they are satisfied with the level and timing of LAN training provided.

Post audit:

The auditor should ensure that the suggestions made by him have been implemented. If the suggestions are not implemented then the management must satisfy the auditor about the reasons for non-implementation of the suggestions. The audit should cover all the business areas that are connected to LAN. The audit must be conducted annually and management must ensure that all areas are covered. Ad hoc audits may be conducted when there is a change in the system.

Answer: [b] Software meets the demand of the company and the license agreement exists

Module:4

Reference No:M4071

Question: The auditor while reviewing the local area network (LAN) takes into consideration the purpose and processing environment. In the pre-audit phase the auditor

- [a] Considers LAN utilities, which are used by the company and takes training on the same
- [b] Ensures whether the hardware inventory contains a unique identification number
- [c] Ensures whether the procedure exists for operation staff to manage change control
- [d] Review the problem resolution log to determine if the problems are recurring

Module 4 - Audit of LAN Part 1

A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are commonly shared by multiple computer users.

The auditor while reviewing the LAN should take into consideration the purpose and processing environment. The primary purpose of audit is to ensure that access to and use of LAN resources is appropriate and authorised.. Audit of LAN must be tailored individually because all network components do not receive uniform attention, and vary with the type of audit, the complexity of LAN and the operating environment. The audit phase of LAN can be categorised into

- Pre-audit phase
- Audit phase
- Post audit phase

In this article we cover the pre-audit phase of audit of LAN.

Pre-audit phase

During the pre-audit phase the auditor should obtain an understanding of LANs in general and a more specific understanding of the LAN environment in the company. The tasks during the pre-audit phase that the auditor must perform are

Familiarisation with

1. LANs and LAN review: If the audit on LAN is being conducted for the first time, the auditor should first familiarise himself with all relevant theories on LAN. He should refer to materials on LAN package, LAN terminology, LAN workings, LAN security, LAN audit, LAN issues, risks and impact.

2. Specific LAN environment: Having understood the general concepts related to LAN, the auditor should start communicating with the LAN administrator and look into

- The features of LAN in the company including a flowchart of LAN and confirm that his understanding is correct
- Company standards and LAN policies
- The areas of LAN audit conducted earlier and the reports
- The risk areas, problems that existed earlier and whether these issues were sorted out. If so how, and if not why?
- The LAN utilities used by the company and and undergo training on the same to understand the features

Planning: During the planning stage, the auditor should

- Obtain a list of file servers, database servers and print server names from LAN administrator.
- Determine the data that is stored on each server.
- Ascertain if the LAN is connected to other LANs or the corporate backbone.
- Obtain an understanding of the business areas being supported by LAN applications from the LAN administrator.
- Obtain an understanding of security aspects of the environment.
- Determine what facilities are relied upon for what information.
- Understand key components and interfaces.
- Define initial scope of reviewing the plan.
- Determine the areas of LAN environment critical to the business area under audition.
- Look into the problematic areas.
- Discuss with the management any special area or aspect requiring audit concentration.

Detailed planning on specific tasks: In this phase the auditor should

- Determine the tests to be conducted, the criteria for evaluation and the like.
- Determine the software product to analyse workstations for software compliance testing.
- Identify the areas beyond his competence so as to avail the services of an expert.
- Contact the experts and provide them with the information as per the needs and the amount of time that is required.
- Explain the client about the standards of evaluation.
- Obtain ID and password to gain access to LAN environment.

Answer: [a] Considers LAN utilities, which are used by the company and takes training on the same to understand the features

Module:4

Reference No:M4072

Question: One of the basic objectives of LAN audit is to ensure that

- [a] Effective controls exist for the security of organisational data files and program libraries
- [b] Logs are maintained for recording of all security related incidents
- [c] Passwords are chosen carefully
- [d] Administer account are renamed to deter intruder hacking

Module 4 - Audit of LAN Part 2

The audit of LAN is one of the important area on which the auditor focuses his attention during the course of his audit.

This is the second of a seven part series on Audit of LAN. The earlier article covered pre-audit phase of LAN. This part deals with the LAN standards and data integrity of LAN audit.

The audit of LAN must meet and satisfy the basic objectives laid down by the management. Thus the purpose of audit is to ensure

1. Standards for effective and efficient operation of the end user environment.
2. Effective controls for the security of organisational data files and program libraries.
3. Maximum system availability and performance through such controls, for all the phases of operations.
4. Proper controls for installation, maintenance, and use of vendor developed software residing on LAN.

5. Adequate physical security for computer equipments.
6. Contingency plan for timely and logical recovery of processing operation.
7. Policies and procedures to protect sensitive data from being changed, intercepted or unprotected on the LAN.
8. Training users on effective and efficient utilisation of system resources.

Audit procedure

LAN Standards: Standards include the management policies, procedures and the direction for operations. These guidelines are important documents especially for companies having several branches. They ensure uniformity in procedures and practices. The guidelines must

- Identify and authorise person responsible for the operation, maintenance and usage of LAN.
- Ascertain if procedures exist for start up and shut down of systems.
- Determine the existence of the policies, procedures and standards manual.
- Determine if the policies, procedures and standards are current.
- Determine if the policy has been communicated to the users.
- Determine the role of operators, network support, and IT personnel in monitoring security.
- Determine the way in which the management enforces compliance with security and acceptable usage of policies.
- Ascertain the existence of emergency procedures.
- Determine if procedures exist for tape and disk management.
- Determine if effective control exist over stock paper and negotiable instruments.
- Determine that procedures exist for the classification of data and the effective security over sensitive data.
- Determine if the management has developed strategic plan for utilising LAN technology.
- Determine if there is a formal job description for the LAN administrator.

Data integrity: Data is an important asset. Integrity of data implies that data can be accessed and modified only by the authorised users. When integrity of data is not maintained, the functioning of the company will be affected since the employees will be met with ignorance. This puts the reputation of the company at stake and may lead to heavy losses. Hence it is necessary to

- Determine if the LAN files have been classified as critical and sensitive.
- Determine if the files are protected from unauthorised access and update.
- Determine if the controls are in place to ensure complete and accurate data transmission through the LAN network.
- Determine if the proper authorisation exist for
 - Software changes.
 - Testing software changes before implementation.
 - Backup of old versions of software.
 - Making changes and updates to software.
- Review sample files labeled non-sensitive to ensure that the classification is correct.

Answer: [a] Effective control exist for the security of organisational data files and program libraries

Explanation: Other options are verification procedures to check controls.

Module:4

Reference No:M4073

Question: For ensuring adequate security of LAN, the auditor must exercise control over

- [a] Password
- [b] Policies
- [c] Firewall
- [d] Applets

Module 4 - LAN and Security of Data - Part 1

Data is an important asset of an organisation. The primary responsibility of the management is to safeguard data. Data stored and transmitted through servers is vulnerable if it is not protected properly. Added to this is the problem of unauthorised access. Hence an audit of security of data in a LAN becomes necessary.

This is the first of a two part series on LAN and security of data.

1. Controls over server data

1.1 Physical access control

- Determine if the physical security to the server is adequate

1.2 Logical access control

- Determine if the security features on the system prevent and detect unauthorised access attempts to the file server
- Determine whether the passwords used are in accordance with the password policy of the organisation
- Determine the frequency at which passwords are changed
- Determine whether the system automatically gets disconnected after sustained inactivity

1.3 Administrative control

- Identify the person responsible for dial up activities

1.4 Other controls

- Determine if the dial up number is confidential.
- Determine if dial back is being used.
- Determine if there is procedure to be followed for monitoring dial up activities.

2. Control over applications

2.1 Other controls

- Determine if guidelines exist for purchasing LAN applications.
- If the applications are developed in-house, determine if there exists a formal development methodology or process to develop the applications.
- Determine if the documents exist for applications.
- Determine if the applications are adequately tested before implementation and are according to the business needs of the organisation.

3. Controls over password

3.1. Logical access control

- Determine if access control software is in use.
- Determine if additional passwords are required to access sensitive data.
- Determine if the password policy framed by the organisation is being followed (refer password policy).

4. Control to prevent unauthorised alteration of data

4.1. Logical access control

- Determine if the access rules exist.
- Determine if the network operating system has security features to restrict certain types of transactions on the server data.
- Determine if the access to special utilities on the network operating system is restricted.

4.2. Administrative control

- Identify the person responsible for implementing the access table.

4.3. Other controls

- Determine if the audit trails and transaction monitoring exist for sensitive applications.

5. Controls over encryption of data

5.1. Other controls

- Determine if the process has been defined for encryption.
- Determine whether the management has defined the policy for identifying the data and whether such data is encrypted.
- Determine if the keys used for encryption are adequately secured.

6. Controls over server resources

6.1. Administrative control

- Determine if the service staff exists to support the staff/users.

6.2. Other control

- Determine if the device protection features (UPS for instance) is being used.
- Determine if the processing and data storage resources (disk duplexing, processor duplexing) are used.
- Determine if escalation procedures exist for diagnosis and trouble shooting.
- Determine if there exists a resource capacity planning and monitoring.

Answer: [a] Password

Module:4

Reference No:M4074

Question: Data is an important asset in an organisation. To prevent the interception of data the auditor should determine

- [a] Whether the redundant network cabling schemes and communication resources are being used
- [b] Whether access controls exist at the source and destination of data transfers
- [c] Whether the audit trails and transaction monitoring exist for sensitive applications
- [d] Whether the system automatically gets disconnected after substantial inactivity

Module 4 - LAN and Security of Data - Part 2

Security of data is a high priority task for any organisation. Hence there should be efficient control mechanisms to ensure its security.

This is the second of the two part series on LAN and security of data.

Controls over sever data, applications, password, unauthorised access, encryption and server resources have been covered in detail in the first part of the article. More such control mechanisms have been dealt in this part.

1. Control over dial up

1.1. Other controls

- Determine if the phone numbers of dial up ports are kept confidential.
- Determine if the phone number of dial up ports are being changed periodically.
- Determine if the vendor maintenance is prohibited via remote dial up.

2. Controls over Communication

2.1. Other controls

- Check for any redundant network cabling schemes and communications resources.
- Determine if the fault tolerance in critical applications is adequate.
- Determine if the contingency plan takes into consideration the communication server.
- Determine if the plan has been tested.

3. Control to prevent interception of data

3.1. Physical access controls

- Determine if the physical layout and cabling is secure.
- Determine if LAN hardware identifiers are used (Network interface card).
- Determine if the use of modems and dial up lines is restricted.
- Determine if the physical security over the location of communication servers, bridges and gateways are adequate.

3.2. Logical access control

- Determine if the data message is authenticated.
- Determine if access controls exist at the source and destination of data transfers.

3.3. Administrative control

- Authorise the person who is responsible for controlling the use of modems and dial up lines.

3.4. Other controls

- Determine if the procedures exist for monitoring sensitive upload/ download operations.
- Determine if sensitive data is encrypted before it is transmitted.
- Determine if the sensitive applications and data isolated on stand alone PC or specific LAN workstation.

4. Controls over line penetration/ interception

4.1. Other controls

- Try gaining access as an authorised user.
- Try eavesdropping on telecommunications transmissions.
- Try intercepting, modifying and re-transmitting.

5. Controls over backup procedure

5.1. Physical access control

- Determine if the back up is stored in a secure place.

5.2. Logical access controls

- Determine if the file server data is routinely backed up.
- Determine if the restart and recovery procedures are tested on a periodic basis.

5.3. Other controls

- Determine if data redundancy such as disk shadowing, mirroring is used for important data on server.
- Determine if the policies exist with regard to use of unlicensed software. (Refer software policy).
- Determine if the virus protection/detection software exists on the server.
- Determine if disaster recovery procedure exists.
- Determine if the procedure has been tested.

Answer: [b] Whether access controls exist at the source and destination of data transfers.

Module:4

Reference No:M4075

Question: LAN configuration if altered without proper controls may lead to disrupted operations. Which of the following is the control objective over configuration change control for the continuous satisfactory operation of LAN?

- [a] Log book is maintained for LAN downtime
- [b] LAN server is adequately protected
- [c] There exists a procedure for changing configuration
- [d] Access to LAN is on need basis

Module 4 - Control Objectives of LAN

When a LAN is installed, it is the responsibility of the management to ensure its effective functioning. Hence there is a need for control objectives viz.

- Framing policies
- Physical security
- Logical security
- Support and management
- Control over changes

Framing policies: The management must ensure that a policy exists to intercept the selection, acquisition and implementation of LAN.

- The policies must address issues pertaining to
 - Procedure for selection, acquisition and installation of LAN.
 - Standards for network architecture.
 - Cost benefit analysis.
 - Documentation of installation.
 - Data security and confidentiality.
 - Procedures for backup.
 - File naming conventions.
 - Equipment inventory controls.
 - Software inventory controls.
- Policies must be communicated to the employees.
- Develop a strategic plan for effective utilisation of LAN.
- There is appropriate segregation of duties in the selection, authorisation and implementation of LAN.
- Vendor reliability/ support considered before purchasing LAN hardware and software.

Physical security: The physical assets if not protected will be exposed to physical threats. To protect them, the management must ensure that

- LAN server is adequately protected.
- LAN server is connected to uninterrupted power supply (UPS).
- LAN server is protected from damage which may arise due to electric power surges/ spikes.
- Transmission media is adequately protected.

Logical security: Logical security ensures that there is no unauthorised addition, alteration, or deletion to access controls. The management must ensure

- Procedures for any addition, deletion or alterations to LAN access.
- Access to LAN is on need basis.
- Request for change to LAN is on a standard form.
- Review and approval process are included in the standard form.

- The security management adequately supports changes to LAN user access profiles, that include
 - Access control via change made to user accounts, password.
 - Encryption of data or password.
 - Log in and log out of audit trails.
 - Diskless workstations.
 - Disabling of workstation after certain number of unauthorised logon attempts.
 - Restricted off site log on capability.
 - Automatic log off after a short period of inactivity.
 - Monitoring of access/ use of LAN resources.
- Process of restricting, identifying and reporting authorised/ unauthorised users of LAN is automated.

Support and management: The LAN operation should not be interrupted as it affects the functioning of the entire company. For this purpose there should be a sufficient network management and support. For uninterrupted reliable operation of the LAN the management must ensure that

- There is an efficient network management and support team.
- Procedures exist for periodical review of LAN.
- Users are provided with adequate response time and sufficient disk data storage space.
- LAN administrator is responsible for troubleshooting the problems.
- Log book is maintained for LAN downtime.
- Backup person exists for LAN administrator.
- Cyclic applications are documented.
- LAN utilisation and performance are periodically reviewed.
- Preventive maintenance schedule exists.
- LAN administrator and users are adequately trained.

Change control: LAN configuration if altered without proper controls over changes to configuration may lead to disrupted operations. For continued satisfactory operation of the LAN the management must ensure that

- There exists a procedure for changing the configuration.
- The above process is documented.
- Adequate backup procedures are made before a change is implemented.
- Users are given adequate notice before implementing a change.

Answer: [c] There exists a procedure for changing configuration

Explanation: Option (a) - Support and management

(b) - Physical security

(c) - Change control

(d) - Logical security

Module:4

Reference No:M4077

Question: Connection Establishment and Termination in Transmission Control Protocol (TCP) do not require?

- [a] connect" and "disconnect" request
- [b] Confirmation of request
- [c] Acknowledgement of confirmation
- [d] Encryption of connection established message

Module 4 - TCP Connections

Transmission Control Protocol is a connection-oriented, reliable, transport layer protocol in the TCP/IP Protocol suite. Each of these terms is described below:

Connection-Oriented

A connection-oriented protocol creates a virtual path between the source and the destination. When data is to be sent, the TCP protocol, establishes a connection between the sender and destination stations. Only after establishing the connection, is the data sent. The connection is maintained as long as data is to be sent. After all the data has been sent, the connection is closed.

It is similar to the telephone system, in which after the receiver lifts the phone, the line is dedicated to the conversation and is broken only after.

TCP data transmission takes place in full-duplex mode, i.e., both the hosts transmit data simultaneously.

Connection Establishment and Release

Before any data can be sent between two hosts using TCP, a connection must be established. The sending and receiving stations transfer data in the form of segments. A segment consists of a fixed 20-byte header and may contain zero or more data bytes.

One host, called the server, listens continuously for connection requests. The host requesting a connection is called the client. There are three steps for establishing a connection between the two computers.

1. A "connection request packet" is sent from the sending machine (requesting machine) to receiving machine.
2. The receiving machine (responding machine) responds with a connection confirmation.
3. The requesting machine returns a packet acknowledging the confirmation.

These three steps together are known as the 3-way handshake and only when it is completed is a TCP/IP connection established between the source and the destination.

Once the connection is established, data can be sent and received. After complete transmission of data, the "close" formalities should be observed for "connection termination." This is also a 3-way handshake process.

The steps for terminating the connection are:

1. Requesting machine sends a "disconnect" request packet.
2. Responding machine confirms the request.
3. Requesting machine acknowledges the confirmation.

Answer: [d] Encryption of connection established message

Module:4

Reference No:M4078

Question: What function does Address Resolution Protocol (ARP) perform?

- [a] It relates IP addresses to Ethernet addresses
- [b] Prevents two computers from using the same IP address
- [c] Enables a diskless workstation to know its IP address by broadcasting its Ethernet address
- [d] Resolves a name like www.themanagementor.com to the IP address of the computer hosting the web site

Module 4 - Address Resolution Protocol

A network is an interconnection of computers connected together by devices such as bridges and routers. To communicate on the network, each computer must have a Network Interface Card (NIC), which takes care of the physical aspects of transmission.

Each computer must have an address so that other computers can send data to it. There are two types of addresses: physical and logical addresses. Physical addresses are usually the addresses imprinted in the NIC (except in a few cases such as LocalTalk). They are 48-bits in length and must be unique within the network, but may not be outside the network. Such addresses are also called Medium Access (MAC) layer address. If for any reasons, the NIC of a machine fails, it is replaced by another NIC with a new physical address. The problem arises when the server holds only the relation between the NIC and the IP address and does not update when a new NIC card is used. When a machine in a network wants to send and receive message from outside, it should have an IP address irrespective of its physical address. This IP address has universal jurisdiction and cannot be changed.

Ethernet and Token-Ring cards only know how to recognize the MAC addresses and any computer to communicate on a network must be able to specify the MAC address of both itself and the destination of its messages. Just knowing the IP address of the destination computer, like 128.200.10.4, is not sufficient. Hence, to transfer data from one machine to another, we need to have both these addresses. So we need to map physical address to its IP address and vice versa. This mapping is done by Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP). Address Resolution Protocol can be used to find out the physical address of a computer if the IP address is known while RARP is used to find out the IP address given a physical address.

When the router receives a packet with a specific IP address and it does not know the physical address of the machine to send it, the router formats an ARP query and sends it to all the machines in the network. The machine to which the IP address belongs responds back with its physical address. On receipt of this response, the router sends the packet.

Similarly, when a host is a diskless node or get connected to the network for the first time, it may not know its IP address, so it sends a RARP with its physical address. The server on which this machine is connected responds back indicating the machine's IP address.

In addition to ARP and RARP, there are two more protocols associated with the TCP/IP network layer, ICMP and IGMP. ICMP (Internet Control Message Protocol) notifies to the sender of a message when it is not delivered to the final destination. It handles only the Datagram, which has only the addresses of sender and receiver. ICMP only notifies, but does not correct.

IGMP (Internet Group Message Protocol) is useful in sending a single message to a large number of recipients simultaneously.

Answer: [a] Address Resolution Protocol can be used to find out the physical address of a computer if the IP address is known.

Module:4

Reference No:M4079

Question: Which one of the following statement is true with respect to VSAT?

- [a] Usage is restricted to geographical boundaries
- [b] Very high cost due to the usage of fibre optic cables
- [c] Though quality of data is high, it doesn't support high bandwidth
- [d] It operates in two frequency bands namely Ku and C.

Module 4 -VSAT

What is VSAT?

VSAT (Very Small Aperture Terminal) is a form of satellite communication system designed for portable usage in homes and businesses. Data, voice and video signals are transmitted through a satellite to the required destination. About 56 Kbps of data transfer takes place via VSAT.

Structure

VSAT is composed of two parts namely a transceiver, and end user system. The transceiver is a device that receives and sends signals to a transponder of the satellite. The transceiver is placed facing the satellite and is interfaced with the end user's PC.

The PC is taken as the reference ground or central hub for the satellite to send and receive signals. This forms a star topology since each user is connected to the central hub.

Operational modes

VSAT systems operate in two frequency bands namely Ku and C.

1. Ku-band systems utilise smaller antennas. They are widely used in Europe and the US.
2. C-band systems use larger antennas and are used in Asia and Africa.

Network types

The network arrangement is dependent on the end user's dedicated facility. Accordingly, VSAT networks are either Point-to-Point, Point-to-Multipoint or on demand. Typically, five to thirty sites are connected through a mesh system for smaller networks. High-end networks deploy as many as thousands of sites.

VSAT over terrestrial lines

Costs involved in landlines or cables are distance dependent, whereas VSAT provides high scalability since the costs are not dependent on distance. As the number of users increases, costs also reduce considerably. Comparison is based on three parameters namely installation, geography and bandwidth. This leads to the following findings:

1. Geography: There are no geographical boundaries for the usage of these networks and they cover deserts, mountains and even remote islands.
2. Installation: The inherent feature of not using wires provides the advantage of speedy installation and operation.
3. Bandwidth: a high range of bandwidth is made available by the use of satellites. This enables transmission of high quality data, video, and voice

Applications

Some applications are recommended only for receiving while some others for both transmission and reception. These include:

- Video conferencing
- Internet
- Voice telephony
- Bank transactions
- Database queries
- Reservation systems
- Electronic fund transfer
- Stock market updates
- Distribution of video, TV and music

Insurance companies, drug stores, supermarkets, car rentals, oil exploration companies, petrol pumps, health care companies, hotel chains, mines, heavy industries, electrical utilities and the like employ VSAT networks. Household applications go for services like the DirectPC connection. Companies usually deploy their own leased VSAT system.

Advantages

Reliable and cost effective transfer of data to any remote location through multiple sites is made possible by VSAT networks. They provide efficient, value added services support to the Internet, LAN and public network communications solutions. Business and home applications have the privilege of higher speed data

transfer in comparison with telephone lines and ISDN connections. Further, these systems are easily expandable and upgradeable. This in turn makes management and performance monitoring an easy issue.

Answer: [d] It operates in two frequency bands namely Ku and C

Module:4

Reference No:M4080

Question: Which of the following uses RTP (Real-time Transport Protocol)?

- [a] Fiber Distributed Digital Interface (FDDI)
- [b] Ethernet
- [c] Mbone
- [d] Backbone

Module 4 -Backbone

Heavy traffic in a network is handled by the backbone. The main connections that make up the network are collectively referred to as the backbone. It is also used to denote a bus i.e, the main wire that connects different computer nodes.

What is a backbone?

The basic structure that holds a network or several networks together is called a backbone. It is the main trunk cable that is used for networking within a building (vertical cabling). Dissemination of information vertically from floor to floor is done by the backbone.

Rationale

Same cables could be deployed to connect all networks. This means the same wires being used to connect the different nodes in various locations serially. But this has the limitations of distance, the number of networks that can be connected and above all the scalability of such a network. Backbone structures are therefore essential for effective networks.

How is it used?

For example, let us consider a company that has three networks in four different buildings. A single high-speed access line that connects these networks together is a backbone. Fast and reliable communication is possible through these networks.

Internet backbone

Main trunks of the Internet that carry most of the traffic are together termed the Internet backbone. This helps a wide range of end users to get connected to each other, to share and access information resources on the Internet.

Multicast backbone

An extension to the Internet that supports multicasting of Internet Protocols is known as Mbone (Multicast Backbone). Multicasting is a two-way transmission of data between multiple locations or networks. This is seen as a step towards upgrading the Internet to handle live multimedia communication. These are equipped with Mbone servers of Class D IP addresses.

How is multicasting possible through Mbone?

The TCP/IP protocol in the Internet breaks messages into packets and transfers each packet independently. These packets traverse different paths to reach their destination. This implies that they arrive in random order, with considerable delay between the first and the last packet.

Further each receiver of data should ensure that separate packets are sent from the source to the destination. This holds good for static information like text and graphics, but not for real-time audio and motion pictures.

Mbone does not split up a single packet for transmission to multiple destinations till the last moment. This provides flexibility to the packet to pass through different routers, before it is broken to reach its final destination. The result is efficient transmission of data with packets reaching multiple destinations, at approximately the same time.

Mbone structure

The use of tunnels and IP multicast protocol forms the basis of Mbone. Multicast packets are transmitted point-to-point between multicast routers or mrouters. For multicasting and broadcasting, LAN technologies like Ethernet and FDDI (Fiber Distributed Digital Interface) are used. To ensure reliable flow of information between networks Real-Time transport Protocol (RTP) is employed.

Answer: [c] Mbone.

Module:4

Reference No:M4081

Question: When emails are exchanged over the Internet, one server handles incoming mails and the other outgoing. With respect to this, which of the following options is true?

- [a] SMTP handles incoming mails and POP3 handles outgoing.
- [b] POP3 handles incoming mails and SMTP handles outgoing.
- [c] Microsoft Outlook handles incoming mails and Outlook Express handles outgoing.
- [d] Outlook Express handles incoming mails and Microsoft Outlook handles outgoing.

Module 4- Email Software

Millions of people use email daily. It is the, cheapest, fastest and most popular means of communication. Earlier, message transfers could happen only between two computers. With advances in technology, messages can be exchanged between different computers in a network by using the "@" symbol.

To send an email, a stand-alone email client such as Microsoft Outlook, Outlook Express, Eudora or Pegasus is required. Emails can also be sent from web-based clients such as Hotmail, Yahoo!, Rediffmail and the like. Stand-alone email clients such as Microsoft Outlook would have to be configured to a web based email server for use on the Internet.

Emails exchanged on the Internet have to go through two different servers, running on a server machine. One is the SMTP server and the other is the POP3 server.

Simple Mail Transfer Protocol (SMTP)

The SMTP server handles outgoing mails. The email client interacts with the SMTP server when a mail has to be sent. The SMTP server listens on port number 25.

For instance, if an email has to be sent from the Hotmail account of Raj to a Yahoo account of Ram, the email accounts would be Raj@hotmail.com and Ram@yahoo.com.

When Raj sends his mail through Outlook Express to Ram, Outlook Express connects to the SMTP server at Hotmail.com using port 25. The Outlook Server informs the SMTP server about the address of the sender, the address of the recipient, and the body of the message. It then breaks the recipient's address into two parts. One part contains the recipient name (Raj), while the other the domain name (Yahoo.com).

Delivery of the message is done using a program called delivery agent. If the same message is being sent to a recipient other than Raj in some other domain, the SMTP has to communicate with the other domain separately.

The SMTP server then interacts with Domain Name Server (DNS) and maps the IP address/addresses to the SMTP server of Yahoo.com. The SMTP server of Hotmail.com then connects with Yahoo.com using port 25. It passes on the message given by the stand-alone client, Outlook Express to the Yahoo server. The Yahoo server then identifies that the domain name for Raj is at Yahoo and hands the message over to Yahoo's POP3 server, which is then dropped into Raj's mailbox.

If for some reason the Hotmail SMTP server is not able to connect to the SMTP server at Yahoo, the message is put in the sendmail queue, using a program called sendmail. It then tries to send it every 15 minutes. If it is unsuccessful even after four hours, it sends a mail informing the sender of the problem. After five days, it returns the mail back to the sender marking it as undelivered.

POP3 Server

The POP3 server maintains a collection of text files for each email account. When an email arrives, it simply appends it to the bottom of the recipient's file. When the user wants to check his mail, he logs on to the POP3 server, using his username and password. The POP3 server opens the text file, and allows him to access it. The stand-alone email client, therefore acts as an interface between the email client and the text file containing the message.

Answer: [b] POP3 handles incoming mails and SMTP handles outgoing.

Module:4

Reference No:M4082

Question: Which area of the ISO Network management Model is responsible for identifying problems, logging reports and notifying the users, so that the network runs effectively?

- [a] Performance Management
- [b] Accounting Management
- [c] Fault Management
- [d] Configuration Management

Module 4 - Network Management

As the size of computer networks increases, so is the challenge to manage and maintain them. Network management is essential for effectively utilising networks.

Network management therefore seeks to control and monitor related activities from a central location. . It involves maintaining distributed databases, autopolling network devices, providing high end workstations, generating real time graphical views of network topology changes, traffic and the like.

Network Management Architecture

Networks generally have the same basic architecture. The various elements of network architecture are as follows:

Network management station: It runs the network management application, which gathers information from the management agent present in a managed device, about all the managed devices. It processes large data, reacts to events and displays the required information. It helps the operator to view the entire network, in the form of graphs.

Management agents: These agents provide information regarding the devices attached to the network, and accept control information.

Managed devices: Devices attached to the network such as a computer, printer, fax machine or routers are referred to as managed devices. They have a management agent.

Network management protocol: The management agent and the network management application use this protocol to exchange information.

The ISO Network Management Model has laid down the key functional areas of network management. The five areas are:

Performance management: It is set up to define the acceptable level of user performance. It includes gathering performance data, analysing it to determine normal levels, and then fixing performance thresholds for each variable. If these thresholds are crossed, it creates a network problem. It therefore helps in establishing the amount of utilisation, and the level at which errors occur.

Accounting management: It is used to measure the network utilisation. Usage of network by groups or individuals is then standardised with this information. It can also be used to create billing information, and to keep network performance at an acceptable level.

Security management: It manages the network by categorising resources into authorised and unauthorised areas. It therefore limits access to network resources, identifies sensitive network resources and differentiates them from other resources in the network.

Fault management: It helps the network management to identify problems, log reports, notify the users and fix network problems automatically, so that the network runs effectively.

Configuration management: Configuration management monitors the network and system configuration information. This helps in tracking and managing the effects of various software and hardware devices in the network.

Answer: [c] Fault Management

Module:4

Reference No:M4084

Question: _____ is not exchanged immediately after a session between two nodes is started.

- [a] DLSw (Data Link Switching) Version number
- [b] NetBIOS (Network Basic Input/Output System) support
- [c] Search frames support
- [d] MAC (Media access control) address of devices

Module 4 - Data link Switching (DLSw)

Data Link Switching (DLSw) is a method of transporting IBM Systems Network Architecture (SNA) and Network Basic Input/Output System (NetBIOS) traffic over a network.

The primary functions of DLSw are:

To maintain the Switch-to-Switch Protocol (SSP) between two DLSw nodes or routes.

To reduce link layer timeouts across WANs by the termination of SNA data-link control (DLC)

Local mapping of DLC connections to a DLSw network.

DLSw SSP

The DLSw uses Switch-to-Switch Protocol to establish connections between two points, handle flow control, forward data, locate resources and handle error recovery. The SSP switches packets in the SNA data link layer. It uses TCP between DLSw nodes for reliable transport over IP-based networks.

DLSw Operation

Two TCP connections known as peer connections are established between the nodes (routers) of DLSw. Each of these peer connections can carry many circuits. A TCP connection is of great help because it guarantees the safe delivery of IP traffic and also maintains the integrity of data. Once the connection is set, DLSw nodes exchange information regarding the capabilities supported by each of them, as there is a possibility of the nodes being made by different manufacturers.

DLSw performs its functions in three mechanisms:

DLSw Capabilities Exchange:

When a session between two nodes is initiated, the information exchange related to the capabilities supported by each node takes place. During this exchange, a number of capabilities are acknowledged. The capabilities can be: the DLSw version number, initial pacing window size, NetBIOS support, NetBIOS name lists, Search frames support.

DLSw Circuit Establishment:

The target end system is identified and a data-link layer (DLC) connects each end system to its local router. DLSw provides a transport mechanism for SNA traffic. The SNA circuit is then established in the following stages.

An explorer frame with MAC address of other SNA devices is sent through the LAN. On receiving this frame the DLSw internetworking node sends a canureach frame to partner DLSws. The frame asks each DLSw to locate the device having the specified MAC address. When a DLSw succeeds in reaching the device it responds with an icanreach frame, which means that it can provide a communication path to that device.

Two DLSw partners can start a circuit after exchanging the canureach and icanreach frames. A DLC connection is formed between each router and locally attached SNA end system. A TCP connection is also formed between the DLSw partners. This circuit is identified by source and destination IDs. The SNA DLSw circuit ID consists of MAC address, a link-service access point (LSAP), and the DLC port ID.

A NETBIOS circuit is formed that is similar to an SNA circuit establishment, but with minor differences.

DLSw Flow Control

This helps to control the flow of traffic and thereby maintains integrity and ensures the delivery of all data.

DLSw Flow Control Indicators

The number of units that a sender is permitted to transmit is called granted units. These are incremented with a flow control indication from the receiver. The flow control indicators are

Repeat: Granted units are incremented by the current window size

Increment: Window size is increased by one, and granted units are increased by the window size

Decrement: Window size is decremented by one and granted units are incremented by the new window size.

Reset: Window size is decreased to zero and granted units are set to zero. This stops all transmission in one direction until an increment flow control indicator is sent.

Answer: [d] MAC Address of devices.

Module:4

Reference No:M4085

Question: A packet-sniffer is a software application which-

- [a] Identifies the packet that is required by the user.
- [b] Captures a packet moving across a network with help of a Network Interface Card.
- [c] Identifies packets which have leaked while travelling through the network.
- [d] Identifies packets, which are not safe to travel without encryption.

Module 4 - Security Issues on the Internet Network security has become an important issue for administrators whose network is connected to Internet. Most of their time is spent in protecting their systems within and outside the network. Although a lot of tools are available to scan and detect intrusion, they provide little help in averting a possible attack on the network.

Information present on a network, can be of two forms- in a physical storage media, such as a hard disk, CD-ROM etc, or in transit passing from one machine to another machine through a wire. Both these forms are vulnerable to attacks from users within a network, or from outsiders if the network is connected to the Internet.

Following are ways in which information can be attacked on a network.

Network Packet Sniffers

When information is transmitted from one machine to another, the data is broken into small pieces of information and then transmitted. These are called network packets.

When travelling through a network packets are present as clear texts and are not encrypted. Any application, which can single this information, and process it, can definitely understand it.

A network protocol clearly defines the packet's content and its destination so that it can reach there intact. The Packet sniffer is a software application, which seizes packets travelling across the network with the help of a Network Interface Card. Since the information transmitted is not encrypted it can be easily captured and understood. It can even provide its user with the username and password of the network users. In a

networked database, it can even give queried results of the database.

Network Administrators use packet sniffers to diagnose and fix network related problems. So there is possibility of administrators stumbling across sensitive information being spread across the network.

IP Spoofing and Denial-of-Service Attacks

A hacker from outside the network uses an IP address within the range of the network or an authorised external IP address, which has been provided to access resources on the network. The attacker enters data or commands into the stream of data while it is passing between the client and server. To enable two-way communication the routing tables are changed to suit the spoofed IP address.

In Denial-Of-Service (DOS) attack, the user makes a request to the system for some service. The system tries to respond to it by establishing a return communication path, during which system resources are exhausted to such an extent that it finally cannot respond even to rightful users.

Password Attacks

The user name and passwords for a user account can be known by different methods like IP spoofing, packet sniffers etc.

Programs such as Brute Force can also identify passwords. Brute Force is a dictionary program, which gains access to server and gives the attackers all the privileges of an authorised user.

Distribution Of Confidential Information

Frustrated employees or ex-employees can share confidential information with persons outside the organisation . An employee can easily place sensitive information on an FTP server or email to an outsider.

Man-in-the-middle Attacks

This happens when an attacker gets access to information packets travelling over networks. For example a user working with an Internet Service Provider could easily gain access to packets of information being routed through the ISP. The attacker could easily steal the information, extract information about the network and its users, transmit corrupt data or introduce new information sessions.

Answer: [b] Captures a packet moving across a network with help of a Network Interface Card

Module:4

Reference No:M4086

Question: Which of the following statements is true.

- [a] A Proxy server is the best option for caching heavy network loads.
- [b] Network caching facilitates the storage of user data in the network.
- [c] Stand alones are costly and require large scale deployments.
- [d] The capacity for storing content on the user's hard disk is decided by the local network cache.

Module 4- Network Caching Technologies

Millions of people use the Internet to access email or search for information. However, most of the time it has been observed that many people access the same websites again and again. For example, if there is a cricket match, many people would like to access a site like cricket.com. When this website is accessed from a

machine for the first time, the web cache stores the web pages and its content in a storage device physically or logically near the user. Since most of the content resides near the user's machine, when the same user or another user accesses the website again on the same machine after some time, the time taken for the web pages to load into that machine would be very less.

How Web Caching Works

- (a) The user requests a web page from the URL.
- (b) After analysing the requests and considering certain parameters, the requests are re directed to the nearest local network cache.
- (c) The cache checks whether it has the requested a web pages along with its content. If it is not available then it again sends its own request to the original web server.
- (d) On getting the request from the local network cache, the original web server sends the web page and its content to it. The local network cache then stores the content in its local storage and sends a copy of the same to the user.
- (e) Later, when any other user requests for the same web page, the local network analyses the request and depending upon certain parameters redirects the request to the local network storage.

Uses of Network Caching

- (a) Cost reduction: Since the web cache is placed at tactical locations it is responds to requests very fast. Fast access does not require high bandwidth. This again means decreased cost.
- (b) Increase in Productivity: Response from the web server is very fast. The web page downloads very quickly when compared to the ones which do not have a web server.
- (c) They help administrators enforce security by a site wide access policy through URL filtering.
- (d) Operations: Network administrators can check out the URLs visited, the number of requests per second that the cache is serving, and how many URLs are going through the cache?

Types Of Cache

Proxy Servers

Proxy servers are software applications placed between client applications for instance between a web browser and a web server. It accepts all requests meant for the web server and checks if it can be done locally; otherwise it sends the same to web server.

A Proxy server is not the best option for caching and cannot work under heavy network loads. A Proxy server inspects all traffic that passes between a client and server. This makes the traffic all the more slow. Since the proxy requires configuration of each user's browser, it becomes a very costly and laborious task for Internet Service Providers and large enterprises.

Stand-alone Caches

Stand-alone caches have been designed keeping in mind the shortcomings of a proxy server.

The problem with stand-alone caches is that they are not network integrated and therefore incur high costs and are less attractive for large-scale installations.

Browser-Based Client Caching

Whenever the user accesses a web page, the browser stores the web page in the users local hard disk. The user decides on the amount of storage that he wants to dedicate for this purpose. So, when the user

accesses the web page next time, the browser gets it directly from the hard disk. Graphics such as logo, images and icons appear very quickly the second time.

Answer: [c] Stand-alones are expensive and require large-scale deployments.

Module:4

Reference No:M4087

Question: The use of multiple disks in Redundant Array of Independent arrays results in_____

- [a] Increased MTBDL (Mean Time Between Data Loss)
- [b] Decreased Fault tolerance
- [c] Decreased Fault tolerance
- [d] Striping

Module 4 -RAID (Redundant Array of Independent Disks)

Storage of information is one of the most important aspects of information management in an enterprise. With the emergence of Internet and other shared resources the storage requirements have skyrocketed. Several technologies have evolved to cater to the storage requirements of devices ranging from mainframes to personal computers. One such technology that has come to the limelight is RAID (Redundant Array of Independent Drives).

What is RAID?

A disk array is a combination of hard disk drives arranged in a computer so as to appear as a single unit. This gives a standardised method to store and retrieve data. These disk arrays are used as the basis for developing a technology aimed at enhancing storage performance. An approach to store the same data in multiple locations on multiple hard disks is termed as RAID. Also known as redundant array of inexpensive disks.

Principle

Data is loaded into multiple disks in such a manner so that input-output operations take place in a shared mode resulting in improved performance. Discrete disk drives are connected directly to a host computer system. In the case of RAID the data is spread across the system and parity data is also stored. This ensures that the failure of any single drive doesn't result in the loss of data. Storing the redundant data or error correction information separately from the data within the RAID array prevents data loss. Thus, the usage of multiple disks and storing data redundantly increases the Mean Time between Failure (MTBF) and fault-tolerance respectively. The additional bit of information stored along with the original data to make sure that the original data is reverted in the event of an error is called as parity.

Mechanism

A simple technique called "striping" is involved in presenting RAID as a single operating system. Striping is the act of partitioning the drives storage capacity. This partition is done on a sector of 512 bytes or up to several megabytes. The partition stripes capacity depends on the demand for a specific application.

Advantages

The three primary benefits provided by RAID are fault tolerance, data availability and high performance.

- **Fault tolerance:** The ability of a storage system or device to withstand a system failure without loss of data is termed as fault tolerance. Most of the disk crashes result in permanent loss of data. RAID ensures data redundant storage in other functional drives in order to reconstruct the original data lost.
- **Data availability:** It is the ability of a storage subsystem to sustain a component failure without loss of functionality. Fault tolerance is a driving factor here since, a failed storage component results in storage subsystem failure. The ultimate effect of component failure is the data-down condition or lack of data availability. Here reliability measurement is different as it is measured as Mean Time Between Data Loss (MTBDL). It is nothing but the mean time for a failure that will result in data loss or data unavailability.
- **High performance:** It is the ability of a storage system to perform input-output operations in addition to flawless high rate data transfers. The two categories of RAID systems namely independent access arrays or parallel access arrays ensure that high performance is delivered consistently.

Answer: [a] Increased MTBF (Mean Time Between Failure)

Module:4

Reference No:M4088

Question: Which of the following is not a part of the Global System for Mobile Communication (GSM) network?

- [a] Telecommunication standard Institute (ETSI)
- [b] Switching System (SS)
- [c] Base Station System (BSS)
- [d] Operation and Support System (OSS)

Module 4 -GSM (Global System for Mobile communication)

Evolution

The term "Cellular" is used for a telecommunication application that employs a low power transmitter whose frequency can be reused within a geographical area. Earlier, various systems had been developed without any standards and posed compatibility problems. The framework for GSM was laid down with the idea of ISDN compatibility for services offered and control signalling used. GSM is a radio technology that is digital in nature. The European Telecommunication Standards Institute (ETSI) in 1989 took up the responsibility for building GSM specifications. The first phase of specifications were drawn by ETSI in 1990. Since, then a number of digital technologies have been incorporated into GSM standards.

What is GSM?

GSM is a globally recommended standard for cellular communication, which deploys a digital mobile telephone system. A variation of Time Division Multiple Access (TDMA) is used in GSM, and is the most widely used among the three digital wireless telephone technologies (TDMA, GSM, and CDMA). GSM's digital radio technology permits synchronous and asynchronous data to be transmitted as a bearer service to or from an ISDN terminal. Data rates ranging from 300 bps (bits per second) to 9600 bps are supported by GSM.

GSM network

Three main elements that make up a GSM network are the

1. Switching System (SS)
2. Base Station System (BSS)
3. Operation and Support System (OSS).

Switching system

The switching subsystem performs subscriber related functions and call processing. Functional units operational here include Home Location Register (HLR), Mobile services Switching Center (MSC), Visitor Location Register (VLR), Authentication Center (AUC), and Equipment Identity Register (EIR).

Home Location Register: This register is a database of a subscriber's service profile, location address, and activity status. The data stored is of much significance as it is the permanent repository for subscription information.

Mobile Switching Center: The switching function of a telephone system is done by the mobile switching center. Call controls, network interfacing, toll ticketing and channel signalling are some of the other functions of the MSC.

Visitor Location Register: For the MSC to service visiting subscribers, a temporary database is needed which is provided by the VLR.

Authentication Center: This subunit has been incorporated to prevent the occurrence of fraud in mobile systems. The AC authenticates a user's identity. Encryption is also done by the AC to ensure confidentiality of the call.

Equipment Identity Register: This contains a repository of information on mobile equipment making it difficult for intruders to break into other networks/users.

Base Station System (BSS)

Base Station Controllers (BSCs) and Base Transceiver Stations (BTS) are present in the BSS. This unit caters to all radio related transmission and reception.

BSCs: All control and physical links between MSCs and the BTS is provided by the Base Station Systems. Radio frequency power level adjustments, and cell configuration for the base station transceiver are done by the BSC.

BTS: The Base Transceiver stations establish a radio interface with the base station. It consists of antennas and transceivers.

Operation and support system

The operation and support system is connected to all other subsystems and to the base station. The implementation of this system is referred to as Operation and Maintenance Support System. Controlling and monitoring of the network is carried out from this centralised location.

Answer: [a] Telecommunication standard Institute (ETSI)

Module:4

Reference No:M4089

Question: Which of these benefits is unique to CDMAone?

- [a] Capacity gain
- [b] Improved call quality
- [c] Enhanced privacy
- [d] Soft handoffs

Module 4 – CDMA (Code Division Multiple Access)

What is CDMA?

CDMA (Code-Division Multiple Access) is a digital interface standard, possessing eight to fifteen times the capacity of an analog cellular system. CDMA is a digital multiple access technique having a cellular aspect that is specified by the telecommunications industry. CDMA is a form of multiplexing which accommodates multiple signals in a single transmission channel for communication, thus making optimum use of the bandwidth. This technology is deployed in ultra-high-frequency (UHF) cellular communication systems between the range of 800MHz -1.9GHz bands.

Underlying technology

1. CDMA is inherently a spread spectrum technology. When information contained in a particular signal is spread over a much wider bandwidth than the original signal, it is referred to as spread spectrum technology. Conventional technologies allocate separate RF (Radio Frequencies) or channels for differentiating subscribers. In CDMA, unique digital codes are used to differentiate between subscribers. Both the mobile station/cellular phone and the base station share codes called pseudo-random code sequences. This separation brought about by a unique code enables all the users to share the same frequency band. The frequency of the transmitted signal varies according to the defined pseudo-random code. A receiver's frequency response that is programmed with the same code can intercept this. In this manner trillions of frequency-sequencing codes are generated which enhance privacy and make cloning difficult.
2. Analog to Digital conversion (ADC) is another technology that is used in CDMA. By using an analog-to-digital converter, audio input is converted into digital form binary elements. CDMA networks deploy the soft handoff scheme. Soft handoff refers to the overlapping of repeater coverage zones, so that every cell phone set is always well within range of at least one repeater (also called base station). This minimises signal break-up when a handset passes from one cell to another.

Benefits

Some of the advantages provided by CDMA One include:

1. Improved call quality with high fidelity sound, relative to analog systems.
2. Simplified planning of systems by using the same frequency in every sector of every cell.
3. Spreading of voice signals that enhance the privacy of the system.
4. Coverage characteristics are improved since only fewer cell sites are allowed.
5. Portable devices have an increased talk-time.

Variants

Some of the CDMA protocols that evolved over the years are:

1. CDMA One
2. CDMA 2000
3. WCDMA

4. CDMA One: This falls under the second-generation (2G) wireless network technologies. CDMA One was standardised by the International telecommunication Union (ITU) as an ITU IS-95 specification. The two versions of CDMA One namely IS-95 A and B vary in their usage of carrier frequency. IS-95 A uses the 1.25 MHz carrier and operates in radio-frequency bands of 800 MHz or 1.9 GHz, and supports data transfer rates up to 14.4 Kbps. IS-95B on the other hand can afford transfer speeds of 115 kbps by the simultaneous usage of eight channels to the maximum.
5. CDMA 2000: This figures in the third-generation (3G) of mobile wireless technology. Data communications at speeds ranging from 144 Kbps to 2 Mbps are covered by this standard.
6. WCDMA: Also known as IMT-2000 direct spread, WCDMA (Wideband Code Division Multiple Access) is a third generation (3G) mobile wireless technology. It offers much higher speeds for mobile and portable devices like Personal Digital Assistants (PDAs).

Answer: [d] Soft handoffs

Module:4

Reference No:M4090

Question: Which of these statements is true?

- [a] There can be only one internal perimeter router in a network.
- [b] There can be more than one internal perimeter router in a network.
- [c] An internal perimeter router distinguishes between a network under control and another that is not under control.
- [d] An internal perimeter distinguishes between the network and the ISP.

Module 4- Network Security Perimeter

While designing a network, it is important to frame a security policy. This helps in securing the contents and users from loss and damage. A network firewall installed in the organisation, helps in monitoring incoming and outgoing traffic, and imposes restrictions in accordance with the security policy.

Perimeter routers are installed between private networks, intranets, extranets or the Internet. The internal and external networks are protected by firewalls.

A network security policy concentrates on network traffic and conventions. It clearly states the domain of the user, his rights and responsibilities. It takes appropriate measures when policies are violated, and tactically enforces security on the user's boundaries. These boundaries are called perimeter networks.

Perimeter Network

Networks of computers, which are to be protected. They are referred to as trusted or untrusted:

Trusted network: A network present within the security limits of an organisation is referred to as a trusted network. This network often has confidential information related to the organisation. In consequence, the network manager has to prioritise its security and integrity. The networks are attached to the firewall server through adapter cards.

Untrusted network: A network, which is not defined within the security limits of an organisation, is termed as an untrusted network. It doesn't fall within the scope of the network manager, and he has absolutely no control over its administration, or enforcement of security policies.

A firewall server is established as a gateway for all communication between the trusted and untrusted network to provide better security at the perimeter. A network can have more than one network within it.

The relative position of each network is described with reference to three perimeters: the outer perimeter, internal perimeter and the innermost perimeter. The outer perimeter distinguishes between networks that are under control, and those that are not under control. A router is deployed at this point to separate the network from the ISP. The internal perimeter is relative to each network, and there could be more than one in a network.

The firewall placed between the internal and outer perimeter router gives additional protection from either side. It reduces the amount of traffic that the firewall server has to evaluate, which enhances its performance. The outermost perimeter is reserved for routers, firewall servers, and Internet servers, such as HTTP, FTP and Gopher servers. It is vulnerable to attacks, and intruders can gain access to internal networks.

The following aspects should be taken care of, while designing the network and security policies:

Cost: Security measures are assessed in keeping with various factors such as inconvenience, delay of work, which can in turn increase the administrative costs; it may also involve computing resources and dedicated hardware that are used.

Potential threats: The potential enemy has to identify different ways through which the network can be attacked; what could be the damage caused by such an attack; and then the security should be designed accordingly.

Secrets: Confidential information in an organisation such as username, password, encryption and the like should be closely guarded. Security systems should be designed, so that only a restricted number of people can access the information.

Identifying assumptions: Any assumption regarding the confidentiality of the information should be made after deliberation. For instance, the password accessibility of a particular application. However, a mistaken assumption can jeopardise the safety of the network.

Physical Security: Physical security of a system is also a priority. Physical access by an authorised person to a network link can allow him to tap that link, jam it or even inject traffic into it.

Answer: [b] There can be more than one internal perimeter router in a network.

Module:4

Reference No:M4091

Question: Which RAID (Redundant Array of Independent Disks) type makes use of embedded operating systems?

[a] RAID-3

[b] RAID-6

[c] RAID-53

[d] RAID-7

Module 4 - RAID:Types

Introduction

RAID is a method of storing the same data in multiple hard disks to enhance performance and fault tolerance. Nine types of RAID exist, in addition to a non-redundant array named RAID-0. Each type has inherent characteristics, which make it suitable for specific applications.

RAID-0

This level is termed 'striped array disk', and is without fault tolerance. The 'R' in RAID is eliminated, and it can be aptly called 'AID', since redundant data is not stored in level 0. Instead, data is divided into blocks, and stored next to each other in a sequential pattern. Typical applications of this level include file storage in video servers and the like.

RAID-1

Redundant array design is incorporated in RAID 1, whereby mirrored pairs of disk drives are present. A duplicate of the contents of one disk drive is mapped onto another. Due to this reason, it is referred to the 'disk mirroring drive'. There is no striping mechanism that partitions disks storage space. 'Write' performance is relatively slower than RAID-0, but 'read' is faster. In a multi-user environment, this level provides the best performance and fault tolerance.

RAID-2

A bit-oriented scheme for striping of data is introduced in RAID-2. Separate disk drives are employed to store each data bit in a sequential manner. Apart from this, the checksum is calculated for each word bit, and written into the error-correction drive. This is termed as Error Checking and Correcting (ECC) information. Input/output operations are slow for small files, as separate drives must be accessed for every operation.

RAID-3

This scheme uses striping, and allocates a drive exclusively for parity information. Mathematical functions involving logic gates (a functional electronic component) like Exclusive OR /XOR are employed. I/O operations have to cater to all the drives simultaneously. It involves high data-transfer rates, and is applicable to large files like video streams in a single user environment.

RAID-4

Data is processed as blocks, which reduces overhead processing and enhances data-transfer speeds. This level eliminates I/O overlapping as all 'write' operations update the parity drive.

RAID-5

A block-oriented approach similar to RAID-4, it involves storing of parity bits in a distributed fashion across the entire array. It enhances the 'write' performance since it includes a rotating parity array, which effectively addresses the limitation of level 4.

RAID-6

Apart from the parity scheme present in level 5, yet another scheme is introduced here, which provides high fault-tolerance and drive-failure tolerance features.

RAID-7

This level is like an inherent real-time embedded operating system that employs a controller. Here, caching of data is done by a high-speed bus, and it has the features of a standalone computer system.

RAID-10

This level consists of an array of stripes in which each one is a RAID-1 array. This provides better performance, but the cost involved is higher.

RAID-53

An array of RAID-3 stripes makes a RAID-53 array. Here too the performance is enhanced, but at a higher cost.

Answer: [d] RAID-7

Module:4

Reference No:M4092

Question: Which of these services offered by the GSM provides a personal security code to subscribers?

- [a] Short message service
- [b] Cell broadcasting
- [c] Advice of charge
- [d] Voice mail

Module 4 -GSM (Global system for Mobile Communication)-II

GSM, a standard for digital mobile communication systems, employs a variant of Time Division Multiple Access to achieve both synchronous and asynchronous data transmission. The *GSM* network consists of a number of subsystems. The functional systems in the network include the message center (MXE), the mobile service node (MSN), gateway mobile switching center (GMSC), and *GSM* internetworking unit (GIWU).

Message center: Integrating different data streams like voice and fax, and providing data messaging services are functions of the MXE node. SMS (Short Message Service), e-mail and voice mail notifications are also handled by the message center.

Mobile service node (MSN): Mobile Intelligent Network (IN) system services are attended by this node.

Gateway Mobile Switching Center: A gateway is employed to connect two networks. Implementation of this gateway is done at a switching center, which is referred to as *GMSC*.

GSM Internetworking Unit: A collection of hardware and software bundled together to provide an interface between various networks in a data communication network is the *GIWU*.

GSM services

The two basic types of services provided through the *GSM* include telephony and data. Telephony or teleservices are voice services that ensure complete communication between subscribers. Transmission of appropriate data signals between two network access points is done by the data services. Some of the other subscriber facilities provided by the *GSM* include the following:

Short message service: Messages having a maximum of 160 alphanumeric characters can be sent or received through a mobile station using the SMS facility of a GSM service. In case a subscriber's mobile is switched off, the service ensures that the messages are stored in an offline mode and made available to the user as soon as the he switches his mobile on. This holds good even in cases when the subscriber moves out of the calling area and re-enters it once again.

Dual-tone Multifrequency (DTMF): Control functions like remote control for the answering machine etc involving tone signalling schemes are supported by this DTMF service.

Cell broadcast: A variant of SMS through which a maximum of 93 characters can be broadcasted to all cell stations within a certain geographic limit. Applications include short messages about traffic congestion, accidents and the like.

Facsimile group III: A special fax converter is installed in the exchange to ensure compatibility with the analog system. Through this, conventional fax services can benefit from the use of GSMs connectivity.

Voice mail: A network level answering machine within the control of the subscriber is provided by GSM. By using a personal security code the subscriber checks for messages sent and stored in a network answering machine.

Additional Services

Some value added services come along with basic telephony and data services. These are aimed at generating revenue and fall under the GSM specifications.

Barring of incoming and outgoing calls: The service that allows blocking of either incoming calls to the subscriber or outgoing calls from the subscriber is available in GSM.

Advice of Charge: This includes two types of AOC services that provide a charge estimate for the mobile subscriber and includes the immediate bill for the calls and the estimate of the same.

Multiparty service: In the normal telephony connection, a closed simultaneous interaction between four to five subscribers is possible through this multiparty service.

Answer: [d] Voice mail

Module:4

Reference No:M4093

Question: Which feature gives Time Division Multiple Access the edge over other spread spectrum technologies?

- [a] Hierarchical cell structures
- [b] Extended TDMA
- [c] Elimination of interference
- [d] Reduced infrastructure costs

Module 4 -Time Division Multiple Access (TDMA)

What is TDMA?

In a multiplexing scheme, frequency bands available to the network are divided into time slots. When each user is assigned a specific time slot at regular intervals for transmission, it is known as Time Division Multiplexing.

This technology is used in digital cellular communication to effectively improve transmission signals. It allows three signals to be transmitted over a single channel. The TDMA standard for cellular phones divides a single channel into six time slots. Two time slots are used by each signal for transmission.

TDMA was first specified as a standard - Interim Standard 54 (IS-54), and IS-136 is an evolved version of IS-54. The standard has been incorporated into the European GSM standard, the Japanese standard of PDC (Personal Digital Cellular), Digital-American Mobile Phone Service (D-AMPS) and the Digital Enhanced Cordless Telecommunications (DECT).

How it works?

Audio signals are divided into small packets of digitised data. A single frequency channel is allotted for some time, and then the data is moved onto another channel. In this manner, a single transmitter sends digital packets that occupy different time slots in several bands simultaneously. The access technique used in TDMA allows three users to share a carrier frequency of 30KHz.

Advanced TDMA

Though TDMA improved the efficiency of analog cellular systems, an inherent drawback was the wastage of bandwidth. This meant that a specific time slot was allotted for a particular application like a conversation, without taking into account whether there was a conversation or not. An extended version of the TDMA standard known as ETDMA- Extended Time Division Multiple Access overcomes this limitation. Here, bandwidth is allocated dynamically on a need basis. ETDMA sends data through pauses or gaps that are part of normal speech. A buffer queue picks each bit of data sent by the subscriber for transmission, and allocates the bandwidth dynamically. When the subscriber has no data for transmission the buffer picks the data bit of the next subscriber in the queue. In this manner, wastage of bandwidth is avoided.

Advantages

Some of the advantages of TDMA include:

Many of the spread spectrum technology signals face a lot of interference during transmission. The use of TDMA ensures

that specific time slots are allotted for each user, thus eliminating interference from any other transmission. The subscriber benefits from extended talk time and battery life.

Maintenance and operational costs are minimum in TDMA. Further, base station equipment and infrastructure are nominal in

comparison with other cellular technologies.

It is cost effective to migrate and upgrade from analog to digital system.

Hierarchical Cell Structures (HCSs) are best utilised by TDMA technology, as it offers cell structures ranging from pico to

macro measurements. HCSs are aimed at customising the cells for effective utilisation of specific applications.

Service compatibility with FDMA based analog systems is possible with the use of dual-mode handsets. Dual band is used

for operations in the 800/1900 MHZ range.

Answer: [c] Elimination of interference

Question: What is Telecommunication Management Network (TMN)?

- [a] A set of standards for all networks
- [b] A set of international standards for telecommunication network
- [c] A programming language
- [d] A type of software

Module 4 – Embedded Telecommunication Management Network

Communication networks have increased exponentially, over the years. In consequence, a common standard is required to manage these networks effectively. It assumes greater significance in the light of embedded real-time applications.

What is a telecommunications management network?

An application that runs on a Network Element (NE) and provides the ability to manage the element with the help of some management system is termed as a Telecommunications Management Network (TMN) agent. To manage a telecommunication device employing a Real-time Operating System (RTOS), an embedded TMN agent is used.

What is a TMN agent?

A TMN agent resides on a board of shelves that is housed in an equipment rack, which in turn contains the network element. The boards are known as Shelf Control Units (SCUs) or Management Processing Units (MPUs). The agent runs as a real-time operating function, which is best suited for telecommunication networks. It does the function of performance management. Specific requests are sent from an application manager in a remote system.

Structure

Communication between the agent/ application and the manager takes place through a Common Management Information Protocol (CMIP), which is placed over the OSI (Open Systems Interconnection) protocol stack. CMIP is an object-oriented protocol for network management based on TMN recommendations.

Telecommunication equipment is used by network management systems to fulfill a number of functions, such as Operations, Administration, Maintenance and Provisioning (OAM&P). In the light of the TMN framework, these OAM&P includes configuration management, fault management, performance management, accounting and security management.

The TMN structural framework gives a pyramidal outline with the network element at the bottom and business management at the top. Between these are the element management, network management, and service management as it moves up the structure. The embedded TMN agent occupies the lowest layer of the pyramid in the network management layer.

Embedded telecommunication environment

Embedded system environment allows applications to be configured ,so that they can be executed for a predefined period of time, with a specific amount of memory space. An embedded system is preferred in telecommunications due to the following inherent benefits:

Embedded products are included in the telecom management package as debuggers and compliers. Though the developmental costs of these packages are high, the installation costs are low . This is because licensing costs are low for bulk installation.

Embedded packages can be tuned to different memory requirements and resources. Therefore, the main application is loaded into the ROM (Read Only Memory) and then into the RAM (Read Access Memory) for execution. This is because of the faster processing capability of the RAM. Special non-volatile RAMs like NVRAM that have a type of flash memory are used for this purpose.

More systems deployed for these applications because of the huge volumes of data that is processed. Only systems of small memory capacity like 32Mb to 8Mb are used.

Embedded telecommunication systems employ object-oriented technologies in the form of containment trees, which are nothing but a database of object instances.

Answer: [b] Set of international standards for telecommunication network management.

Module:4

Reference No:M4095

Question: What is the similarity between a GSM (Global System for Mobile Communication) network and EDGE (Enhanced Data for GSM Environment)?

- [a] Both use the TDMA frame structure
- [b] Both deliver a data rate of 384 Kbps
- [c] Both use the same transceiver unit
- [d] Both use phase shift modulation

Module 4 – EDGE: Enhanced Data for GSM Environment

EDGE is a technology that gives GSM (Global system for Mobile Communication) the capacity to handle services for third generation mobile telephony. With the help of EDGE, mobile Internet services are now available at three times the speed of GPRS (Global Packet Radio Switching) using. A new modulation technique with enhanced radio protocols that operating with the GSM is incorporated into EDGE.

What is EDGE?

It is a faster version of the GSM wireless service, which delivers multimedia and broadband applications to mobile phones and computer users. Data rates up to 384 Kbps are transmitted through EDGE. It is based on the GSM standard and employs the same Time Division Multiple Access (TDMA) frame structure, with a logic channel and a 200KHz carrier bandwidth.

Drivers behind EDGE

With the rapid growth in mobile Internet services, traffic is expected to increase exponentially. This will put high demands on an operator's mobile network capacity; more so because mobile Internet services are to be made available on a nationwide basis.

To cater to the growing coverage and capacity demands, need 2G and 3G networks need to be enhanced. EDGE will be the ideal choice for the existing infrastructure and GSM spectrum.

EDGE assumes significance for operators with GSM or GPRS networks evolving into WCDMA. With the help of existing and new infrastructure, interoperability between different parts of the network can be established. This will shape into a seamless network.

How it works?

The working principle of EDGE is primarily based on spectrum efficiency and capacity enhancements. Coding schemes, packet rates and faster services are the key attributes of EDGE.

Coding schemes: EDGE possesses nine coding schemes known as Modulation Coding Schemes (MCS). Four of these coding schemes use a GSM modulation technique, termed as Gaussian Minimum Shift Keying, which is easier on batteries.

The remaining five use a newer Phase Shift Keying modulation.

Packet rates: EDGE is capable of providing 384 Kbps of data transfer. New modulation techniques, error-tolerant transmission methods, and improved link-control mechanisms contribute to this higher data capacity. Enhanced applications such as wireless Internet access, e-mail and file transfer are provided.

Faster service: A normal TRU (Transceiver Unit) with three GPRS users delivers a data communication rate of 14.4 Kbps. If an EDGE-capable TRU replaces this, three EDGE mobile users using datacom can be combined into one time slot. This frees the remaining two time slots and enables three more users to use the facility. Therefore EDGE triples the capacity of a GPRS/GSM standard.

Implementation

For systems with GPRS implementation, the Base Station System (BSS) contains network parts that facilitate EDGE. EDGE-capable Transceiver Unit (TRU) plug-ins and some software updates are additional modalities that should be included. The transceiver units handle voice, GPRS and packet-switched EDGE simultaneously. The software required is downloaded remotely and existing cellular infrastructure are used.

Answer: [b] Both use the TDMA frame structure.

Module:4

Reference No:M4096

Question: Which SAN (Storage Area Network) architecture is most widely used?

- [a] Optical fibers
- [b] Fiber loop
- [c] Mainframes
- [d] Network attached storage

Module 4 - Storage Area Networks

What is a SAN?

A special-purpose high-speed network or sub network that connects different kinds of data storage devices having respective data servers is termed as a Storage Area Network. This in turn serves a large group of

users. SANs are part of an overall network of disks for storing data. They are also referred to as high-speed sub networks of shared storage devices.

SAN architecture

All storage devices are made available to all servers on a LAN or WAN. Any number of storage devices that are added to a SAN are also accessible from any server in the larger network. The server acts as an interface between the end user and the stored data. Since stored data does not reside directly on any of the network servers, server power is utilised for business applications and network capacity is released to the end user.

A SAN is usually set-up in close proximity to mainframes. It even reaches remote locations for backup and archival storage. For remote connections, Wide Area Network carrier technologies like Asynchronous Transfer Mode or Synchronous Optical Networks are deployed.

Infrastructure

SAN deploys available communication infrastructure like optical fibres. Newer fibre Channel technologies can also be included. Another scheme for SAN system integration is to use a common storage bus (the path for flow of data) in a computer, which is shared by storage devices like a hard disk and CD-ROM player.

SAN services

SANs support a variety of services like disk mirroring, backup and restore, , data migration from one storage device to another, and sharing of data among different servers in a network. SANs also incorporate sub networks with network-attached storage (NAS) systems.

Fiber loop

The term "Fabric" is used to refer to hardware that connects nodes and servers to storage devices in a SAN. The fabric enables connectivity through the use of Fibre Channel switching technology. One of the most widely used infrastructures for implementing SAN is a Fiber channel loop, also known as Fiber Channel Arbitrated Loop (FCAL). An FCAL configuration comprises servers, storage devices, and a Fibre Channel switch or hub. The Fibre Channel supports several configurations, which includes point-to-point and switched topologies. The Fiber Channel Access Loop provides high reliability in addition to high-speed interconnection between storage devices.

Advantages

SANs have the capacity for allowing additional bandwidth without burdening the main LAN. With a SAN, it is easier to conduct online backups dynamically without users feeling a bandwidth surge or pinch.

As storage requirements increase, additional drives are not required to be connected to a specific server. Instead, they are simply added to the storage network and made accessible from any point.

A SAN allows central management of all the devices connected to it. Storage is managed as a single entity and does not include managing the network on a per-device basis. Therefore, dealing with storage networks, consisting of hundreds of servers and devices becomes relatively easy.

Answer: [b] Fiber loop

Question: Which one of these features is specific to cross bar switches?

- [a] Direct control
- [b] Call supervision
- [c] Common control
- [d] Identification of path

Module 4 – Switches:Concept
What is a switch?

A switch is a network device that establishes a circuit or path for transferring a unit of data to its next destination. Switches also function as routers, (a device or program that determines the specific route for data in a network to be transmitted to its next destination). In the OSI (Open Systems Interconnection) model, switches occupy the Data Link layer, which is the second layer. Also, switches present in the third layer (Network Layer) are referred to as IP switches. Transistors having different configurations also work as switches.

Functions

In telecommunication, the main function of a switch is to provide a path for a call made by any subscriber. In order to process a call, the switch has to perform functions like identifying the subscriber, setting up the communication path, and supervising the call.

1.Identifying the Customer: In older telecommunication systems, customers were identified by the jack (a electrical component) position they occupied on a switchboard. Newer systems however, deploy electromechanical switches in which customers are assigned telephone numbers, which are also referred to as line or station numbers. With electronic switches, a telephone number is no longer wired to a specific component in the switch. The subscriber's cable line is terminated and cross-connected to the main distributing frame.

2.Establishing a communication path: The first task that the switch does while processing a call is to determine the type of call that is being made. The switch analyses the first digit (0/1) or the first three digits/prefix. This helps the switch determine whether the call is intraswitch or inter-switch. For an intra-switch call, the switch allocates a path called 'line', which is on line side of the network. In the case of an inter-switch call, the switch establishes a trunk path.

3.Supervising the call: The supervision function is transparent to the customer. Supervision is significant because it can have a direct impact on the efficient functioning of the switch.

Automatic Switching

The biggest limitation in a centralised network is that the originator no longer has any control over the call. The purpose of the electromechanical switch is to pass the control of the call back to the customer. Automatic switches of earlier days were of analog and electromechanical type. Automatic switches are either Step-by-Step (SXS) or Cross bar switches.

Step-by-Step Switch

The basic principle behind a SXS switch is that telephone calls progress in steps through switches. Each step is a response to dialing a digit.

SXS provides direct control.

The customer gains control over the common equipment used to process a call.

Cross Bar Switch

The common control feature is introduced in a cross bar switch. The customer /subscriber and the switch share control over common equipment used in processing calls.

A set of contacts called cross points make up a cross bar switch. These are arranged one on top of the other in a vertical bar structure.

Answer: [c] Common control

Module:4

Reference No:M4098

Question: Which of the following statements is not a benefit for using the Voice-over-Internet protocol?

[a] High quality voice

[b] Security

[c] Use of vocoder

[d] Use of TDMA

Module 4 –Voice Over Intranet Protocol

Introduction

The Internet protocol that has been customised for voice communications is now known as VOIP-Voice Over Internet Protocol. The introduction of the VOIP has come as a boon for low cost telephony, particularly for long distance communications. The major requirements for any communication network are reliability, quick access, multiple users, and high-quality audio, video and data transfer. An Intranet view of the VOIP would greatly enhance public safety.

Why have the Intranet in IP (Internet protocol) based VOIP?

VOIP through the Internet suffers from limitations such as slow access time, call priorities and poor security standards. An intranet design will enhance response times; provide higher network capacity, high quality voice and security for critical communications. The Internet uses packet switching technology. Here the conventional calls are converted into packet-based transfers using asynchronous transfer mode switches. The features that intranet based VOIP can provide have been elaborated as follows:

What is a vocoder?

An audio processor that captures the characteristic features of an audio signal and then utilises this signal to affect other audio signals is termed as a vocoder. This technology aims to synthesise speech. The frequency of a sound and any associated disturbances in it picked up by the vocoder analysis is known as the formant.

High-quality voice

A low-bit-rate vocoder is used in VOIP applications. It employs the H.323 telecommunications standard. This standard does not offer services like pre-emption or emergency calling, priority and group calling, which are inherent to public safety applications. Vcoders are designed for point-to-point voice telephony applications. This makes them unsuitable for use in moving vehicles or over low bandwidth radio channels. An intranet system with a special vocoder will ensure superior performance in high bit-rate environments, which are more appropriate for public safety mobile communications.

Security

The Internet is vulnerable to intrusion by hackers who can disrupt the communication channel. By operating in a private intranet system and deploying end-to-end encryption techniques security is enhanced in the

network. Compression techniques enhance the network's capacity to withstand increased voice traffic. End-to-End encryption is achieved through voice encryption over the air and over the packet switched network backbone.

Cost advantages Higher economies of scale and cost savings are possible. This is attainable since commercially available switching infrastructure and standard software are used

The IP architecture is a scalable one. This makes the process of expanding the LAN simple and easy

The distributed IP network can be expanded incrementally and economically

The IP based framework enables "plug and play" whereby integration costs are reduced. Thus, data applications on a wired LAN can be integrated and interfaced to a wireless application without using a middleware

TDMA (Time Division Multiple Access) technology can be used in VOIP to integrate voice and data. This offers significant cost savings over separate voice and data systems

Answer: [c] Use of Vocoder

Module:4

Reference No:M4099

Question: Which part of the Universal Mobile Telecommunication system (UMTS) network houses the ATM (Asynchronous Transfer Mode) standard?

- [a] Core Network
- [b] Radio Access
- [c] User Equipment
- [d] Mobile Station

Module 4 -UMTS: Universal Mobile Telecommunication System

Evolution

3G or Third Generation systems provide global mobility and a plethora of services ranging from telephony and paging to messaging, Internet and broadband data. The International Telecommunication Union (ITU) defines a standard for 3G systems, which are referred to as International Mobile Telecommunications 2000 (IMT-2000). The Europe European Telecommunications Standards Institute (ETSI) is responsible for UMTS standardisation. In 1998, the Third Generation Partnership Project (3GPP) came into being to continue technical specification work. UMTS is one of the most important 'third generation' (3G) mobile communications system developed within the framework defined by the International Telecommunication Union, and is known as IMT-2000.

UMTS Architecture

The UMTS system interacts closely with other systems in a telecommunication network. Other elements in a UMTS environment are:

- A UMTS system along with a satellite
- Public Land Mobile Network (PLMN)
- Mobile Services Switching Center (MSC) or Visitor Location Register (VLR)
- Location Area
- Routing Area
- UTRAN Registration Area
- Cell
- Sub cell

A UMTS network is made up of three interacting domains. They are- the Core Network (CN), UMTS Terrestrial Radio Access Network (UTRAN) and the User Equipment (UE). CN provides switching, routing and network management functions. UTRAN is related to air interface for user equipment.

Core Network

This network comprises both circuit and packet switched domains. Some of the circuit switched elements include Mobile Service Switched Center (MSC), VLR, and Gateway MSC. Packet switched elements include Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN). ATM (Asynchronous Transfer Mode) is defined in the core transmission of the network. Circuit switched connections are handled by the ATM Adaptation layer type 2 (AAL2), while the AAL5 caters to data delivery. Number Portability Database (NPDB) is employed to achieve compatibility while switching from older telephone systems to new UMTS standards,. The Gateway Location Register (GLR) is deployed to optimise subscriber handling.

Radio Access

The Base Station is referred as Node-B, and the control equipment used for Node-B is called Radio Network Controller (RNC). Wide Band CDMA is used for providing an air interface for UTRAN. WCDMA works in two modes namely, Frequency Division Duplex (FDD) and Time Division Duplex (TDD). The functions of Node-B includes the following:

- Modulation/Demodulation
- Air interface Transmission/Reception
- Error coding
- CDMA Physical Channel Coding

The functions of RNC include radio resource control, channel allocation, admission control, ciphering, power control settings, broadcast signalling and the like.

User Equipment

User equipment terminals function as an air interface for Node-B. They derive their roots from GSM specifications. The specifications are underlined below:

- Mobile Station ISDN (MSISDN)
- International Mobile Station Identity (IMSI)
- Temporary-Mobile Station Identity (TMSI)
- Packet Temporary-Mobile Station Identity (P-TMSI)
- International Mobile station Equipment Identity (IMEI)
- International Mobile station Equipment Identity and Software Number (IMEISV)

UMTS mobile station operates in Packet switched (PC)/Circuit Switched (CS) mode, PS mode, or CS mode.

PS/CS mode of operation: The condition by which the Mobile station is attached to both the Packet switched and Circuit switched domain, and is enabled to operate both PS and CS services simultaneously.

The PS mode of operation: The Mobile Station is attached to the PS domain with CS like services (Eg: VoIP) being operational.

The CS mode of operation: The Mobile station is exclusively attached to the Circuit Switched domain and similar services only.

Answer: [a] Core network

Question: Which feature in UMTS (Universal Mobile Telecommunication system) security is not derived from GSM standards?

- [a] Subscriber identity module
- [b] Radio interface encryption
- [c] Security against false base stations through mutual authentication
- [d] Subscriber identity confidentiality

Module 4 -UMTS:Services & Security

Introduction

UMTS is a Third Generation (3G) mobile system developed by International Telecommunication Union's International Mobile Telecommunications 2000 framework. The coverage for this mobile service is provided by a combination of cell sizes ranging from tiny Pico Cells to Global Cells. Satellites deployed for this system provide services to remote regions of the globe.

Services

A range of teleservices like speech, SMS and bearer services are provided by UMTS. These services rely on the capability of information transfer between access points. The services can either be connection oriented or connectionless for Point-to-Point and Point-to-Multipoint communication. 'Quality of Service' (QoS) defines a set of attributes related to the performance of a network and it is categorised into user and network oriented attributes. Different QoS parameters are available for maximum transfer delay, delay variation, and bit error rate for bearer services. Some widely used data rate targets include:

- 384 kbps for satellite and rural outdoors
- 144 kbps for satellite and rural outdoors
- 384 kbps for urban outdoors
- 2048 kbps for outdoors and in range

Four types of traffic exist for different QoS classes in a UMTS network

1. Conversational class (voice, video telephony, video gaming)
2. Streaming class (multimedia, video on demand, web cast)
3. Interactive class (web browsing, network gaming, database access)
4. Background class (email, downloading and SMS)

UMTS introduces the concept of a Virtual Home Environment (VHE) through its service, which is aimed at personal service environment portability between network boundaries and terminals. A personal service environment is one in which users are provided with the same personalised features, user interface customisation, and services, independent of networks, terminals or location. UMTS also provides location-based services.

UMTS Security

The security functions of UMTS are similar to that of Global System for Mobile communication (GSM). Stronger encryption algorithms are included in the base station, and the NODE-B to radio network controller (RNC) interface.

The main security features taken from GSM and incorporated into UMTS includes:

- Authentication of subscribers
- Subscriber identity confidentially
- Subscriber Identity Module (SIM)
- Radio interface encryption

Additional UMTS security features that were incorporated in the developed stage are:

- Encryption that was extended from air interface only to include Node-B to Radio Network Connection Security against using false base stations through mutual authentication
- Security data in the network was protected in data storages while transmitting ciphering keys and authentication data in the system.

Security Feature Groups

The five security feature groups that come under the UMTS specification include-

1. Network access security: A group of security features that enable users to have secure access to 3G services. This is more focused on protecting against attacks on radio access links.
2. Network domain security: A set of security features that help nodes in the service provider's domain to exchange signalling data securely, and safeguard against attacks on the wireline network.
3. User domain security: The set of security features that provide secure access to mobile stations
4. Application domain security: The set of security features that enable applications in the user domain and the provider domain to securely exchange messages.
5. Visibility and configurability of security: The set of features that enable the user to know if a particular security feature is in operation or not, and to assess if a specific service should depend on that security feature.

Answer: [c] Security against using false base stations through mutual authentication

Module:4

Reference No:M4101

Question: The size of a cell does not depend upon_____

- [a] The subscriber density
- [b] Demand in an area
- [c] The landscape
- [d] The subscriber's conversation time

Module 4 -Cellular: Basics

What is cellular mobile communication?

The term "cellular" is used to describe a telecommunication application that makes use of a low power transmitter whose frequency can be reused within a geographical area. The low power transmitters are used to create cells, which form the basic geographic area of a mobile communication system. The size of a cell varies according to the subscriber density and demand in a particular area. Cell sizes can be changed by applying varied power levels to existing cells.

Principles of Mobile communication

Each handset that provides mobile communication is termed as a 'Mobile'. These mobiles are set to various temporary radio channels to communicate with a cell site. Channels communicate with each other through a

pair of frequencies. One frequency is for transmission from the cell site, which is termed as 'forward link', and the other is for the cell site to receive calls from the user and is called 'reverse link'.

Cellular in Mobile communication

Conventional mobile systems faced a number of problems related to interference with channels in adjacent areas. Hence, the concept of frequency reuse was reconsidered. On further study, it became obvious that interferences were caused not because of the distance between areas but because of the ratio between the areas and the transmitter power/radius of the areas. It was found that a fifty percent reduction in the radius could show a four-fold increase in potential customers. The subscriber's conversations are handed from one cell to another to maintain a continuous phone service as the user moves between cells.

What are cells?

Cells are basic geographic units in a cellular system. Base stations transmit over Cells. Cell shapes may vary according to the landscape but are usually hexagonal in shape.

What are clusters?

A group of cells is known as a cluster. There is no channel reuse within a cluster.

Frequency Reuse

Due to the limited number of radio frequency channels available for mobile communications, there was a necessity to reuse frequency channels. The cellular industry standard came up with a solution called 'frequency reuse' or 'frequency planning'. Frequency reuse assigns a group of radio channels to each cell used within a small geographic area. This group of channels is completely different from the ones used for neighbouring cells.

A footprint is the coverage area of the cell. A boundary is set to limit the footprint so that the same group of channels can be used in different cells. Further, footprints making use of the same group of channels are placed away from each other so that their frequencies don't interfere.

Cells having the same number use the same frequency set. For instance, if the number of frequency channels available is seven, then the frequency reuse factor is 1/7. This means each of the cells use 1/7th of the available cellular channels.

Answer: [d] The subscriber's conversation time

Module:4

Reference No:M4103

Question: Which of the following modulation schemes does Orthogonal Frequency Division Multiplexing (OFDM) deploy?

- [a] Multicarrier modulation
- [b] Phase shift keying
- [c] Amplitude /Phase keying
- [d] Digital amplitude modulation

Module 4 –Orthogonal Frequency Division Multiplexing: Basics

Introduction

Orthogonal Frequency Division Multiplexing has wide spread application in a number of digital communication systems. OFDM has been adopted as the standard for Wireless LAN applications. A basic understanding of the concepts of digital messages, carrier waves, modulation, and multiplexing is essential to gain an insight into OFDM.

Digital Messages

Two remote locations exchange messages using radio waves that travel through free space. Messages ranging from raw data to voice, music, image and video are converted into the digital form comprising 1s and 0s (called bits or binary digits).

Carrier Waves

Electromagnetic waves that carry messages to some distance in free space are termed as radio signals or carrier waves. A carrier wave resembles a sine wave and propagates at the speed of light. The number of times per second that a wave goes up, down, and up again as it moves in a sinusoidal path is the frequency of the carrier wave. It is measured in cycles per second or hertz.

Modulation & Demodulation

The process in which a carrier wave of a particular frequency is modified by the message signal, so that the modulated carrier wave is used to carry the message over a distance. The process of splitting one high-speed digital message into several low speed messages is called modulation, and converting it back into a single high-speed message is called demodulation. Three basic kinds of modulation associated with digital signals are:

- Amplitude Shift Keying (ASK) or Digital Amplitude Modulation: the amplitude of the carrier wave is changed in a step-by-step manner in accordance with the message signal.
- Frequency Shift Keying (FSK) or Digital Frequency Modulation: the frequency of the carrier wave is changed in comparison with the message signal.
- Phase Shift Keying (PSK) or Digital Phase Modulation: the phase of the carrier wave is modulated to keep pace with the message signal.
- When ASK and PSK are used at the same time on one carrier, it is called Quadrature Amplitude Modulation (QAM) or Amplitude/Phase Keying (APK). The receiver is designed in such a way that it receives the carrier wave, detects the amplitude, phase shifts in the carrier, and thus recovers the original digital message. At the receiving end, this process is termed as demodulation.

Orthogonal Frequency Division

Frequency division is where each channel of communication is represented by a different carrier frequency. Orthogonal Frequency Division is where the spacing between the carrier signals is equal to the speed (bit rate) of the message. It is based on the concept of establishing a communications link using multiple carriers, each carrying an amount of information that is identical to the separation between the carriers. Here the carriers are spaced at the bit rate, in such a way that the carriers fit into the nulls of other carriers.

What is Orthogonal Frequency Division Multiplexing?

The scheme of using many carrier waves instead of one, and using each carrier wave for transmission of only a part of the message is called OFDM. It is also known as multi-carrier modulation (MCM) or Discrete Multi-Tone (DMT). OFDM is not regarded as a modulation scheme since it does not come in conflict with other modulation schemes. It is more a coding or a transport scheme for transmission. Top

Answer: [a] Multicarrier modulation

Module:4

Reference No:M4104

Question: Which of these wireless technologies deploys Radio Frequency (RF) for a WLL (Wireless Local Loop)?

- [a] Analog Cellular
- [b] Digital Cellular
- [c] Personal Communication system (PCS)
- [d] Proprietary systems

Module 4 -Wireless Local Loop (WLL)

What is a WLL (Wireless Local Loop)?

In a telephone network, a wireless local loop (WLL) is a generic term used to describe an access system that makes use of a wireless link instead of a conventional copper cable to connect subscribers to the local exchange. This is also known as Radio in the loop (RITL) or Fixed-radio access (FRA). The WLL system includes proprietary fixed radio access, fixed cellular systems and cordless access systems.

WLL implementation

Five categories of wireless technologies can be enablers for WLL implementation. They include:

1. Analog cellular
 2. Digital cellular
 3. Personal Communication Services (PCS) / Personal Communication Network (PCN)
 4. Cordless Telephone (II Generation) / Digital European Cordless telecommunications (DECT)
 5. Proprietary systems
- **Analog cellular:** The three main analog cellular systems employed include AMPS-Advanced Mobile Phone System, Nordic Mobile Telephone (NMT) and TACS-Total Access Communications System. Some limitations of analog systems are capacity and functionality. However, they find widespread application in low to medium-density markets/subscriber base.
 - **Digital Cellular:** Major digital cellular standards prevalent around the globe include GSM (Global System for Mobile Communication), Time Division Multiplexing (TDMA), Extended TDMA (E-TDMA), and Code Division Multiple Access (CDMA). Among these, GSM occupies the bulk of the market. Digital cellular can support a higher capacity of subscribers than analog cellular and is therefore used widely. Like in wired networks, new functionalities can be incorporated into the systems. The only limitation of these wireless technologies in relation to analog systems is scalability.
 - **PCS/PCN:** These systems incorporate both digital cellular and cordless standards in addition to Radio Frequency (RF) protocols. Using low-power antennas and lightweight inexpensive handsets, these systems deliver low-mobility wireless services.
 - **CT-2:** Cordless Telephone Systems between a handset and a base station were developed for small-scale and household business applications. This is not considered as a wireless connection since the base station is wired to the Public Switched Telephone Network (PSTN). When a public network provider gives a wireless service directly to the user and not through a wired line it is a Wireless loop. Scalability and functionality are enhanced in cordless systems. DECT provides a higher data carrying capacity, better voice quality and can carry a higher level of traffic.
 - **Proprietary systems:** Several technologies and configurations are available to construct these proprietary systems. They are however, not available in public wireless domains and are developed only for specific customised applications. Proprietary systems are positioned for basic fixed wireless telephony in low and medium-demand density applications.

Technical requirements

- Communications quality: WLL systems serve as access lines for fixed telephone sets. This makes it essential for WLLs to provide the same level of quality as conventional telephone systems. Various parameters that are considered are speech quality, grade of service (GOS), connection delay and speech delay. Since radio waves are used, protection of confidentiality and terminal authentication is another important consideration.
- Short construction period
- Low cost
- No interference from other wireless systems
- High traffic volume.

Answer: [c] Personal Communications Systems

Module:4

Reference No:M4105

Question: A peer-to-peer network works under _____

- [a] A centralised environment
- [b] A decentralised environment
- [c] Server control
- [d] All of the above

Module 4 -Peer-to-peer computing

In business processes, situations might arise where large amounts of disk space, bandwidth and computing power are needed. Peer-to-peer networks provide the answer to this need.

P2P (peer to peer) refers to a category of systems that allow multiple computers (peers) to share resources such as bandwidth, disk space and computing power in a decentralised environment. Clients use a P2P network to communicate with each other. P2P can act as a server too. P2P networking is also gaining importance in the areas of research, product development and investment. Benefits of P2P computing are:

It does not rely on centralised points and hence improves scalability of the process.

Increases cost effectiveness by allowing direct communication between clients.

Facilitates resource aggregation.

P2P application can obtain resources from anywhere in the network. For example, an application can get disk space from one place, and bandwidth from some other place in the network.

Requirements of a P2P network

Some of the criteria that are mandatory for a peer-to-peer system to run successfully are:

1. The network should use a standard set of protocols to communicate.
2. Secure information exchange should exist.
3. The network should support policy-based authorisation.
4. The network should facilitate specific and effective search.
5. The information network should be easy to use.

Characteristics of P2P

P2P business applications exhibit the following characteristics:

1. **Dynamic:** Peer-to-peer networks have made communication interactive, extensible and flexible. They also allow easy use applications, and computer systems and gadgets such as mobiles, cameras and printers.
2. **Real-time:** In certain cases, timely and personalised information is required on demand after a specific period of time. Although most of the communication in P2P network is immediate, store and forward techniques are adopted sometimes.

3. **Collaborative:** For a value added service, there should be proper coordination between the application and the users. This collaboration should be secure, should support multiple participants and enable the discovery of new network resources.
4. **Service based:** Integrating new or potential services into the existing system, devices and applications can help evolve new business applications and opportunities.
5. **Cost effective:** solving business problems by using P2P networks leads to reduced cost in a business process and also assists in maintaining better on-line relationships.

Problems with P2P

Some of the challenges of P2P networks are:

1. **Security:** Since P2P is decentralised, there is no centralised control over network.
2. **Burden:** Individual computers need to bear a heavy data burden.

Solutions

As far as security is concerned, P2P networks install servers to gain some hold on the security aspects. "Watermarking" is a security precaution, which involves authentication for a given part of the software. An inbuilt facility for encryption and algorithms allows the user to set their configuration safely.

Application of peer-to-peer computing

It is divided into three categories:

1. **Distributed file sharing:** Applications like the popular Freenet and Morphous allow P2P networks to share data with other members (peers) of the same group in an application-based virtual network.
2. **Person to person messaging:** Requires unique and quick identification of peers and fast updates of online users. This ensures the presence of on-line peers. Instant messaging systems such as jabber or yahoo messenger enables peers to exchange data.
3. **Distributed computing:** In a distributed peer-to-peer network, a node gathers information by computing raw data that is distributed across several processors in a network.

Answer: [b] A Decentralised environment

Module:4

Reference No:M4106

Question: The function of an access gateway is to:

- [a] Connect components in the same network
- [b] Access information for an end user
- [c] Connect one network to another
- [d] All of the above

Module 4 -Access Gateways

The Internet is a network of networks. Networks are often interconnected to provide information to the end-user. However, each network may work on a different set of protocols and standards. A Gateway is as an entrance point from one network to another. For example, an Access gateway connects telephone networks working under different standards and protocols. It also takes care of protocol conversion needed to interconnect these networks, so that message can be delivered easily over a TCP/IP network. There are several applications that use access gateways for connections between a telephone network and the Internet.

Applications of Access gateways

1. **User network interface and Switch trigger control** are implemented in an access gateway point between a telephone network and the Internet.
 - **User-network interface scenario:** Websites are sometimes used for telephonic applications. A website provides a better interface to the user than wireless keypads for searching and receiving wireless short message services, mobile telephone services, and for sending/receiving messages that can interact with website for the services using access gateways.
 - **Telephone switch trigger control scenario:** Integrating a telephone network and the Internet is beneficial because of the ability of the Internet to trigger the telephone switch. The ability to turn the trigger "on" or "off" for an individual subscriber is extremely important. Internet based applications can communicate with an access gateway to request a change in the status of a telephone network trigger for a specific subscriber. The access gateway then communicates with the appropriate telephone switch, via the SS7 network, changing the status of the trigger.
2. **Internet enhanced Call waiting**

When a subscriber is connected to an Internet Service Provider (ISP), incoming calls do not activate the subscriber's call waiting number i.e. the user is not aware of any incoming calls. However, after the integration of the telephone network with Internet, it is possible for the subscriber to be aware of incoming calls, while connected to Internet. Information regarding the call can also be displayed on subscriber's screen (monitor). This can be made possible through access gateways.
3. **Shared subscriber information and call/connection control across networks**
 - **Shared subscriber information:** Subscriber information on a telephone network is distributed to multiple locations and stored in different formats. In this scenario, the access gateway centralises information access by connecting the telephone network. This helps in sharing subscriber information. Access gateways act as a connecting point between two networks. They also act as a translation point for protocols used for information access on two networks.
 - **Call/Connection control across networks:** This application scenario focuses on controlling calls or connections on two networks. For small telephone switching system (from telephony side), control equipment like Computer Telephony Integration (CTI) is available. For medium to large switches Integrated Service digital network User Part (ISUP) signalling is used.

Similarly, the Internet also has connection control capabilities like Internet work Operating Systems (IOS), which guide routers, hubs and network devices.

Access gateways help in translating different signals from different networks. The Internet can provide voice call on telephone networks through access gateway protocol conversion.

Answer: [c] Connect one network to another

Module:4

Reference No:M4107

Question: Under normal conditions, which of the following offers the fastest connection to the Internet?

[a] Analog connections

- [b] ISDN
- [c] DSL
- [d] Cable

Module 4 -Internet Connection Types

The Internet has become absolutely essential for any organisation seeking to do business in today's global scenario. The bandwidth of the connection must be high enough for fast access to the Internet and most importantly, the reliability of the connection must be high to ensure low downtimes.

The various types of Internet connectivity suitable for most organisations can be classified as:

1. **Dial-up:** These connections can be further divided as Analog connectivity and Integrated Services Digital Network (ISDN). They need a telephone line and a modem to function.
2. **"Always on":** These connections are available round the clock and do not need any numbers to be dialled to access the Internet and are termed as broadband connections. The basic types are: Digital Subscriber Line (DSL), its derivatives and cable connections

Analog Connections

This is the basic type connection that is required for accessing the Internet and also the cheapest. This type of connection is possible even when there is a phone line only and hence can be used anywhere.

To use analog connections, the computer is connected to the phone line through a modem (Modulator-Demodulator). The modem converts the phone signals to signals, which the computer can understand, and vice-versa. The user has to dial-up to the Internet Service Provider (ISP), which allots him a connection to the Internet. When the user wants to log out, all he has to do is remove the connection. This is similar to making a phone call to another person.

The highest speed that can be achieved with an analog connection is 56 kbps (Kilo bytes per second), which is enough for accessing web sites that are textual in nature. For graphic and video intensive sites, the downloading is very slow and with an increase in the number of users connecting to the ISP.

ISDN

ISDN provides speeds of up to 128 kbps and also an error free service, since it is digital transmission. ISDN is also available in almost all areas where an Electronic Telephone exchange is available. However, a router that can understand ISDN needs to be installed at the user's end.

DSL

DSL also uses the telephone cables, but it is a broadband "always on" connection. However, it is very cheap and a fixed monthly charge is levied, irrespective of usage. DSL is becoming popular due to these factors and is available in most cities.

There are many forms of DSL, such as:

1. **Asymmetrical DSL (ADSL)** - It offers speeds of up to 8 Mbps for downloads and uploads of up to 1 Mbps.
2. **Symmetrical DSL (SDSL)** - It offers a constant rate of 1.54 Mbps for both uploading and downloading streams.

DSL is offered only when the location of the user is within 3.5 miles of the Telephone Company's Central Office. The benefit of DSL is that it is nearly 140 times faster than analog connections, 60 times faster than ISDN and 4 times faster than the T1 lines that are currently used by many organisations.

Connection through Cable

It is also a broadband connection offering always on access with speeds of up to 42 Mbps for downstream traffic and 10 Mbps for upstream traffic. The high speeds are possible since cable TV wires are used, which have high bandwidths compared to telephone line cables. Also, since cable television is mostly used in homes, it is generally available only in residential locations. However, a drawback of cable is that it is a shared connection and hence with increase in the number of subscribers, the speed tends to become slow.

Answer: [d] Cable

Explanation: Cable has access with speeds of up to 42 Mbps for downstream traffic and 10 Mbps for upstream traffic, faster than the other types of connections.

Module:4

Reference No:M4109

Question: The integrity of system cannot be lost due to

- [a] Trojan Horse
- [b] Packet Sniffers
- [c] Brute force attack
- [d] Firewalls

Module 4 -Network System Integrity

A network has to be protected from external threats like virus, intrusion, hackers and internal threats like pilfering and destruction of information. This apart, it is important to protect the integrity of the network, which ultimately helps in protecting the information content. This is because the security of network depends on the weakest link and not the strong one. Any instance of break down of integrity of a network may lead to high monetary losses, precious time and effort and can further promote similar attacks. Therefore, in order to maintain the integrity of network care is taken to protect the physical network, network software and other network resources. The computers and users are recognized and checked whether they are working within the realm of network and are operating properly.

Commonly tried methods of attack, to break the system integrity are as follows.

- 1. Network Packet Sniffers**

Packet sniffers generally give in vital system information like user account and passwords. The packet sniffers also provide information related to topology of network such as services provided by the network, number of computers in the network, which computer has access to which service and the like. The sniffers from the packets that flow through the network deduce the above stated information. When an external user gains access to a system-level user account, the attacker can create a new account any time he wants and use the network resources. It is possible for the network packet sniffer to inject new information or change existing information in a packet that can shut down the system or network connections.

- 2. IPSpoofing:**

IP spoofing also gives critical information about the user accounts and passwords. With IP spoofing it is possible for the attacker to send emails to the business partners or clients and make it appear as if sent by the organisation itself. These are generally done by combining simple spoofing attacks with that of message protocols.

- 3. Password Attacks**

Similar to packet sniffing and IP spoofing, password attacks like the brute-force password attack give in easy access to the accounts and network files and services. The brute force uses a dictionary program to enter all the combinations for a password. An example could be modifying the routing

tables of the network that may lead to transmitting to network packets to the attacker instead of the destination. The attacker could also monitor the network traffic.

4. **Denial of Service**

It is implemented using common Internet protocols, such as TCP and Internet Control Message Protocol. They try to take advantage of overall weakness of the system's architecture instead of software bug or security loophole. It can also involve overflow of unrequired information to the network, thereby giving wrong information about the status of network resources.

5. **Application Layer Attacks**

The application layer attacks can be done in different ways.

Trojan Horse attacks: In a Trojan horse attack, the attacker substitutes different programs from the commonly used programs. For example, it displays a screen, banner, or a prompt that looks similar to the user. It then captures the information fed in by the user such as username, password and the like and passes the same to the attacker.

Recent forms of application layer attacks take advantage of openness of new technologies like Hyper Text Markup Language (HTML) specification, web browser functionality, and the HTTP. These attacks involve passing harmful programs across the network and then loading them in user's browser.

Answer: [d] Firewalls

Module:4

Reference No:M4110

Question: Which of the following is false related to watermarking?

- [a] It embeds copyright information in the object
- [b] It is sufficient to prove the ownership of the article
- [c] It should be invisible
- [d] It identifies the user with the help of a serial number

Module 4 -Watermarking and Fingerprinting

Rapid strides in Information Technologies have made communication easier, more so with digital advancements. But distributing copies of information via digital media result in heavy losses to the original creator, considering his investment in terms of time and money. So a definite mechanism is required to control such unfair practice. This would help in building a global commercial information infrastructure.

The digital media used for this purpose could be text, picture, audio, video and so on. A few mechanisms, which help in giving copyright to the recipient of the information and that discourage data piracy are watermarking, fingerprinting and digital signatures.

Water Marking

Watermarking is a technique whereby copyright information can be secretly attached to the digital object. Such information, which includes details related to its ownership, usage and the like, acts as a valuable evidence to prove one's ownership. Though quite effective, this method is not without drawbacks.

- The watermark is not safe and foolproof. It can be subjected to attacks and can be forged.
- The ownership of an object cannot be simply proved by the watermarks. It has to compulsorily involve a trusted third party to prove its authenticity.

Security In order to make it more secure, water marking is done throughout the digital object without interrupting the normal usage of the object. This allows for detection even when only a small part of object is being taken. Therefore it is advisable to have robust watermarks, i.e., strong enough to bear the routine transformations to digital object, such as compression. Weak watermarking techniques limit its scope.

Fingerprinting

The fingerprint is a type of user identifying watermark. The fingerprint identifies the authorised user with the help of "a serial number" assigned by the vendor. This is meant to restrain the illegal redistribution of the data by the original buyer of the object.

This process gives the identity of the person who was originally given the copy, who in turn provided the same to a third party.

Essential features of watermarks

- The watermark should be very robust and should not be easily removable.
- In a document, which already has a watermark, it should be very difficult to add a new watermark.
- It should be strong enough to subsist routine transformations like filtering, compression, re-sampling, cropping, channel noise, and other related activities.
- It should interrupt the normal working of the object.
- It should be preferably invisible, to retain the proof of illegal copying.

Answer: [d] It identifies the user with the help of a serial number

Module:4

Reference No:M4112

Question: Security assessment of capability levels does not involve:

- [a] Firewall rule set
- [b] Application server Configuration
- [c] Manual inspection
- [d] Eliminating the incorporation of security architecture

Module 4 -Security Assessment Methodology

When assessing the capability levels of security architecture three important features are taken care viz. planning, deployment and configuration and operational phases.

The methodology is carried out in different phases.

Discovery Phase

In this phase the documentation related to the security architecture is thoroughly re-evaluated. The documentation would include security policies, standards, guidelines, information classification and access control plans and application security requirements. Infrastructure security design as a whole is also required, which includes network partitioning design, firewall rule set, intrusion detection configuration, the application server configurations and the like.

Manual Inspection

Manual inspection is done in the second phase.. Here the documented architecture is compared to the actual one. There are chances of discrepancy between the documentation and the actual architecture. This can be

done using either manual or automated methods. Details pertaining to network and platform discovery tools, network paths, host operating system types and version number are obtained. Tools like NMAP can be used to scan all the ports on a host and identify the type of device and version of software.

Vulnerability Test

This phase determines the adequacy of security measures, identifies security deficiencies, and evaluates the effectiveness of existing and planned safeguards.

It starts with a network, platform and application vulnerability test, which is done to inspect the system from the attackers point of view. This can be done in different ways like within the organisation's intranet or externally from the Internet, an Extranet partner inbound to the organisation. Tools used in vulnerability are mixture of commercial tools like ISS scanner and Cisco Net-Sonar and publicly available tools like Nessus and NMAP. The method of working is similar to all the vulnerability tests are:

1. The testing starts with scanning of all the network ports on a given component like firewall, router, VPN and the like. On detecting an open port, all the known exploits are tried on them.
2. Platform scanning: The platform scanning or system scanning is then done to verify whether the configuration is compliant with a given security policy. It checks security vulnerabilities, mis-configurations and exploitable network services. On determining a secure build, a base line is formed, which is monitored at a scheduled time to detect any considerable changes.
3. Thirdly, application scanning is done, which is generally a manual process. This is done to stimulate a situation how the attacker would try to exploit the application when authorised
4. The last phase is done to include the process portion of the security architecture consisting of automated alerting facilities that depend on the person responsible for configuration of all the security architecture components like firewalls, Intrusion Detection Systems.
5. Following points are to be taken care of while doing the vulnerability test.
 - Security architecture monitoring and alerting facilities should be full of activity.
 - Security logs should be cleared to allocate disk space.

The above points are combined and analysed as overall risk analysis document.

Answer: [d] Eliminating the incorporation of security architecture

Module:4

Reference No:M4113

Question: While planning for the security of the organisation

- [a] Old policies should never be followed
- [b] The statements in the documentation should be abstract for quick understanding
- [c] Information classification and access control should be of more importance than password management
- [d] The security policy could be treated as optional to be provided to the employees

Module 4 -Security Maturity Model

A Maturity model measures the capability and effectiveness of an organisation's software, hardware and system. The security assessment methodology requires analysing three important aspects: the planning, the technology and configuration, and the operational processes.

The security architecture has four capability levels.

- **Level A:** Not Effective (50 Percent)
Here the security architecture does not address the corporate security policies, regulatory concerns, and best business practices.
- **Level B:** Requires Improvement (65 Percent)
The security architecture is not effective and is very less (35 Percent).
- **Level C:** Adequate (Up to 85 Percent)
Corporate security planning, deployment, configuration and process controls and other goals of security architecture are met.
- **Level D:** Excellent (More than 100 percent)
The planning, deployment, and configuration and process controls, which are the important aspects of security assessment methodology, are exceeded.

Security Planning

An organisation can face many problems while framing its security planning. The planning document must be carefully written and should be absolute. The problems could be any of the following:

- The policies could be very old and therefore not suitable for application at present time. Policies should therefore be updated annually to be inline with technology.
- The statements in the document should not be very abstract and in turn should be very comprehensive. This is because developers, risk managers and auditors use the documents and could therefore be interpreted in different ways.
- Most of the organisations feel that its security depends on password management. They should go beyond this and start working on information classification and access control planning document.
- The users should be made aware of the security policies, which should not be locked from being accessed. Rather, it should be posted in the intranet site. This because if the employee is not aware of the restrictions pertaining to browsing the net, during the office hours, he cannot be held responsible for it.

Technology and Configuration

Today, we find innumerable security vendors and products. But the fact is not one of them provide 100 percent security solution. Instead most of them are point solution like firewalls, intrusion detection systems, authentication servers and the like. These solve only a limited set of problems. The organisation should carefully select a set of products, install correctly in the infrastructure, configure appropriately and support them.

For instance, some organisations feel installation of a firewall would give 100 percent protection. This is partly true from the network point of view. But it cannot protect the applications, provide platform protection and cannot give the information regarding intrusion detection.

Operational Process

The operational Processes involve the support and maintenance required by security components, which are more or less similar to the support required by the mainframe and application servers, Change management, business continuity, security awareness training, and security alerting and monitoring. The security tools require a good configuration, which is generally very complex task. A security awareness program should include custom prepared newsletters, custom and commercially available video presentations, security awareness days, posters and the like.

Answer: [c] Information classification and access control should be of more importance than password management.

Module:4

Reference No:M4114

Question: In an Internet URL, "http://www.themanagementor.com", what is the use of .com?

- [a] Identifies the protocol being used
- [b] Identifies that the site is on the Internet
- [c] It is an additional information and is not needed
- [d] Identifies the purpose of the site. It stands for "commercial"

Module 4 -Hyper Text Transfer Protocol (HTTP)

Did you ever think how typing "http://www.themanagementor.com" in your browser's location bar gets you the web site? This article explains the above address, called a URL (Uniform Resource Locator).

http is the protocol being used. Http stands for Hyper Text Transfer Protocol and is the common protocol for the Internet. The protocol is the method or procedure for transferring information.

www means the site can be found on the World Wide Web, which is part of the Internet. On modern browsers, www is automatically taken as default and hence can even be left out.

Themanagementor is the name of the host or domain, and also sometimes called an alias.

.com is the type of domain or site and com stands for "commercial enterprise." Other domain types are **.gov** (U.S. government), **.mil** (U.S. military), **.net** (network), **.edu** (educational institution, university), **.org** (an organization).

These are known as top level domains (TLDs). There are also several other sub domain types and each country has its own domain code (i.e., .in is India, .ca is Canada). Some other TLDs have been recently introduced, such as, .museum, .info etc.

What is the difference between HTTP and HTML?

HTML stands for Hypertext Markup Language. The document in web browsers is written in HTML. HTTP is the protocol transfers this HTML document to your browser window. HTML contains text to be displayed and tags that tell the browser how to display them. In the previous sentence the word "tags" was italicized. Within the HTML document the word "tags" is enclosed in tags that look like this: < I >tags< /I >. The < I > tells the browser to begin italicizing text and the < /I > tells the browser to stop italicizing text.

Every web site, whether it displays it in the location bar or not, has a default HTML page called "index.html". For instance, the default page of http://www.themanagementor.com is "http://www.themanagementor.com/index.html". Typing in the two different addresses produces the same result. However, we can configure web servers to accept default homepages other than index.html by proper configuration. Some of the most commonly encountered home pages other than .html are default.html, home.html, index.asp, index.jsp etc.

HTML is sometimes spelled HTM. This is because some systems do not recognise more than three letters in a document file extension. The page index.html is not the same as index.htm.

.HTML is a type of file name like .doc is a MSWord document, and .txt is a text document.

Slashes in URLs?

The address of a page other than the home page is typically like the following URL:

http://www.themanagementor.com/icaai/articles/sampletest.asp, where:

1. //themanagementor is the name of the host domain.
2. /sampletest.asp is the name of the document you are viewing.
3. /articles is the name of the folder the document is located in.
4. /icaai is the name of the folder that the "articles" folder is located in.

Each folder is separated by a slash.

Networks on the Internet can be configured in many different ways. Internet addresses can be termed as "hosts" or "domains" or "aliases" or a variety of other names. Different numbers can be used to uniquely identify computers. For instance, Serial numbers, Ethernet address numbers, TCP/IP addresses and others. These numbers are long, difficult to remember and all look the same after a while. In order to make thing simpler, names are assigned so that it is easy to identify computers. These definitions may clear up some of the confusion:

Host

A host computer is typically the central server on the network. Early computer systems consisted only of "dumb" terminals, connected to a server that stored all the files and applications. The terminals had only communication facilities to access the host. Most computer networks now consist of several hosts to handle email, printer management, network security and file management. Remote users can Dial-in to hosts from personal computers over public telephone lines. In Internet jargon, a host is a computer that stores the files or applications shared over the Internet.

Domain

A domain name is a name in user-friendly format for a network of computers or services on one computer. For instance, the domain Yahoo has network of computers that can be accessed through the name www.yahoo.com.

Server

A server is a specially configured computer that provides a service to users. An Email server provides email service. A Web server can provide Internet access from within a network or Web site access from outside a network. These machines are usually protected or separated by a firewall.

A web server may have several aliases. A company's files may be accessed through the Internet at the address www.company1.com, but the name of the machine within the company's walls may be, say, Computer1. Company1 may then allow another company called Company2 to put up their site (for instance, www.Company2.com) on the same Computer1 system. Company1.com, Company2.com and Computer1 are all aliases for the same computer.

Client

The client to a web server is usually a "web browser" or simply, a browser. The browser requests the Web server for a particular document and displays it correctly to the user.

The HTTP Protocol and the GET Method

Assume that a user enters into browser, <http://www.yahoo.com/index.html>. This request is made to the server using the GET method. The user (client browser) makes a request to GET the document index.html. It looks like this:

```
GET /index.html HTTP/1.0
```

The server then returns to the browser the file requested, i.e., index.html. The browser then parses (converts) the HTML syntax and presents the data in a format that the user understands.

Answer: [d] Identifies the purpose of the site. It stands for "commercial"

Module:4

Reference No:M4115

Question: Satellite communications cannot be used in which of the following cases?

[a] Unencrypted Confidential data is to be sent

- [b] Mobile Communications
- [c] In case of natural calamities
- [d] Communication in rocky areas

Module 4 –Satellite Communications

Till the advent of satellites for communications, long distance transmission was possible either by using undersea cables or by antennas mounted on tall towers and spaced at regular distances.

This limited the range and effectiveness of communication. The advent of satellites was the turning point in the growth of Telecommunications as a discipline by itself.

Satellites are of many categories. A Communications satellite is defined as any spacecraft orbiting the earth at a pre-defined height and provides radio-frequency communications.

Introduction

Early Satellites were just like towers on the ground in that they acted as repeaters; they reflected the signals back to earth and hence reflections were in all directions. As technology progressed, powerful satellites with sophisticated equipment for receiving, storing and transmitting data only to specific ground stations were launched.

The first passive satellite was Echo 1, launched in 1960, while Score was the first active satellite launched later. Today, there are hundred of communications satellites in orbit around the earth. For error-free communication, the signals have to be transmitted in such a way that they do not overlap with one another. Hence, separate frequency bands have been allotted for different purposes. Frequency of transmitted and received signals is measured in "Hertz" (Hz), equivalent to cycles per second.

For instance, 6 Giga Hertz (GHz) of bandwidth is necessary for satellites to receive information (uplink) and 4 GHz for transmission (downlink). Mobile stations use a small band of 1.5 GHz as on ships, vehicles and aircraft communications.

Types of Satellites

Satellites used for remote sensing are generally of two types:

1. **Geo-stationary or geosynchronous**, i.e., stationary with reference to earth at about 36000 km altitude
2. **Polar orbiting**, i.e., orbiting the earth at about 1000 km, generally in the north- south direction with a little inclination to make it cover an area which is constant and uniform illumination from the sun and providing coverage over different parts of the earth repetitively

It must be noted that most of today's communications satellites follow the geosynchronous orbit, which provides continuous communication between the ground station and the satellite.

Services Provided by Communications Satellites

The cost of providing communication services has decreased due to recent advances in Technology. One reason for this is that the cost for transmitting any single message is the same for any distance. Further, the error in this type of communication is very low. Hence the number of services being offered and the quality of service has increased dramatically in the past few decades. Some of the services being offered are:

1. Global broadcast of Television programs
2. Programs for cable Television and for Dish antennas
3. A type of digital communications using Very Small Aperture Terminals (VSATs) is being used for business
4. Increasing capacity and quality of Telephone services due to improved digital source coding techniques

The INMARSAT (International Mobile Satellite Organisation) is an international communications network, providing telephone, Fax, ship-to-ship, Ship-to-Shore and aircraft communications through a digital link.

From a security viewpoint, it is not advisable to use satellite communications, since anybody tuning to the correct frequency can receive the transmitted data. Only strong encryption, if used, can make satellite communications safe and private.

Uses of Satellites

The delay for communication between two stations on the ground is a fixed 540 milliseconds (270 msec for upward transmission and 27 msec for downward transmission). Fibre optic cables, on the other hand, are much faster and hence are preferred for land-based communications. However, satellites can be used in situations where fibre optic cables cannot be used:

1. For Mobile Communications at sea and air
2. For situations such as natural calamities where a message has to be sent to all stations
3. For communication where it is not feasible to lay cables, such as rocky areas or between islands

Answer: [a] Unencrypted Confidential data is to be sent

Module:4

Reference No:M4116

Question: Which of the following provides mobile user network access over an air interface in Wireless IP?

- [a] Core network
- [b] End-user Services Network
- [c] Radio Access Network
- [d] GSM

Module 4 -Wireless IP

Wireless Technology has become an established industry. With the traditional connections through physical connectivity giving way to mobile communications, the next step is to bring wireless into the Internet.

WAP and Bluetooth have already achieved this to some extent, but the full power of the Internet will be evident when the underlying protocol TCP/IP is changed to address issues in wireless.

The new wireless-based architecture will be peer-to-peer packet-switched networks rather than the current circuit-switched topology.

The new wireless IP architecture is expected to provide the following major benefits over current implementations:

- Provide a better experience for the end-user through easy customisation, speedy access and rich content. The full range of multimedia services such as video and voice must be present.
- Provide a smooth shift from existing architecture without any hiccups or glitches.
- Provide the same functionality for Internet-based applications through wireless as through cable. All services currently running on the Internet must be accessible and with superior performance. New applications must simultaneously be available to both the communication media.
- The Total Cost of Ownership (TCO) must be reasonable for vendors, so that it is financially feasible for them to undertake the venture.

The wireless architecture consists mainly of three layers:

- Radio Access network

- Core network
- End-user Services network

The existing networks such as the Internet, Plain Old Telephone System (POTS), ISDN, SS7 signalling, Global System for Mobile communication (GSM) are compatible with the second layer, i.e., the Core network.

Radio Access network (RAN)

This network is responsible for providing the basic services for the user to connect and use the resources of the other two networks. In short, the basic transmission, radio control and management tasks are taken care of by this network. It also converts the signals transmitted through air into packets that the computers can understand.

Core Network

This constitutes the heart of the whole system. It provides the necessary functionality for linking the wireless users to other networks such as the Internet through internetworking gateways. It also provides the interface for the RAN and adds mobile device management, security management and signalling functions. This network is designed to be independent of the method of access. IP is used for control and transport. Similar to cable access, clients like browsers will be able to interface between the end-user and the core network, making the user feel familiar about the system. A user may have several sessions on simultaneously, allowing an "always-on" effect to the user.

End-User Services Network

The end-user services network provides functionality similar to the "application" layer in traditional networks. Services such as Internet connectivity, news, video, audio and other information will be provided by wireless network operators, Internet Service Providers (ISPs) and third-party content providers. Since these services will be provided through mobile platforms, users can have the benefit of these services while being free of the necessity to stay at a physical location.

Answer: [c] Radio Access Network

Module:4

Reference No:M4117

Question: Short Message Service (SMS) cannot be used to provide which of the following services?

- [a] Notify a user if new email comes to user's email account
- [b] Inform a user about news headlines or weather
- [c] Provide transmission of short messages between two users
- [d] Display a graphic-rich web page

Module 4 -Short Messaging Service (SMS)

Short Message Service (SMS) is a wireless service that can deliver messages consisting of alphabets and numbers between mobile users and other systems such as email, pagers etc.

SMS was first introduced in 1991 in Europe and was part of the Global Standard for Mobiles (GSM) digital wireless technology.

In the United States and the rest of North America, SMS was available only on certain digital wireless systems built by companies like BellSouth Mobility. Then sophisticated technologies for Personal Communication Services (PCS) such as GSM, Code Division Multiple Access (CDMA) and Time Division Multiple Access (TDMA) brought SMS into full deployment.

SMS is a point-to-point technology that allows short messages to be transmitted from one wireless handset to another. A SMS Centre (SMSC) relays messages to and from between the handsets in a store and forward manner.

What then is the difference between paging services and SMS?

The difference lies in the way SMS messages are transmitted. Any message sent through SMS is guaranteed to be delivered, unlike paging services. If the network experiences temporary failure, then the message is stored at a SMSC and then delivered when possible. Another feature is that a user is able to send or receive a message at some time, irrespective of whether he is busy or not.

Elements of SMS

The main elements of the SMS are:

- **Short Messaging Entity (SME):** The terminal at the user end. It may be a fixed system, a mobile or handheld device or located at another SMS station. It is responsible for the transfer and reception of messages.
- **Short Message Service Centre (SMSC):** The Centre stores and forwards the messages between a SME and mobile station

Applications of SMS

Some potential applications of SMS are:

- **Notifications:** Through SMS, if a user receives email, voice mail or fax in his inbox, they can be notified by the service provider. Another interesting use is that of providing calendar/scheduling services, where a subscriber is notified of appointments and other reminders.
- **E-mail:** Existing email protocols such as SMTP etc can be modified easily to allow SMS to provide two-way communication of short messages.
- **Paging:** Integrating Paging with SMS would allow existing wireless users to use these services through a uniform interface.
- **Information Services:** Information that is relevant to a subscriber can be delivered automatically without requiring him to search for it. For example, weather, news, stock quotes etc can be transmitted through SMS.

Issues

In spite of many organisations assuring people that transactions over the web are secure, most people are quite paranoid about making purchases or banking on the Internet. Commerce through wireless devices will take a lot of research and development before it becomes commonplace. In SMS, security is more complex than its wired counterpart. Since the SMS message first is transmitted to the Short Message Service Centre, or SMSC, which is operated by the cell phone service provider, then transmitted to the mobile switching centre (MSC) and finally the Base Station System (BSS). Security must be strengthened adequately in all these places, since leaving a small hole anywhere can compromise the whole system.

Some other issues that have to be addressed are that SMS technology must work with the different and often mutually incompatible protocols and should integrate seamlessly with the existing networks. Mobile devices at the user ends also have to undergo a lot of improvement. User interfaces such as keypads are currently not so friendly for typing messages rapidly.

Answer: [d] Display a graphic-rich web page

Module:4
Reference No:M4118

Question: Which of the following features in Internet Information Server (IIS) 5.0 from Microsoft logs the CPU resources consumed by Web Services?

- [a] Application Protection feature
- [b] Centralised Administration
- [c] Kerberos
- [d] Process Accounting

Module 4 -Internet Information Server (IIS)

The Internet has changed the way business is done. If any organisation does not have a presence on the net, it loses its competitiveness. With this growing dependency on the Web, it becomes imperative to have a web site that is secure enough to do business on.

This security of the web site is dependent to a large extent on the Web Server that is running the web site. Microsoft's Internet Information Server (IIS), first introduced with Windows NT is a robust, enterprise-scale Web Server that runs many web sites today.

The latest version is IIS 5.0, shipped along with Microsoft Windows 2000 Operating System, and runs as an enterprise service under the OS.

The major improvements in IIS 5.0 over its previous versions lie in four major areas:

1. Reliability and Performance

If any problem occurs with IIS, it can now be restarted without restarting the Operating System. The "Application Protection" feature allows applications to be run in a pool and in a memory area different from the web services and improves reliability. This feature applies to the operating system process under which the applications are run. In earlier IIS versions, all Internet Server Application Programming Interface (ISAPI) applications ran in the same memory space as the server. This enhanced performance, but if one application or even an ASP script misbehaved, it took the entire server and other applications down with it.

IIS 4.0 allowed the applications to run along with the web services or run separately. IIS 5.0 provides one more option: running applications in a "pooled" process separate from the Web services. The CPU Throttling and Socket Pooling feature in IIS 5.0 can further increase reliability and performance.

Web developers can use script-less Active Server Pages (ASP) and other enhanced ASP features to deliver dynamic content on the web site.

2. Management

Installation and maintenance of IIS is now easier due to:

- *Centralised Administration:* Administration in IIS 5.0 is now managed through the Microsoft Management Console (MMC).
- *Remote Administration:* IIS 5.0 provides for Remote administration through two ways, from a browser or by using the MMC. However, using the MMC has a few drawbacks. It requires that Windows 2000 be installed on the remote system and more importantly, the Internet firewall of the Server must be opened slightly for MMC to function properly.

The browser-based Internet Services Manager allows remote administration of some IIS features over the Internet.

- *Delegated Administration:* For web sites spread over multiple locations or for multiple sites on the same web server, management can be a problem. IIS 5.0 provides for administrators to create user accounts with limited privileges, called web site operators, to help administer the web site. For instance, a web hosting company has all the sites of its clients on a single server. Hence, it can create web site operator accounts for representatives from each company for managing their respective web sites. However, this does not allow these web site operators to access other web sites, IIS or the operating system.
- *Process Accounting:* This new feature in IIS 5.0 logs the amount of the CPU resources the web site uses

3. **Security**

Security in IIS has always been a slight problem. However, IIS 5.0 is now more inherently secure than many other commercial web servers. The major industry-standard protocols included in IIS 5.0 are:

- Digest Authentication
- Server-Gated Cryptography
- Kerberos v5
- Transport Layer Security (TLS) and
- Fortezza
- Further, three new wizards have been included to help administrators set different security settings easily.

4. **Application Environment**

IIS 5.0, along with Windows 2000, provides a rugged and secure application development environment for application developers. Features such as Active Directory and Component Object Model (COM) provide flexibility and security for these applications. Further, scriptless ASP processing and better error-control provisions in application development allow efficient programs to be written.

Answer: [d] Process Accounting

Module:4

Reference No:M4119

Question: LDAP (Lightweight Directory Access Protocols) has an edge over X.500 in Directory Enabled Networks (DEN), because it supports:

- [a] Static routing
- [b] Dynamic routing
- [c] Both
- [d] None

Module 4 -Directory Enabled Networks (DEN)

Introduction

Networks have certainly made the life easy for corporate, but there are problems that have to be dealt with. Some measures to overcome these problems are quick corporate responses, cost effective administration and management, consistent security policies, accurate data and the like.

DEN

Directory Enabled Network (DEN) is the most effective and efficient way to achieve the benefits described

above. It allows the network manager to co-ordinate activities of the entire network by optimising allocation of bandwidth and latency. It is done on a global basis, considering all the needs of an enterprise. DEN enables users to correlate different characteristics of the database, so that various applications can effectively use relevant data from anywhere in the organisation, in whatever format it may be. Two components of DEN are:

- Directory
- Policy server

1. **Directory**

Directory is a software procedure to store and retrieve information about data like locating user files, getting network addresses and the like. DEN correlates all LAN directories and integrates them into a single logical entity. It provides an automatic mapping mechanism to shuffle between different data formats. It categorises a part of the network into separate entities such as policy server, the directory server, the application server and the like.

- **The X.500 project**

It was the first project for open standardised directory promulgated by ISO/ITU (the International Organization for Standardization/International Telecommunication Union). Its attempt was to standardise the worldwide telephone service. Soon the ISO realised that the standards were applicable to a far wider range of application, particularly in the field of distributed applications. Therefore, the standards took more than a decade to develop.

- **Schema descriptions**

The developers of X.500 quickly realised that entities could also be addressed as schema description. A schema is the way in which data is represented from a logical, physically viewpoint. Each site in a distributed network is given schema for an entry that can store and retrieve data relating to X.500 request. It can then and transmit that data to other sites whenever requested. Defining a universal set of common schema is an important part of standardisation.

- **The X.500 directory**

The X.500 service is referred to as 'directory'. Its contents are attribute-based, and the basic directory entity is the 'entry'. An entry is a set of attributes having a unique name. The schema defines the type these attributes can take. If one directory understands the schema of another co-operating directory than they can

Module:4

Reference No:M4121

Question: Which of the following AIN (Advanced Intelligent Network) components functions as an intelligent router?

- [a] Intelligent peripheral
- [b] Service Control Point
- [c] Service Switching Point
- [d] Signaling Transfer Point

Module 4 -Intelligent Networks- An Introduction

What is an Intelligent Network (IN)?

In telecommunication, a service independent network is termed as an intelligent network. Here, the service providing logic or intelligence is moved from the switch to all the nodes in a distributed network. The network operator can develop and control service logic and other related activities efficiently. Through an Intelligent Network, new services can be evolved and customised according to user requirements.

What is an Advanced Intelligent Network?

A telephone network architecture that separates service logic from switching equipment and allows new services to be added without redesigning switches is known as an Advanced Intelligent Network.

AIN Architecture

The network topology for AIN architecture houses a number of elements that require an associated database. Some of the important elements that constitute an AIN structure includes:

- **Service Switching Point (SSP):** A telecommunication switch that identifies calls which require advanced service processing, and forwards them to an appropriate Service Control Point is known as an SSP. It has a large and exhaustive database that allows it to identify calls properly.
- **Service Control Point (SCP):** Calls requiring advanced service processing are handled by the SCP. In order to achieve high performance, each SCP is configured to process calls for a single service and therefore contains a number of processors. All these processors can access a common database of services and subscribers, or each processor can have its own database. This depends on the implementation. After, the SCP receives a request from an SSP, it queries the database for necessary information and then processes the call.
For example, if a customer wants calls to a specific number to be routed to different physical locations depending on the area code of the caller, then the SCP looks up the physical location that should receive the call. The SCP may also seek other information from the user. To process these calls, the SCP will route the call to an Intelligent Peripheral (IP), which interfaces with the customer.
- **Signaling Transfer Point (STP):** STP is an intelligent router whose function is to route requests from SSPs to appropriate SCPs.
- **Intelligent Peripheral (IP):** Devices that are similar to the ones that process touch-tones and the voice that accepts input from customers are termed as IPs.

Fig: AIN architecture

The figure above shows a typical AIN architecture along with the databases.

- **Service Management System (SMS):** SMS is a non-real-time system responsible for managing the operations of SCPs. Each SMS is designed to manage different SCPs offering varied services. Other functions of the SMS include updating SCP databases, configuring SCPs, and provisioning new services. Data for each SCP is stored in the SMS master database. The SMS and SCP databases contain the same information but use different formats.
- **Service Creation Environment (SCE):** SCE is a non-real-time system for creating, testing, and deploying new services. It is a warehouse of tools for creating service processing logic and databases. The SCE has a special database of its own that contains the building blocks for various services. With the help of these building blocks, developers can create new services in record time.

Answer: [d] Signal Transfer Point

Module:4

Reference No:M4122

Question: Dynamic Synchronous Transfer Mode (DTM) supports implementation of Virtual Private Networks (VPNs) because of :

[a] PDH (Plesiochronous Data Hierarchy)

[b] IP (Internet Protocol) over DTM

- [c] SDH (Synchronous Digital Hierarchy) tunnelling
- [d] DTM Local Area Network (LAN) Emulation (DLE)

Module 4 -Dynamic Synchronous Transfer Mode (DTM)-II

Introduction

Dynamic Synchronous Transfer Mode (DTM) is a technique that provides complete control over the network resources. It increases the utilisation of opticfibersnd decreases the load on the nodes. It has been developed to support a wide variety of services like real-time broadband traffic, and multicasting. DTM offers three types of reservation schemes namely guaranteed bandwidth, on-demand bandwidth, on demand bandwidth with best effort. It transfers data through channels. Each channel is divided into frames of 125 microseconds. Each frame in turn is divided into 64-bit slots.

DTM services

The bulk of the data that is transmitted over networks makes use of the Internet Protocol (IP). DTM caters specifically to this mode of traffic. It also deals with Plesiochronous Data Hierarchy(PDH) based data since. Many of the old networks employ this standard. PDH supports data transfer that is partly synchronous and partly asynchronous. DTM is able to effectively several network features. Some of the services that are available because of this integration :

- **DTM Local Area Network (LAN) Emulation (DLE):** Using DLE geographically distributed LANs can be internetworked, and Ethernet packets can be transmitted through DTM channels. Therefore, the nodes work as if they are a part of the widespread Ethernet LAN. Virtual Private Networks (VPNs) is a case in point.
- **IP over DTM:** For the transfer of IP packets, two transmitting techniques are used by DTM -IP over DTM and IP over DLE. IP over DTM enables the data carrying capacity of a DTM network to be fully utilised, on a hop-by-hop basis. In IP over DLE, virtual LANs are established to effectively transfer IP packets.
- SDH/SONET tunnelling
- PDH transport

DTM solution for enterprise access

A network access point with DTM is used by service providers to cater to the communication needs of a large enterprise. The network can be optimally used by integrating DTM with the transport level of the network model. A special DTM device provides service access through several Ethernet ports, and implements the enterprise access solution.

Some of the advantage of using the access device as a network integration device includes the following:

- A single network layer between the user and the service access point
- High level of scalability that allows price differentiation
- Synchronous circuit switching that guarantees Quality of Service (QoS) for effective customer satisfaction
- Control features in the bandwidth reception that support customisation
- Internet traffic control which ensures non-interference with the corporate data network
- High quality communication for videoconferences and the like
- Layer three independent service -Data Link Service (DLE) that ensures interoperability and preserves the existing LAN architectures.

Answer: [d] DTM local Area Network (LAN) emulation (DLE)

Module:4**Reference No:M4123**

Question: Which of the following is true (with regard to Dynamic synchronous Transfer Mode (DTM))?

- [a] It uses circuit switching
- [b] It uses only packet switching
- [c] It employs both circuit and packet switching
- [d] It uses multidirectional data transfer

Module 4 -Dynamic Synchronous Transfer Mode (DTM)-I**Evolution**

The evolution of the Internet , multimedia and animated services created heavy demand for higher transfer rates, through the networks. Both voice and video had to be transmitted efficiently over the networks. The capacity of the networks was increasing faster, than the processing speed of the computers. With the advent of fibre optic transmission technologies, the network carrying capacity increased manifold resulting in transmission bottlenecks. These were the result of processing and buffering at switches and access points on the network. It then became imperative to establish a network standard that would not be based on the computers or their storage capacity. Rather it had to be one , which would limit the complex operations, performed on the nodes, resulting in high transmission capacity. DTM emerged as the real-time standard.

What is DTM?

Dynamic Synchronous Transfer Mode is a high speed networking technology. It employs the best transmission technologies to provide high quality , and has the capability to adapt swiftly (dynamically) to changing bandwidth requirements. The DTM design seeks to integrate the services into distributed and one-to-one communication networks. It can be deployed directly as in application-to-application service, or as a carrier in higher layer protocols like the Internet Protocol (IP).

Basic feature

Essentially, DTM combines features of both circuit switching and packet switching. They include:

- Simple non-blocking, real-time traffic-supporting properties of circuit switching.
- Dynamic resource handling properties of packet switching.

These features have created a transport-network architecture that caters to high transfer capacity, using dynamic allocation of resources. Basically, the DTM is a circuit-switched Time Division Multiplexing (TDM) scheme, with a guaranteed data transfer rate. Dynamic reallocation of bandwidth is also possible when the DTM works in tandem with the Asynchronous Transfer Mode (ATM). Thus, the network can adapt to changes in traffic/load, and divide its bandwidth with the available nodes, according to the demand.

Principle

The basic building blocks of the DTM scheme are frames and slots. It is based on unidirectional data transfer with multiple accesses. Commonly used topologies like double ring, point-to-point, dual bus and the like can be implemented. The figure gives the fundamental structure of a multiple access medium.

Fig: DTM Multiplexing medium with multiple access

The time division multiplexing scheme divides the transmission capacity of a channel into small time units. The total link capacity of transmission is divided into fixed sized frames of 125 microseconds. These frames in turn are divided into a number of 64-bit time slots. The time slots per frame are dependent on the bit rate.

The specific use of 125 microseconds and 64 bits per time slot enables adapting to digital voice and Plesiochronous Digital Hierarchy (PDH).

Plesiochronous (pronounced as plee-see-AH-krun-us, is derived from Greek-"plesos" means close, and "chronos" means time) describes operations that are almost, but not quite, in synchronization - in other words, almost synchronous. Plesiochronous Digital Hierarchy (PDH) is the most widely used system for data transmissions between continents. It makes small adjustments in the differing data rates between systems.

Answer: [c] It employs both circuit and packet switching

Module:4

Reference No:M4124

Question: Which of the following is not true with regard to SNMP?

- [a] It is a connectionless protocol
- [b] It guarantees data transmission
- [c] It can accommodate devices from different vendors
- [d] It reduces the resources required, and makes network management simple

Module 4 -Simple Network Management Protocol (SNMP)

The SNMP is a network management specification developed by the Internet Engineering Task Force. It is a communication specification that describes the exchange of management information, between network management applications and management agents. It makes network management very simple, and reduces the resources required to maintain it.

It is a connectionless communication sub-network; there is no predefined communication path for data transmission. However, this makes delivery of data unreliable. SNMP implements two protocols: the User Datagram Protocol and the Internet Protocol. It However requires Data Link Layer protocols like Ethernet to transmit data between the management and the managed agent.

A network management system primarily consists of two elements:

1. **Manager:** The network administrator ensures that various functions are implemented, and the network is managed well.
2. **Agents:** They are entities that interface with devices that are managed.

The managed devices have managed objects, which reside in them. The managed objects could be hardware, configuration parameters, performance statistics and so on. Bridges, hubs, routers or network servers are some of the managed devices.

Architecture

The SNMP architecture contains the following:

1. **Network Management Stations (NMSs):** The NMSs are workstations on which the network management applications are run.
 2. **Network Management Application (NMI):** It provides control information to agents, and polls management agents for information.
 3. **Management Information Base (MIB):** A database of values is maintained by managed device, based on the definitions in the MIB. The MIB is implementation dependent, and is not a database.
- Management Agent:** It accepts control information ,and provides the information contained in the MIB to management applications.

There are a lot of devices present in a network. Each managed device has to be carefully monitored, modified according to changing requirements and controlled. For instance, as the network address or counter. The managed object is a characteristic of a managed device. An MIB has a database of managed objects that reside on the agent

The managed objects are monitored by the network management system, with the help of the following operations:

1. **Get_Next_Request:** The subsequent object instance in a table, or list from an agent is requested.
2. **Get_Response:** This is the response given by the managed object for the *Get_Next_Request* Or *Get_Request* Or *Set_Request*.
3. **Get_Request:** The network management requests for the value of an object instance.
4. **Set_Request:** The values of an object instance are set within an agent
5. **TRAP:** A trap is sent by an agent to inform about a condition. The condition could be a change in the state of a device, device failure or agent initialisation.

The SNMP specifies the protocol to be used between the network management application and the management agent. It enables devices manufactured by different vendors to be managed by the same network management application.

The SNMP is very simple to implement ,and accommodates devices of different vendors. It does not require large computational or memory resources, which are otherwise required.

The SNMP manages the network by polling and asynchronous events.

Each agent collects the information such as performance statistics, which is related to the device in which it resides. It then stores the information in the agent's own MIB. When the SNMP polls for information gathered by each agent, then the MIB is forwarded to the manager.

Trap messages are generated based on certain device parameters. It is these trap messages that force SNMP events. The parameters are usually vendor device specific.

Answer: [b] It guarantees data transmission

Module:4

Reference No:M4125

Question: How can OFDM (Orthogonal Frequency Division Multiplexing) be implemented efficiently?

- [a] By using oscillators
- [b] Through Quadrature Amplitude Modulation (QAM) only
- [c] Through Fast Fourier Transform (FFT) only
- [d] Using FFT and QAM

Module 4 -Orthogonal Frequency Division Multiplexing-II

A digital modulation scheme, in which a signal is split into several narrowband channels at different frequencies, is termed as Orthogonal Frequency Division Multiplexing (OFDM). This evolved while conducting a research on minimising the interference among adjacent channels in multiplexing schemes. OFDM differs from FDM (Frequency Division Multiplexing) in the manner in which signals are modulated and demodulated. This technology is used widely in digital television, wireless local area networks etc.

Why implement OFDM?

As radio signals travel from one place to another, they are likely to bounce off surrounding objects like buildings, trees, mountains etc resulting in multiple paths being created between the transmitter and receiver. This is similar to echoes or reflections building up into multiple copies at the receiver at different times. The combination of all paths at the receiver end causes distortion to the modulated message signal. Wireless communication systems have to be designed to cope with multipath distortion. This can be understood with an example. Consider two paths for the carrier wave- the line of sight path, and a reflected

path from the ground. If one of the messages is sent at the right speed, then the second/reflected copy of the message may arrive exactly a little (one bit time) later than the first/direct message. At the receiver end, two different bits that are mixed are received, resulting in a distorted version of the original message.

Principle

OFDM has been used to avoid problems caused by multipath reflections. This is achieved by sending message bits slowly so that any delayed copies/reflections arrive late by only a fraction of a bit time. In order to maintain a high bit rate, multiple carriers are used to send many low speed messages at the same time. These are combined at the receiver to obtain a single high-speed message. Thus, distortion caused by reflection is eliminated effectively.

OFDM Implementation

Separate local oscillator components were used in multicarrier systems to generate a number of carriers. This method of implementation was costly and inefficient. An alternative solution was reached through the use of a mathematical functional transformation called the 'Fast Fourier transforms'-FFT. This ensured that individual carriers with orthogonal property were produced. The FFT algorithm changes the signal from the time domain (expressed here as a series of time events) to the frequency domain (expressed as the amplitude and phase of a specific frequency). Using Inverse FFT, the original signal can be recovered. After the digitised data is coded for error correction and security, it is modulated by QAM (Quadrature Amplitude Modulation). Then the modulated signal is tuned to the appropriate frequency for transmission.

Wideband OFDM

A variant of OFDM in which the spacing introduced between the carriers is large enough so that any frequency errors between the transmitter and receiver are only a small fraction of the spacing is termed as Wideband OFDM (W-OFDM). This ensures that the performance of the system is not degraded due to any impairments..

Answer: [d] FFT and QAM

Module:4

Reference No:M4126

Question: Which feature of the Interior Gateway Routing Protocol (IGRP) prevents large loops of routers?

- [a] Poison-reverse updates
- [b] Split-horizon updates
- [c] Hold down
- [d] Composite metric

Module 4 -Interior Gateway Routing Protocol

The IGRP is a routing protocol. It allows gateways to create routing tables, by exchanging information with other gateways. A gateway first gathers information about the nearest network, which is directly connected to it. It then gets the information about other networks, by exchanging routing updates.

After gathering all the information, the IGRP's main objective is to identify a suitable path to the next network. The path depends on many factors, such as: the gateway to which it is sent, the network interface that is to be used, metric information and the like.

Metric Information: Metric information is a set of numbers, which indicates the quality of the path. It is not necessary that traffic should follow the same path. The IGRP can split the traffic into paths, which it finds suitable.

The IGRP stabilises routing in large or complex networks, gives quick response to changes in network topology, splits the traffic to facilitate quick movement, and provides different types of services from a limited set of information. The metrics it uses are:

1. Topological delay time, which is the time taken to reach the destination using a particular path, in an unloaded network
2. Path bandwidth, which is the slowest link in the path.
3. Channel occupancy, which is the amount of bandwidth occupied.
4. Reliability, which is the current error rate at which the fraction of packets have arrived undamaged.
5. Composite metrics of different paths are prepared to identify the best path. To do so, the gateways continuously update their routing tables and broadcast it to all the neighbouring gateways. This is compared with existing tables, any addition or deletion is noted.

Stability features

Various features have been incorporated to increase the stability of IGRP.

1. **Holddowns:** Holddowns stop unnecessary restoration of a route. Due to update messages, that may not be accurate. In the absence of update messages, new routes are chalked out and sent to the neighbouring routes/gateways. These are then sent to the entire network. However, sometimes the updates do not reach all the network devices immediately. In consequence it is possible for a device, that is not yet aware of the route failure, to send an update message claiming that the route is functioning.
2. **Split Horizons:** It works on the principle that it is unnecessary to send information about a route, in the direction from where it originated.

In the figure given below, router 1(R1) publicises that it has route to Network A. If router 2 (R2) sends the information back to R1, it is redundant as R1 is closer to the network than R2. The Split Horizon rule restricts R2 from sending any such routing updates to R1. It therefore prevents routing loops. Holddowns also provide extra algorithm stability for implementing IGRP.

Loops between adjacent routers can be checked by split horizon; whereas large routing loops are stopped by poison-reverse updates. An increase in routing metrics indicates routing loops. A good IGRP should send poison-reverse updates, when the metric increases, and remove routing loop.

Timers

IGRP has different types of timers and variables containing time intervals:

1. **Update timer:** It specifies the frequency at which routing updates have to be sent. The default is 90seconds.
2. **Invalid timer:** It specifies the waiting period of a router in the absence of routing update messages, before declaring it invalid. The default is three times the update period.
3. **Hold-time timer:** It specifies the hold down period. Its default variable is three times the update timer period plus 10seconds.
4. **Flush timer:** It specifies the time to wait, before flushing out a route from the routing table. The default period is seven times the routing update period.

Answer: [a] Poison-reverse updates

Question: Multi-layer IPsec is different from original IPsec because in ML-IPsec:

- [a] Data is transmitted over different layers
- [b] Datagrams can be divided into different zones
- [c] Multiple datagrams can be sent simultaneously
- [d] All of the above

Module 4 –Multi-layer IPsec

IPsec: IPsec are standard set of protocols that provide secure communication over Internet. IPsec architecture makes use of two protocols viz. AH (Authentication Header) and ESP (Encapsulated Security Payload) to provide secure data transfer. Each protocol provides two modes of usage:

- Transport mode (Provides protection for upper layer protocols)
- Tunnel mode (Provides protection to entire IP datagram)

IPsec takes each and every data transfer as IP datagram. It consists of three parts:

- *IP header:* Used for routing purpose.
- *Upper layer protocol header:* For example Transmission Control Protocol (TCP) header
- *User data:* For example TCP data

In transport mode, AH or ESP is placed in before the upper layer protocol header and after the IP header. This is done to protect the upper layer protocols and user data.

In tunnel mode, the complete IP datagrams are summarised into new IPsec packets. This IPsec packet includes a new IP header followed by AH or ESP header.

Multi-layer IPsec (ML-IPsec): It is different from IPsec in the sense that it divides IPsec datagram into different zones unlike simple IPsec where authentication is applied to entire IP datagram. Each zone has its own set of security links, private keys and access control rules. These are confined to a particular zone and are not shared by other zones.

Working of ML-IPsec: ML-IPsec protects the data traffic from source to destination and takes the responsibility for secure data transfer. At the source the IP datagrams (data in the form of small packets) are rearranged into different zones and then cryptographic protection is applied to it. When ML-IPsec secured data flows over the network, it may happen that some part of datagram may be decrypted, re-encrypted or modified but other parts of the datagrams will not be affected. When the datagram packets reaches the destination, ML-IPsec rearrange and reconstruct the datagrams in its original format

ML-IPsec design: ML-IPsec architecture holds the concept of zones. It is designed such that it should synchronise with original IPsec, both in terms of protocol format and processing software.

- **Zones:** This refers to the portion of IP datagram that comes under same protection design. Some of the properties of zones are: -
 - a. Zones, except that of IP header, cover the complete IP datagram.
 - b. Zones cannot overlap each other.
 - c. In an IP datagram it is not necessary for zones to be in continuous blocks.

- **Security association (SA):** It is a one-way relationship between sender and receiver and for ML-IPsec it requires much strong and complex security between the relationships. When one zone is secured then only next zone can receive the service of ML-IPsec. For this, ML-IPsec requires a new type of Security Association called Composite Security Association (CSA). It is collection of SA and comprise two elements:
 - a. *Zone maps:* It identifies the part of IP datagrams that comes under each zone.
 - b. *Zone list:* All the Security Associations (SAs) for each zone comes under it.
- **AH and ESP headers:** The Protocol for AH (Authentication Header) in ML-IPsec is almost similar to Original IPsec. The only difference is that, in ML-IPsec the Authentication Data section in AH is further subdivided into zones.
On the other hand in ESP (Encapsulated Security Payload), ML-IPsec are more helpful. Here different keys are used in diverse SAs for encrypting IP datagrams.

Answer: [b] Datagrams can be divided into different zones

Module:4

Reference No:M4131

Question: "Proxy servers" acts as a mediator between:

- [a] Two Local Area Networks (LANs)
- [b] Local network and Internet
- [c] Two networks using different protocols
- [d] Router and Internet

Module 4 -Proxy Servers

Introduction

Proxy servers are also called "proxy" or "application level gateway". A proxy server is a computer that acts as a mediator between organisation's local network and Internet. A web browser never connects the user to URL (Uniform Resource Locator). Instead, the browser connects to proxy server, requesting proxy server to get URL for the user. Proxy server isolates user from Internet thus preventing any hacking incidents. This ensures the security of internal address or any confidential details of a private network.

Proxy servers are used in common Internet services like HTTP proxy and SMTP proxy for web access and e-mail respectively. Proxies can store web pages, so that next request from the user can be processed locally. It also reduces the response time of the request.

Pros and cons of proxy server

Pros

- **Security:** Proper and correct configuration of the proxy server in an organisation, reduces the risk of hackers and unauthorised persons encountering internal network. All this all can be done without limiting the user access to Internet.
- **Cost:** The cost of having a huge connection to the Internet via proxy server is less as compared to use of modem for each terminal.
- **Administration:** A proxy server in an organisation enables the administrator to block the access to certain links, which the management finds unsuitable. Details pertaining to the sites visited by the

user, the time taken by the user for completing a specific task can be had with the help of proxy servers.

- **Caching:** Some sophisticated proxy servers have the ability to store the web pages that can be accessed in future thus improving the web browser performance.
- **NAT (Network Address Translation):** It is the ability of proxy server to use small amount of IP addresses to increase the interaction of the internal network with outside environment, irrespective of the number of workstations using private IP addresses on LAN via NAT.

Cons

- **Training:** Some amount of technical knowledge is required for installing, managing and getting better output from proxy servers.
- **Centralised failure:** The Internet usage via proxy server encounters risk of single point failure. If the proxy fails then all the clients associated with it cannot use the Internet until the proxy server is repaired.
- **Analysing specifications:** Each type of proxy server has their own specifications and it is difficult to analyse the specifications for someone who is not much acquainted with proxy servers. So, depending upon the type of proxy (network, disk, memory, processor proxy servers), the role is performed.
- **Security:** Operating system must be configured in accordance with proxy server otherwise it is vulnerable to hacking.
- **Remote users:** It is difficult to use Internet via proxy server, if the user is accessing it from laptop or working from home, because their software is not configured according to the server.

Working of proxy server

Clients (terminals) do not have any direct physical connection with the Internet and hence cannot communicate directly with the Internet. A proxy server is installed between Internet and local network of the organisation.

A proxy is a special HTTP server, which runs on a firewall machine. It waits for the request from the client and searches for results on Internet using suitable protocols. It then sends the results back to the client. While interacting with proxy server, client uses only Hyper Text Transfer Protocols (HTTP) but proxy can make use of File Transfer Protocols (FTP) also.

Answer: [b] Local network and Internet

Module:4

Reference No:M4132

Question: If a web site using the Internet Information Server from Microsoft does not run dynamic scripts, which of the following tools can harden the Web Server?

- [a] IIS Lockdown
- [b] CGI
- [c] URLScan
- [d] Microsoft Management Console

Module 4 -Internet Information Server (IIS) Security

The security of the web site is dependent to a large extent on the Web Server that is running the web site. Microsoft's Internet Information Server (IIS), first introduced with Windows NT is a robust, enterprise-scale Web Server that runs many web sites today.

The latest version is IIS 5.0, shipped along with Microsoft Windows 2000 Operating System, and runs as an enterprise service under the OS.

The four steps for maintaining the security of IIS are:

1. **Hardening:** Any piece of software can be made more secure by appropriately fine tuning its configuration. This is called "hardening." When Windows 2000 is installed, IIS is also installed as part of the default installation. If the computer is on the Internet, but is not being used as a Web Server, then IIS must be uninstalled from the system. Otherwise, the security of the network may be compromised by attacks specifically crafted against vulnerabilities in IIS.
If the computer is to be run as a Web Server and serve only static web pages without use of dynamic components such as CGI (Common Gateway Interface) scripts, (ASP) Active Server Pages or JSP (Java Server Pages), then it is advisable to run the IIS Lockdown tool. The tool secures the Web Server, but must be fully tested before exposing it to the Internet. If dynamic scripting is necessary, the "Advanced options" can be used.
"Patches" are small software programs released by software manufacturers to cover any bug or vulnerabilities in the original software. Installing up to date patches are a necessary function of the system administrator. This can be an exhausting task for the administrator if there are many systems on the network. "HFNetChk" is a tool released by Microsoft to check whether all systems on the network have been patched to a specific state or not. This check can be used on local or remote systems and is done using a database that is updated frequently by Microsoft.
2. **Maintenance:** It is important for the system administrator or Web administrator to be apprised of any vulnerability as soon as it is discovered. To achieve this, Microsoft has introduced a free email service that contains full details on any vulnerability or exploit in any of its products, including IIS, as soon as it is discovered and reported.
3. **Improvement:** Microsoft and other companies have developed many applications to enhance the security of IIS. URLScan from Microsoft, for instance, scans all requests from clients and filters them based on certain rules specified by the administrator. This is very effective, since most attacks involve some sort of malformed requests, such as a request that is exceptionally long, a request that asks for an abnormal action to be performed or encoded in character sets not normally used. The tool's ruleset completely protects a server against all known exploits for IIS and also provides protection against undiscovered attacks. The default rules provided during installation could be changed or new rules added for matching the requirements of a particular server.
4. **Monitor:** Although it is time consuming, it is of absolute importance to monitor continuously the performance of the IIS server. Configuring the security logs to record information about access to either directory and files or server events is the first step. Using Audit Policies in Microsoft Management Console (MMC) can do this. These events are logged in the Windows Security log. The Security log can record security events, such as valid and invalid logon attempts, as well as events that are related to resource use, such as creating, opening, or deleting files.

Answer: [a] IIS Lockdown

Module:4**Reference No:M4133****Question: Where is the service logic located in an Advance Intelligent Network (AIN)?**

- [a] Service Control Point (SCP)
- [b] Service Switching Point (SSP)
- [c] Intelligent Peripheral (IP)
- [d] Location Routing Number (LRN)

Module 4 –Advanced Intelligent Networks–II**Introduction**

An intelligent network is a telephone network architecture that separates service logic from switching equipment and allows incorporation of new services without redesign of switches and other critical components. This was developed by Bell Communications Research, and is recognized as an industry standard in North America. The initial version is AIN (Advanced Intelligent Network) Release 1 which forms the reference model on which new services shall evolve.

How does an AIN work?

A series of steps are involved in the working of AIN which are as follows:

1. A subscriber dials a number, which is received by a switch component in the telephone company central office.
2. This switch is known as the Service Switching Point (SSP). The switch forwards the call over a Signalling System 7 (SS7) network to a Service Control Point (SCP). The SCP is the place where the service logic is located.
3. The SCP has a mechanism to identify the service requested from part of the number that was dialed. Then it sends this information about handling the call to the Service Switching Point. Some of the examples of SCP's services include 5-digit extension dialling service, area number calling service, disaster recovery service, and do not disturb service.
4. Sometimes, the call is handled more quickly by an Intelligent Peripheral (IP), which is attached to the Service Switching Point by a high-speed connection. For example, services of the sort of a customized voice announcement in response to the dialed number or a voice call being analysed and recognised come under the IP's purview.
5. Further there is a provision to add an "adjunct" facility directly to the Service Switching Point for a high-speed connection in order to meet additional, undefined services.

AIN services

AIN service implementation enjoys a greater degree of flexibility and customisability. In order to create a new service the first step to be followed is to create a database. To refine further it is to create a generic model of the data, or schema, that the SCP database will use for calls that use this new service. Generally, the service developers choose from several different data models. The models are chosen based on the flexibility for quicker updates, ease to develop, and quicker response times. Credit card processing service can be implemented with an AIN.

One of the important services made available through an AIN is the Local Number Portability (LNP). LNP is the ability of a telephone customer to retain his/her local phone number if they switch to another local telephone service provider. The Location Routing Number (LRN) makes this LNP available. Phone number portability can be extended so that customers can retain their phone number when they move to another locality.

Advantages

- AIN allows the differentiation of products offered by the operators with new and unique services. This allows more competition among the vendors and brings in more value added services to the customers.
- Effectively eliminates software "bottleneck" (a discrepancy or problem that results in improper or restricted functioning) which is inherent due to switching vendors.
- A considerable decrease in development costs is achieved through the use of AINs.

Answer: [a] Service Control Point (SCP)

Module:4

Reference No:M4134

Question: Which of the spread spectrum technologies is widely employed?

- [a] Frequency Hopping
- [b] Direct Sequence
- [c] Time Hopping
- [d] Multipath Code Division Multiple Access

Module 4 -Spread Spectrum technology-Basics

What is spread spectrum?

A form of wireless communication technology in which the frequency of the transmitted signal is varied to attain much higher levels of bandwidth is called as Spread spectrum. In this technique the frequency spectrum of a data-signal is spread using a code uncorrelated with that signal thus enabling higher bandwidth occupancy. Codes with low correlation values and unique identity are used for each user. Due to this a receiver with knowledge about the code of the intended transmitter is able to select the desired signal.

Processing gain

The performance of a spread spectrum system is determined by its processing gain. It is the ratio between the transmission bandwidth and the information bandwidth.

$$G_p = BW_t / BW_i$$

Where G_p is the Processing Gain

BW_t is the bandwidth of the transmitted signal

BW_i is the bandwidth of the information signal

This ratio is called as ``spreading factor''. The number of users that can be allowed in a system, the amount of multi-path effect reduction, the difficulty to jam or detect a signal etc can be ascertained with the help of processing gain. Spread spectrum systems with high processing gains find wide applications.

Types

A number of techniques like Direct-Sequence (DS), Frequency-Hopping (FH), Time Hopping (TH) and Multi-path Code Division Multiple Access (M-CDMA) are available for signal spreading. The two most popular techniques among these are Direct-sequence and frequency hopping.

Direct-Sequence

Direct sequence spread spectrum is also known as direct sequence code division multiple access (DS-CDMA). It is a spread spectrum modulation technique for the transmission of digital signals over the airwaves or carrier waves. Here the stream of information to be transmitted is divided into small bits and each of them is allocated a particular frequency channel across the spectrum. At the transmitting end the data signal is combined with a higher data-rate bit sequence known as a chipping code, which divides the data according to a spreading ratio. The data signal is multiplied by a Pseudo Random Noise Code (PNcode). In this manner a redundant chipping code is generated which resists interference and also enables the recovery of the original data in case of damage during transmission. Direct-sequence is the mostly used spread spectrum technique.

Frequency Hopping

Frequency hopping spread spectrum is a digital scheme of data transmission. The transmitter frequency is varied at a very high speed with as many as many times each second. This variation from one frequency to another is termed as a "hop". The carrier signals frequency varies according to a unique hopping sequence. The transmitter frequency between these "hops" is stable. The time duration for which the transmitter remains on a particular given frequency between "hops" is known as the dwell time. Frequency hopping uses a much wider bandwidth than is needed to transmit the same information using only one carrier frequency.

Advantages

Some of the advantages of spread spectrum techniques include:

- **Interference limited operation:** The whole frequency-spectrum is utilised in all applications. This ensures interference to the minimum.
- **Privacy due to unknown random codes:** The random codes generated are unknown to a hostile user. This ensures that a nonuser is not able to detect the message intended for the other user.
- **Applying spread spectrum implies the reduction of multi-path effects.**
- **Random access possibilities:** Users have the option of starting their transmission at any arbitrary time. s.

Answer: [b] Direct Sequence

Module:4

Reference No:M4135

Question: Which component of the Local Multipoint Distribution Service (LMDS) is vendor specific?

- [a] Central Office (CO) equipment
- [b] Customer Premises Equipment (CPE)
- [c] Network Operations Centre (NOC)
- [d] Fibre -based infrastructure

Module 4 -Local Multipoint Distribution Service (LMDS)

Introduction

Local Multipoint Distribution System (LMDS) is a broadband wireless point-to-multipoint communication system technology. It is used for delivering voice, data, internet video services and the like, above the frequency range of 25GHz. . LMDS represents:

1. **L (Local):** The signals in this frequency range possess propagation properties that limit their potential area of coverage to a single site, normally up to 5 miles.

2. **M (Multipoint):** This denotes that the type of transmission involved here is point-to-multipoint or broadcast method. But from the user to the base station, the wireless link supports point-to-point transmission.
3. **D (Distribution):** Signals that consist of simultaneous voice, video, data.
4. **S (Service):** A customer subscribes to the . the LMDS network, but the services provided depend on the discretion of the operator.

LMDS architecture

LMDS networks support various architectures. They range from the most commonly deployed point-to-multipoint wireless access designs to the conventional point-to-point and TV distribution systems. Both Asynchronous Transfer Mode (ATM) and IP (Internet Protocol) transport methodologies are incorporated into the existing telecommunications infrastructure. Four primary parts of an LMDS network are:

1. Network Operations Centre (NOC)
2. Fibre-based infrastructure
3. Base station
4. Customer Premises Equipment (CPE).

System Equipment Segments

The Network Management System (NMS) is housed in the NOC (Network Operations Centre). The fibre based infrastructure consists of SONET (Synchronous Optical Network), optical carriers, Central Office (CO) equipment, ATM and IP switching systems, interconnections with the Internet and other Public Switched Telephone Networks (PSTNs). The conversion from the fiber infrastructure to the wireless infrastructure takes place at the base station. Network interface for fiber termination, modulation and demodulation functions, microwave transmission and reception equipment are some of the base station equipment. Local switching ensures billing, channel access management, registration and authentication at the base station. The CPE is vendor specific, and includes the out-door mounted microwave equipment and indoor digital equipment. It provides modulation , demodulation, control and interface functionality at the customer's end .

How does it work?

Microwave radios are installed at two separate sites that are within a five-mile range of each other. The first radio is installed at the LMDS hub or station, while the other is installed at the customer's site. This enables the two radios to transmit very large amounts of information between the two locations. The hub or station is located at a key position to interface directly with the landline or the fiber optic backbones and the standard telephony.

Advantages

- Low entry and deployment costs
- Quick and easy to develop systems, without making too many changes to the existing network infrastructure
- Quicker realisation of revenue
- Scalable architecture because of open industry standards for incorporation.

Answer: [b] CPE (Customer Premises Equipments)

Module:4

Reference No:M4136

Question: Which of these Internet protocols are used by Unified Messaging framework:

- [a] Simple Mail Transfer Protocol (SMTP)
- [b] Post Office Protocol (POP)
- [c] Internet Message Access Protocol (IMAP)
- [d] All of the above

Module 4 – Unified Messaging-Architecture

The advantages of being able to obtain voice messages, e-mail, faxes, and pager information from a single source are obvious, particularly for a professional on the move. The concept of **Unified Messaging (UM)** has therefore come to stay. Many industry observers expect messaging to become the preferred communication method. Some markets are experiencing up to 40% growth in messaging traffic per annum. Messaging is now a core business option for service providers, and no longer a peripheral one.

Making the most of this huge opportunity means having a framework that is flexible enough to support the messaging needs for both today and the future. Organisations are now looking for options that would help them set up the infrastructure for unified messaging in their work environment. Let us take a look at the architectural framework of a unified messaging system.

Internet Support – Building Blocks of UM

Support for Internet messaging standards is vital. There are three standards that are particularly relevant to messaging and are also used as the bases for unified messaging. They are:

- *Simple Mail Transfer Protocol (SMTP)*: Is one of the basic building blocks of Internet e-mail. SMTP is a protocol used to send e-mail messages to a server on the Internet. It has been in use for years and is a core Internet service today.
- *Post Office Protocol (POP)*: This is a simple mail retrieval protocol used by a client program to request a list of e-mail messages and then retrieve them. POP is also widely used by Internet e-mail programs. However, it has one major limitation. Once it downloads messages from the mail server to a local client, messages are removed from the server and hence cannot be accessed from another client.
- *Internet Message Access Protocol (IMAP)*: It is the successor of POP. IMAP permits selective retrieval of messages from a mail server, and also allows archival of messages for users. A user can therefore use several different machines to access messages. It is also convenient for managing messages by having them in one place.

Platform features of UM

- *Scalability*: Just like any other service that is designed to be used by a large number of people, UM must have the ability to be scaled up, or down, as required. It must be possible to easily add users to the system in batches rather than entering them one at a time. A typical scenario for this kind of activity would be when two companies merge together. If one of the companies did not have a UM system in place the merger activity would require the addition of tens or possibly thousands of new users into the system.
- *Interoperability*: Consider the case of a merger of two companies- A and B that have say 5,000 and 3,000 UM users respectively. Company A is going to acquire company B. Everything seems to be going fine until a technical analyst points out that the two UM systems are not interoperable. This problem

involves a substantial cost. Interoperability is hence a key issue that has to be considered while putting a UM system in place.

- *Future proof:* There is no way we can know which technical advancements will grow in the future and which one would fail. Therefore UM applications must have open platform architecture so that new applications can be added anytime.
- *Easy maintenance:* The ease of system administration onsite is a must for any UM system. One of the main drivers behind having an on-site solution is that resident support staff can easily maintain the system. If technicians have to keep requesting assistance from the UM vendor then the "down-time" is bound to increase and it will significantly effect usage and customer satisfaction levels.

Answer: [d] All the above

Module: 4

Reference No: M4137

Question: Unified Messaging is a common way of receiving all kinds of messages like email, fax, etc. through a single interface. Fax messages are received as:

- [a] Simple mail that can be viewed in the editor window.
- [b] Attachments that can be printed out
- [c] Messages notifying receipt of a fax that can be collected
- [d] None of the above

Module 4 - Unified Messaging

Unified messaging or UM is an often used, but poorly understood term. In short, it is embodied in the concept of a universal inbox for all types of messages: voice, fax, e-mail and attachments. While this is a straightforward idea that makes a lot of sense, it has been relatively slow to take off for a variety of reasons. Now, with the emergence of internet-enabled telephony products, we are starting to see a widespread move toward this.

Introduction

The basic idea behind unified messaging is a simple one. Rather than having separate viewers or procedures for voice mail, e-mail, and fax messages, it would be far simpler to put them all into a single integrated inbox. Click on an e-mail message, and it is displayed in your e-mail editor. Click on a fax message, and it is displayed in a fax viewer for display or printing. Click on a voice mail message and it is played back over your PC speaker. However, until recently, one of the key ingredients, phone systems that could talk to computer networks, was missing. But now Internet telephony is very much possible and so the concept of unified messaging has a whole new look about it.

Why UM?

Unified Messaging has been conceived and developed as a solution to message chaos. This results not just from the growing volume of communication, but also because each type of message gets delivered to a different location: voice messages to the voicemail system or answering machine; fax messages to the fax machine, e-mails to the e-mail server, etc. This makes it difficult for the end-user to retrieve messages from different locations and hence costs a lot of time because in the present corporate environment, messages have become one of the most important bases of communication. Unified Messaging exists to simplify working life by putting the user in control of communication. But UM is not just for the corporate, it is for everybody, office based employee, traveling executive or the person in the street. Every user of communications technologies will benefit from having a single point of administration of all messages.

Benefits of UM

Unified messaging has numerous benefits, the foremost being simplicity. With this service, one can check all of his messages in one session rather than several separate sessions. This cuts down on the time required to retrieve and view messages, and also simplifies remote message management, such as for a salesperson on a road trip. Let us see the effect of unified messaging on the traditional messaging methods:

- *E-mail*: Unified messaging is really an extension to existing e-mail services, so it doesn't really add much to e-mail systems, except for the ability to view multiple message types besides plain text.
- *Voice mail*: Voice mail systems are beginning to support unified messaging. This means that one can browse and retrieve voice mail messages just as he would do with e-mail messages. Different vendors use different approaches, however, the usual approach is to attach a compressed sound file to an e-mail message for offline playback.
- *Fax*: Fax servers are also beginning to support unified messaging, meaning that incoming faxes can be routed to a users e-mail inbox and displayed as an attachment that can be printed out. This service is especially useful for companies that receive a high volume of incoming faxes for specific individuals, or have many offsite personnel who need to be able to retrieve faxes remotely.

Answer: [b] Attachments that can be printed out.

Module:4

Reference No:M4138

Question: Extensible Business Reporting Language (XBRL) is an XML based application that is used for financial processing. Which of the following statements is false?

- [a] Data in an XBRL document can be accessed with any office tool such as a spreadsheet etc.
- [b] It is a freely available electronic language for financial reporting.
- [c] It is compatible with virtually any software product that manages financial information.
- [d] The organisation has to disclose additional information than what is required in normal accounting standards.

Module 4 – Extensible Business Reporting Language

Extensible Business Reporting Language (XBRL), formerly code-named FRML or Financial Reporting Markup Language, is an open specification that uses Extensible Markup Language (XML) based data tags to describe financial statements for public and private companies. XBRL is an XML application and benefits all members of the financial information supply chain. It does not establish new accounting standards but concentrates on enhancing the functionalities of the existing ones.

Features of XBRL

1. Data in an XBRL document can be accessed with any office tool such as the spreadsheet, word processor, and the like.
2. Internet being the primary source of all financial information, XBRL enhances efficiency by making web browser searches more meaningful.
3. XBRL is a freely available electronic language for financial reporting.

Applications of XBRL

1. *Financial Statements*: XBRL is used to describe financial statements of all sorts, especially those used to exchange financial information
2. *Taxes*: Specifications for tax returns that need to be filed can be designed using XBRL

3. *Regulatory Filings:* Specifications for large number of filings required by government and regulatory bodies are also designed using XBRL
4. *Accounting and Business Reports:* It is also used to draft management and accounting reports. For example, all the reports that are created by an accounting system using XML, can be easily re-used whenever required by XBRL
5. *Authoritative Literature:* XBRL can be used as a standard to describe literature related to accounting

Benefits

1. It is an efficient alternative for preparing financial statements
2. It enhances distribution and reusability of existing financial statements through automated analysis
3. It ensures efficient data collection that in turn lowers operating costs while concentrating on adding value and increasing transaction capacity
4. It is compatible with virtually any software product that manages financial information thereby increasing its potential for complete interoperability with other financial applications.
5. Does not require a company to disclose any additional information beyond what is normally disclosed under existing accounting standards. Does not require a change in existing accounting standards.

XBRL and Information System Audit

Any financial data is useful if it is meaningful and reliable. XBRL achieves this objective with the aid of technology and information systems. Hence, controlling systems forms one of the most important activities within an organisation and more so for a financial institution. There are four core objectives for auditing any information system. These are:

1. *Maintainability* ensures that changes to the system do not affect the availability and integrity of data.
2. *Integrity* ensures that the system in itself is complete, accurate and gives timely results.
3. *Security* ensures that the system is safeguarded from any unauthorised access.
4. *Availability* ensures that the system is able to state its purpose of existence whenever put to use .

Answer: [d] The organisation has to disclose additional information than what is required in normal accounting standards.

Module:4

Reference No:M4139

Question: Internet Message Access Protocol or IMAP allows _____mode of email access.

- [a] Online
- [b] Integrity and Confidentiality
- [c] Disconnected
- [d] None of the above

Module 4 - Internet Message Access Protocol

Internet Message Access Protocol or IMAP is a method of accessing electronic mail kept on a mail server. In other words, it permits a "client" email program to access remote messages as if they were stored locally. For example, email stored on an IMAP server can be accessed from a desktop computer at home, a workstation at the office, and a notebook computer while travelling. The basic idea behind IMAP is for the email server to maintain a central repository that can be accessed from any machine at any geographic location. IMAP is defined by RFC 1064.

Need for IMAP

Consider this situation. You log on to your mail server that implements POP from your home. The messages are downloaded on to the clients system and are then removed from the mail server. Now these messages reside on the client system. You then go to your office from where you again want to access the same mails but surprisingly you don't find them on the server because they had already been downloaded to the client system at home. The reason for this is that POP is designed to support "offline" message access only, wherein messages are downloaded and then deleted from the mail server and thereafter cannot be accessed from different locations. IMAP has been designed as a solution to this problem. In contrast to POP, IMAP leaves all messages on the mail server and you view a temporary copy of each message when reading your mail. It provides the flexibility of reading your mail from any location, but due to limited space on the mail server, you must ensure not to let too many messages accumulate, otherwise you will be unable to receive new mails.

Features of IMAP

1. *Mobility*: Unlike POP, with IMAP, your email remains in the server unless you delete it. These messages can be organised in different folders and since your email is always there, you can view it from anywhere.
2. *Security*: When you have the option of viewing your messages from any location, the immediate question that comes to mind is how secure is it? All the major IMAP servers allow you to select a mode that encrypts your login ID, password and the entire email reading session. This is especially important while reading your message from a remote web-server.

What Next?

Electronic mails have a wide scope. While POP supported *offline* message access, IMAP came up with *online* reading of mails. The Internet society is now looking up to the challenge of having a protocol that allows the user to send and read messages even in a disconnected mode and when the connection is established again, the server is resynchronised with the current state of the mailboxes.

Answer: [b] Online

Module:4

Reference No:M4140

Question: Normal Post Office Protocol (POP) session has three different stages:

1) Transaction state 2) Update state 3) Authorisation state.

The correct sequence is

- [a] 1,2,3
- [b] 3,2,1
- [c] 3,1,2
- [d] 2,3,1

Module 4 – Post Office Protocol

Post Office Protocol or POP is a standard program for storing email on a mail server until a mail client retrieves it. The conventional port number for POP protocol is 110. The POP standard is defined by RFC 1725.

POP service is an aspect of e-mail that allows clients to check for new incoming messages delivered to their POP e-mail accounts. The POP server performs two basic but important functions. First, it authenticates, or verifies, the identity of those trying to access certain POP accounts in the form of a login and password. Secondly, it allows clients to download any new e-mail they may have in their POP accounts. Think of the POP server in terms of your local post office. The e-mail is routed in a similar fashion as that of a snail mail. Access to the mail requires authentication, whether in the form of a lock and key or login and password. After authentication, one can obtain any mail that might exist in the PO Box or the POP account.

POP supports offline access to mails in the sense that once the messages have been downloaded from the server to the client system, they are deleted from the server and the connection is lost.

POP Session

A POP session has different stages.

Authorisation State

The POP server issues a one-line greeting after the TCP connection has been established by a POP client indicating a positive response. Once the server has issued this one-line greeting, the POP session enters the *Authorisation* state. In this state, the client is required to identify and authenticate itself to the POP server. Once the authenticity of the client has been validated, it is given access to the appropriate mailbox, in which case the POP server acquires an exclusive-access lock on the mailbox to prevent the messages from being modified or removed. If the lock is acquired successfully, the POP server responds with a positive status indicator. The session then enters the *Transaction* state.

Transaction State

In this state, the client may issue any of the valid POP commands, for example:

- 1.RETR [msg] - When the POP server receives this command with the appropriate message number, it will send the message corresponding to that number to the client
- 2.DELE [msg] - After receiving this message, the POP server marks the message as deleted. However, the server actually does not delete the message until the POP session reaches the Update state.

These commands can only be given in *Transaction* state.

Update State

Once the client has issued the QUIT command in the *Transaction* state, the POP session enters the *Update* state. If the client issues the QUIT command from the *Authorisation* state, the POP session terminates without entering the *Update* state. If a session is terminated for some other reason other than a client-issued QUIT command, the POP session does not enter the *Update* state and no messages will be removed from the mailbox.

Answer: [c] 3,1,2

Module:4

Reference No:M4141

Question: Extensible Markup Language or XML differs from HTML in the sense that

- [a] It has predefined tags and semantics
- [b] It allows the applications to define its own tags and semantics
- [c] It has a larger set of predefined tags and semantics
- [d] None of the above

Module 4 - Extensible Markup Language

Introduction

The growth of the World Wide Web has given businesses the ability to inexpensively distribute electronic documents to an international audience. Web documents have become larger and more complex. As companies prepare for e-commerce initiatives, they face the task of integrating their applications and processes with other companies. A challenge for business application developers is to integrate data generated by applications from different vendors. Through the use of an Extensible Markup Language (XML), applications can interchange data without having to manage incompatible data formats.

XML

The Extensible Markup Language (XML) is a web-authoring tool that links the content elements of a page to a Web browser. XML is syntactically similar to HTML in the sense that it also uses tags to define the presentation of text on the web browser. In fact, XML can be used in most of the places in which HTML is used today. But it has some advantages over HTML. .

XML is a markup language for documents containing structured information. Structured information contains both content (words, pictures, etc.) and some indication of the role of such content. E.g., content in a section heading is different from content in a footnote, which means something different than content in a figure caption or content in a database table.

Almost all documents have some structure. A markup language is a mechanism to identify structures in a document. The XML specification defines a standard way to add markup to documents. Applications that will benefit from XML are applications that cannot be accomplished within the limitations of HTML.

Why XML?

In order to appreciate XML, it is important to understand why it was created. XML was created so that richly structured documents could be used over the web. The only viable alternative, HTML, is not practical for this purpose. HTML, as we've already discussed, comes bound with a set of semantics and does not provide arbitrary structure. This is not to say that XML will be able to completely serve the purpose, but it is better equipped to do so.

In HTML, both the tag semantics and the tag set are fixed. Let us now understand the difference between tags and tag semantics with the help of an example. In HTML, if we want to define some text as bold we write it as:

This will be in bold.

Here, "b" is the tag used to convert the text into bold, while the text between tags and is the semantics. The text between the two will appear in bold when viewed on the browser.

XML specifies neither semantics nor a tag set. In fact XML is really a language for describing markup languages. In other words, XML provides a facility to define tags and the structural relationships between them. Since there's no predefined tag set, there can't be any preconceived semantics. All of the semantics of an XML document will be defined by the applications that process them.

Web Applications of XML

The applications that will accept XML fall under the three broad categories:

1. Applications that require the web client to mediate between two or more miscellaneous databases.
2. Applications that attempt to distribute a significant proportion of the processing load from the web server to the web client.
3. Applications that require the web client to present different views of the same data, to different users.

Answer: [b] It allows the applications to define its own tags and semantics.

Module:4

Reference No:M4142

Question: One of the main objectives of e-commerce is to attract as many customers as possible and reach out to them irrespective of where they are. Extensible Markup Language (XML) makes this possible by _____ feature.

- [a] Standardisation
- [b] Internationalisation
- [c] Accessibility
- [d] Manageability

Module 4 - XML- E-commerce Perspective

Despite what we may have heard, the biggest inhibitor to e-commerce is neither security nor reliability, but it's the sharing of data between applications. Moving data between applications, whether on an intranet or an extranet, requires human intervention. Because of the explosion of e-commerce on the Internet, physically mapping each and every application's data element to all other applications we may be communicating with is both time- consuming and expensive. The solution to this dilemma may be XML. Let us now see the advantages of XML towards electronic commerce.

Advantages to Business

- *Standardisation:* Standardization in information representation and transfer is crucial to both B2B and B2C E-Commerce. XML is platform and application-independent and depends on other technologies such as URLs for name identifiers that are all standards.
- *Manageability:* The advantage of data being independent of any particular platform or application is that it can be transformed to produce different types of outputs for different media devices like the Web browser, paper, CD-ROM without the need to modify the original content. XML allows authors to concentrate on authoring rather than formatting and thus to be more productive.
- *Longevity:* Binary formats only last as long as the systems that supports it. XML data exists as plain text. This gives data a longer life span with future readability and reuse. Even if a system becomes obsolete, the data will live on and will remain accessible in the long term.
- *Business-to-Business Communication:* Conducting E-Commerce requires communicating with other companies that often poses a challenge. XML simplifies business-to-business communication because the only thing that has to be mutually agreed upon is the XML vocabulary that will be used to represent the data. Also, neither company has to know how the other's backend systems are organised. XML based solution is scaleable in the sense that if another partner has to be added, it can be done without much of hazard.
- *Internationalisation:* A major advantage of conducting business on the Web is that it broadens the customer-base towards globalisation, without the necessity of having physical office locations. However, in order to communicate, a business must "speak" the language of the region in context. With technology support in XML, Web sites can be multilingual.

Advantages to Customers

- *Personalisation:* Currently there are many ways of accessing the information. XML improves the presentation of information for its end-users as it allows them to customise the view as per their liking.

- *Accessibility:* Web is increasingly being accessed by customers using a variety of devices with differences in screen capabilities and computing power for example desktop computers, personal digital assistants, cellular phones, and so on. It is important for every business to take into account the user's environment. XML, being platform-independent, scales well to provide information on these devices without the need for the user to make adjustments at his end.

Answer: [c] Accessibility

Module:4

Reference No:M4143

Question: "Biometric authentication" is a technique for secure data transfer. This authentication is based on:

- [a] Design features
- [b] Logical features
- [c] Physical features
- [d] Depends upon the application to be authenticated

Module 4 – Client Security

Client computer security comprises security of data transfer and hardware, and the like. Providing security may increase the costs to the owner of the client computer to protect data from theft, viruses, etc.

Physical theft protection:

Portable client computers are becoming an ideal medium for hackers. Therefore, stringent measures need to be taken to protect the system. This involves greater costs. First, the cost of the system itself and second, the cost of useful data stored on the disk. In fact, the second cost is more crucial for the company.

The most commonly used devices to secure data from theft are:

- Locks and cables to prevent system theft.
- Chassis Intrusion sensors that alert the system manager of any change in configuration or any unauthorised physical response.

Three tier secure access to network security:

Network resources should be protected from unauthorised access, viruses, worms or Trojans. Data protection methods can be organised into three levels:

Level 1: Here client computers are protected from unauthorised access. Authentication takes place before the booting of the operating system. Passwords are provided at various levels, which gives further authentication.

Level 2: At this level, the network is protected from unauthorised access. Authentication can be achieved through network password and different biometric devices.

Level 3: This is the highest level of protection and uses advanced techniques to protect data. It includes encryption of data, frequent use of anti-virus packages, and firewall security etc.

Security techniques used across the three levels:

Authentication: It includes verifying the identity of the user. Authentication can be achieved by:

- **Password:** It is the most commonly used authentication practice, but this increases the burden on systems management in the sense that most of the help queries are regarding forgotten passwords.
- **Token device:** It is a security device given to an authorised user. Smart cards are best known nowadays. It has memory and microprocessor integrated into it. Smart cards are used to access the building, computers, and the network. Single-use Universal Serial Bus (USB) token is a substitute for smart cards. These are hardware devices that use Electrically Erasable Programmable Read Only Memory (EEPROM) to store access information. It provides security for system logon, network administration, and network access.
- **Biometric authentication:** Here the user's fingerprints, voice or facial features are stored to authenticate his identity.

Secure communication over public and private network:

Security of data over public and private network is a crucial matter. Three technologies are used for the same:

1. **Public Key Infrastructure (PKI):** In PKI, a digital certificate is given by trusted third party certificate authorities (VeriSign, Entrust etc.) that authenticate the identity of each party transacting over the Internet. Data transfer with the help of PKI is in an encrypted format.
2. **Secure Socket Layer (SSL):** Mostly used for e-commerce transactions. SSL protocols are used to establish a secure and dedicated network between the client and the server. SSL encrypts all the data transferred from client to server or vice versa. A projected standard from Internet Engineering Task Force (IETF) is the Transport Layer Security (TLS), which is the emergence of SSL.
3. **Internet VPNs:** It is a logical (virtual) connection that provides privacy on public networks like the Internet. A technology called "tunnelling" and the protocols associated with it, known as "tunnelling protocols" like point-to-point tunneling protocols (PPTP), are used to establish a secure path over Internet, for data transfer.
Presently, the two emerging protocols for security are the Layer 2 Tunneling Protocols (L2TP) and the Internet Protocol Security (IPSec).

Answer: [c] Physical features

Module:4

Reference No:M4144

Question: Which of the following is not a key feature of distributed firewalls.

- [a] Dependence on network topology
- [b] Using IPSec
- [c] Using Policy language
- [d] Efficiency in detecting internal attacks

Module 4 – Distributed Firewalls

Introduction

Today, business needs are constantly changing. As a result, corporate networks also need to expand to suit the changes. In such an environment, network security has become a critical issue. To tackle this concern, an

entirely different approach called distributed firewalls is being used.

Distributed firewalls

A firewall is a program or a hardware device that filters data packets entering or leaving the network.

Traditional firewalls are placed at the periphery of the network and data packets are made to pass through it. Data packets are allowed or denied based on the set of rules and regulations laid down by firewalls.

Encrypted data is not checked by firewalls and as a result enters the network.

Distributed firewalls, unlike traditional firewalls, are installed throughout the network at all endpoints. Three main points that support distributed firewalls are: -

1. **Policy language:** It is used to set policies for firewalls i.e. rules and regulations, which guide firewalls in evaluating network traffic.
2. **System management tools:** It distributes the above-mentioned policies to firewalls and gathers logging and reporting information.
3. **IPSec:** It is used for securing network traffic and transmitting policies. Here cryptographic techniques are used to verify a sender.

How distributed firewalls work

Most distributed firewalls are implemented at lowest level of the Open Systems Interconnection (OSI) model. A firewall monitors all traffic(Internet data and a company's internal data). A central policy is developed after installing the firewalls. It is then transferred to each firewall by the system management tool. A certificate from IPSec is used to determine the sender of the data. This can uniquely recognise the sender instead of relying on network topology like traditional firewalls. Then, the firewall evaluates data packets based on the central policy and sends logging information to the centre where it can be used for reporting purposes.

Features

Distributed networks do not always rank better in all aspects. They have some disadvantages as well. There are certain tasks that are performed better by traditional firewalls vis-à-vis distributed firewalls. Following are some of the criteria that help in determining the type of firewall required in an organisation: -

- **Network topology:** Traditional firewalls depend on the topology used in the network. The performance can go down due to a single checkpoint. Such flaws do not affect distributed firewalls.
- **Application level proxies:** Traditional firewalls have application level proxies (situated outside a network and transfer data between the Internet and the applications on a desktop). Distributed firewalls do not support this.
- **Intrusion detection:** Although traditional firewalls detect intrusions to a certain extent they do not check internal traffic. Distributed firewalls monitor internal traffic closely. However, a remote user may find the network slow because distributed firewalls send all the log information to a central location.
- **Inside attacks:** Since distributed firewalls are host dependent, they evaluate all the data traffic irrespective of the sender. Traditional firewalls do not monitor such traffic.
- **Central management and reporting:** Both types of firewalls use this method, but distributed firewalls focus on firewall policies and can divide the system in groups for easy management. In traditional firewalls this is not possible because there is only one policy for the entire network.

Answer: [a] Dependence on network topology

Module:4

Reference No:M4145

Question: Digital subscriber line access multiplexer (DSLAM) is used for:

- [a] High-speed data transfer
- [b] Developing efficient digital network over network.
- [c] Accessing remote computer
- [d] Synchronising protocols of different network.

Module 4 – Digital subscriber line access multiplexer (DSLAM)

Definition

To interconnect multiple Digital Subscriber Line (DSL) users to a high-speed data transmission, the telephone company uses a DSLAM. Typically, the DSLAM connects to an asynchronous transfer mode (ATM) network that separates the voice frequency signals from high-speed data traffic. It controls the traffic between end user gadgets (router, modem, Network Interface Card) and the network service provider.

DSL

Digital Subscriber Line can transfer high bandwidth applications efficiently. It can transfer 8 mega bytes per second. DSL supports high-speed Internet access, VPNs, telecommuting, full motion video across the globe and the like.

To implement this technology, service providers should have DSLAM in their network to interact with end user equipments and its location.

Benefits of DSLAM

DSL service can be more effective when accomplished with single integrated DSLAM platform. Most of the DSL systems are not synchronised with DSL technology. This leads service providers to:

- Deploy a limited DSLAM and ignore market segment.
- Install multiple DSLAMs from different vendors.
- Install multiservice DSLAM that can serve broadband access network.

Properties of multiservice DSLAM

1. Multiservice DSLAM supports multiple DSL transmission.
2. When coupled with high capacity asynchronous transfer mode (ATM), Multiservice DSLAM offer scalability, port density, and a redundant architecture for reliability.
3. Multiservice DSLAM offers full ATM switching, traffic management, and Quality Of Service (QOS).
4. Multiservice DSLAM also supports services like ISDN, IDSL, SDSL, rate adaptive DSL-Competitive Access Provider (RADSL-CAP) and RADSL-discrete multitone on a single platform.
5. Multiservice DSLAM assists in routing and security functionalities.

DSLAM Scalability

More the network elements more will be the cost of scalability in network management. Let us suppose that a DSL network requires four software upgrades, two schedule upgrades and two bug fixes each year. Each upgrade takes 2 hours to download and verify correct operation. If \$100 is the cost per hour then \$800 is the annual cost per network element.. This is only one aspect of management cost; others include installation cost, alarm monitoring and periodic maintenance.

Apart from this, there are hidden costs called Trunking cost. For example presently there are about 2000

DSL lines deployed at each central office. Let us suppose that career A's DSLM would require an optical carrier for 3 trunks of 500 lines and on the other hand career B's DSLM requires only one trunk line with 2000 lines. Career B can utilise high-speed trunks and can accommodate more traffic. So for career B high speed trunks have higher cost associated with it. DSLAM is costly, but nevertheless an effective step for high-speed connectivity.

Remoteability

It is the ability to deploy the minimum amount of technology required to synchronise with the demand. A DSLAM's remote solutions bring DSL capability into areas of:

- Message display units (MDU)
- Requiring multiple DSL lines e.g. in large remote terminal sites.

DSLM remote alternative may include remote line card shelf (RLCS) and remote access module. The Digital Subscriber Line (DSL) market will grow considerably between 2000 and 2004 and DSLAMs will play an integral role in the market's evolution. DSLAMs have evolved from simple traffic routers to encompass many different types of DSL as well as support for a variety of value-added services.

Answer: [a] High-speed data transfer

Module:4

Reference No:M4146

Question: A security management system should undertake _____.

- [a] Local data reduction
- [b] Event correction
- [c] Low resource utilisation
- [d] All of the above

Module 4 – Internet Security Management

Introduction

With the proliferation of distributed networks today, information security has become a critical issue. Firewalls, intrusion detection systems, Virtual Private Networks (VPNs) and security applications are needed to secure distributed networks. This creates a need for managing and integrating Internet security data. The extensive use of firewalls and other related devices have reduced security threats considerably, however it also leads to two main problems:

- A huge amount of data is produced by the use of these devices, and hence it becomes difficult to control and analyse the data.
- The manpower costs for monitoring the data are very high. There is also a lack of skilled manpower in this area.

Characteristics of a Security Management System

To take on security challenges, the security management system must have following features:

1. **Event correlation:** Each security device has a specific action (event) to control data. These events must be analysed and correlated to determine their impact on the system.

2. **Timely information management:** Real time information trapping and logging should be done so that the impact of security events is minimised.
3. **Local data reduction:** This is necessary because security devices produce large amounts of data, and therefore the security management system should:
 - Sort event alerts.
 - Follow priority rules.
 - Send only the relevant information to the security professionals.
4. **Integrated hierarchical structure:** Security devices and applications can be supplied by different vendors. The security management system should allow access and integration of all these devices and applications. This enables the administration to automate the security process through a centralised control over the devices.
5. **Low resource utilisation:** The security management system should be designed in such a way that the system resources are efficiently utilised. It should not have any adverse effect on the performance of the devices. At the same time, the regular operations carried out on the network should not be effected.
6. **Presentation of data and trends:** Presentation and distribution of security management information must be convenient and flexible enough to support the system. For this, the graphical interface and web technologies must monitor so that only relevant information is displayed.
7. **Flexible and scalable implementation:** The security management system should be flexible enough to accommodate the needs of an enterprise. It should be in accordance with devices that allow proliferation of security and should also suit the changing enterprise structure.

Architectural structure

Software for automation of Internet security management is available in the market.. This software provides an open interface for network systems and security products. In addition, it enables easy expansion of networks to assist enterprises in installing additional firewalls and other security devices. The following are some of the features of system security software:

- It comprises built-in management activities like file management to control the internal working of the software itself.
- Depending upon the requirement, the security administrator can define actions and incorporate them into the software.
- Multi-host actions i.e. the administrator can specify a single server, multiple servers, or multiple security devices on which the action is to be performed.

Answer: [d] All of the above

Module:4

Reference No:M4147

Question: What happens when the Session Manager opts for a persistent session?

- [a] Session data is stored permanently in the database
- [b] Session data for each transaction is stored in the database
- [c] Session data is stored in the memory for a limited time
- [d] Session data is not related to a persistent session

Module 4 – Session Manager

Session refers to the state in which the user's desktop is. It provides information about applications presently in use, location of windows, windows opened by each application, position of current cursor and so on. It is important for users to save their session, before logging out.

When the user logs in again, the application should be just as it was, before he logged out. This is possible only when applications can record and restore these properties, which are generally not controlled by the Window Manager. The Session Manager controls this activity.

The Session Manager is a collection of packages that brings together all the session providers as a single interface. It uses the Session Interface as a base class, which is easy to learn and re-use.

During a session, a communication channel is established between two entities. The first entity known as the initiating entity creates a session, and the second entity known as the domain can be any thing from a tree to a server. Sessions therefore establish a means of communication between two objects.

On establishing a singular session, an object can communicate with another object in the same domain. The domains could be hierarchical, with child domains narrowing the scope of the parent.

A session by itself is at the top-level of the hierarchical tree and ties all session providers together. Two different sessions can have same domain name, unless the parents are different.

Multi user Session Manager

Here, the Session Manager allows more than two different sessions in the same domain. It is capable of providing multiple distinct authentications simultaneously to the same domain.

Properties

Base memory size: It specifies the number of sessions to be maintained in memory. It depends on two types of sessions.

(a) **In-memory sessions:** The number of possible sessions is specified in the base table. The 'Allow Overflow' property is used to indicate whether to limit sessions to this number for the entire Session manager, or permit additional sessions to be stored in secondary tables.

(b) **Persistent Sessions:** It indicates the size of the cache data. The number of session updates that will be cached, depends on the Base In-memory Size . If the Session Manager is more than this size, then it reverts to reading session updates from the database automatically. This is possible only when cache property is enabled.

Base Memory Size in Use: It specifies the current value of the Base Memory Size.

Cookie Comment: It provides information about the cookie.

Enable Persistent Sessions: It specifies whether to save session data in a database, or delete the session data when the server shuts down.

Yes - The session data is stored in a database for each session transaction.

No - The session data is kept in memory for a single instance of the servlet engine.

Allow Overflow: It specifies whether the number of sessions in memory should be more than that specified in the Base In-memory Size .

True: Allows overflow

False: Limits the number of sessions in memory to Base In-memory Size

Allow Overflow in Use: Specifies the current value of Allow Overflow property.

Answer: [b]- Session data is stored in database for each transaction

Module:4

Reference No:M4148

Question: Which of the following is true regarding Remote Authentication Dial-In User Service (RADIUS): -

- [a] It can authenticate a single client at a time through a centralised database
- [b] It can authenticate multiple clients at a time through a decentralised database
- [c] It can authenticate multiple clients at a time through a centralised database
- [d] It can authenticate a single client at a time through a decentralised database.

Module 4 - Remote Authentication Dial-In User Service (RADIUS)

Introduction

Using a modem for network communication makes the network vulnerable to security especially if it is too large. To overcome this problem, a protocol called Remote Authentication Dial-In User Service (RADIUS) was identified and a suitable system was developed for the same. RADIUS is a distributed security system on the Internet (it allows authentication of multiple client identity through a single central authentication server or database). RADIUS eliminates the need for special hardware and meets the security requirements of distant computing by protecting the network from unauthorised access.

RADIUS Client/Server Architecture

RADIUS is a protocol supporting client-server concept that contains two parts:

- Authentication server
- Client protocols

RADIUS Client is a Network Access Server (NAS) while RADIUS Server is a daemon process (computing a background process that handles requests for services such as print documents, file transfers etc.) running on Windows or UNIX machines. All the information regarding client queries is stored on the RADIUS authentication server. The RADIUS client transmits user queries to the RADIUS server. The server first authenticates the user, before it responds to any query, and then sends the details corresponding to that query.

Working of RADIUS

The process passes through the following stages:

1. The user make use of a modem to establish a dial up connection with the port master communication server (PortMaster is a Internet based software application that allows automatic collection and analysis of real time information. It also allows the user to access an on-line centralised database). The PortMaster then prompts the user for the username and password.
2. The PortMaster generates data packets for the above information (username and password), and for the port number used for the modem connection. For security purposes, PortMaster acts as a RADIUS client and encrypts the password before sending it to the RADIUS server.
3. The data packets are transmitted from the RADIUS client to the RADIUS server via a Local Area Network (LAN) or Wide Area Network (WAN). This will allow the network manager to know the status of the RADIUS client. If the radius server is not located then the RADIUS client re-routes the request to another server.
4. After the Authentication Server receives the request, the validation and decryption process takes place. This is done to access the username and password to authenticate the user. This information is then passed on to a suitable security system (like Kerberos which is a custom developed security system), and UNIX password files etc.
5. The authentication sever checks the username and password for its correctness and sends an acknowledgement to the PortMaster. It contains information regarding:
 - Service requirements
 - The user's network system
 - Resources on the network available to user

On the other hand, if the username or password does not match with the stored details, the RADIUS server sends the rejection details to the PortMaster. As a result, user access to the network is denied.

Benefits of distributed security

1. **Greater Security:** The RADIUS client/server architecture enables all security related information to reside on a central database rather than scattering it over the network at different locations. This will increase security.
2. **Open protocol:** RADIUS is an open protocol i.e. it can be easily synchronised with other protocols, systems or communication devices that are already in use. It saves a lot of time and increases the flexibility of the system by just modifying the RADIUS according to the network rather than configuring the network.
3. **Future enhancements:** Technology is changing at an incredible pace, because of the amount of research done to increase security, and new security initiatives are introduced to secure the applications. Any new security initiatives can be used by adding to it the RADIUS server by the customer or the resource.

Answer: [c]- It can authenticate multiple clients at a time through a centralised database

Module:4

Reference No:M4149

Question: In Telecommunication Management Network (TMN) logical model, which layer supports decision-making process at high level?

- [a] Network-Management Layer (NML)
- [b] Network-Element Layer (NEL)
- [c] Business-Management layer (BML)
- [d] Service-Management Layer (SML)

Module 4 – Telecommunication Management Network (TMN)

Introduction

Telecommunication Management Network (TMN) assists in providing communication and interconnectivity among different operating system and telecommunication networks. TMN has enhanced the flexibility and scalability of the network by standardising the conduct of network management and communication over network. TMN works with telecommunications network to exchange information and share resources among themselves.

Components of TMN

There are six components that work together to run the system:

1. **Operations system (OS):** It assists in monitoring the operations and controlling all the functions of operations system and telecommunications system. It even performs some of the functions of mediation device (MD), Q-adapters (QA) and Workstations (WS).
2. **Mediation device (MD):** It acts as a mediator between local TMN interface and OS. It also ensures the functionality and scope of the process, the way OS expects.
3. **Q-adapters (QA):** It allows TMN to control NEs with non-TMN interfaces. QA render between TMN and non-TMN interfaces.
4. **Network elements (NE):** The information in NE should be controlled and managed by OS, within the scope and limits of TMN. A standard interface is necessary for NE to avoid management via Q-adapter.
5. **Workstations (WS):** It translates information from TMN format to user-friendly visible format.
6. **Data Communication Network (DCN):** It is a communication network within the premises of TMN and represents Open System Interconnection (OSI) layers 1-3 i.e. physical, data-link and network layer.

TMN Logical Model

This model has been divided into number of logical layers, which recommend the management level for a particular function. These layers are hierarchical and are formed on the foundation of the layer preceding it. These layers and their functionalities are as follow:

- **Business-Management layer (BML):** This is used for top management planning and decision-making. It is also concerned with budgeting, goal setting and business-level agreements (BLAs).
- **Service-Management Layer (SML):** It acts as a junction of providing service to customer regarding customer account, fault management and the like. Interaction with service providers and administrative domains also take place at SML.
- **Network-Management Layer (NML):** It overlooks the entire network and is based on the information offered by Element Management Layer (EML). NML controls all the network activities and supports the formation of next layer i.e. SML.

- **Element Management Layer (EML):** The element manager of EML manages each and every network element. It also controls network data, logs and activities. Mediation devices communicate with EML even if MDs are located physically at some other layer like SML or NML. This communication is possible only via Q3 interface.
- **Network-Element Layer (NEL):** It presents the information managed by TMN in the form of network elements.

Tools for Telecommunication Management Network (TMN)

For automating TMN process number of tools are available in the market. In order to maximise the advantages of TMN

· It should support dynamic information modelling i.e. altering network configuration without re-installing or re-implementing the applications.

- It should support automatic prototyping.
- It should be in accordance with all TMN standards.
- It should be platform independent.

Answer: [c]- Business-Management layer (BML)

Module:4

Reference No:M4150

Question: The primary purpose of Quality of Services is to

- [a] Provide efficient services of all applications in the network
- [b] Provide preference to large flows
- [c] Improved services to specified flows
- [d] Give equal preference to all resource

Module 4 - Quality of Services (QoS)

Network traffic includes traffic, which arises due to the use of different technologies that flow through the network. Different technologies may be Frame Relay, Ethernet, Sonet, Asynchronous Transfer Mode and IP routed technologies. Depending on the necessity, one technology would be preferred over other. In such circumstances, the required technology should work very efficiently without affecting the functionality. In short, the aim of QoS is to prioritise flow without leading to the failure of others. A flow can be defined as a combination of source and destination addresses, source and destination socket numbers, and the session identifier or broadly as any packet coming from any application or an incoming interface.

QoS Concepts

QoS facilitates improved service to specified flows. It raises the priority of a flow or limits the priority of another flow. Congestion Management tools are used to raise the priority of a flow by queuing and servicing queues in different ways.

- Queue Management tool avoids congestion, raises priority by dropping low-priority flows in favour of high-priority flows.
- By policing and shaping, a flow is prioritised by limiting the throughput of other flows.
- Link efficiency tools give preference to small flows over large flows.

QoS can also be thought of as a toolbox. It gives different options to deal with a situation. It depends on the user to choose the best one. For instance, when a hole is to be drilled, one opts for a drill and not a hammer. QoS also helps in lessening congestion problems.

Benefits:

QoS tools help in controlling and servicing a variety of complex networks and networked applications and traffic types. Irrespective of type of network (small corporate network or an Internet service provider), any network can work at its optimum level with the help of QoS tools. Different ways by which a network can benefit from QoS tools:

- **Resource Control:** A control can be established over various resources such as bandwidth, equipment, wide facilities and the like. For illustration, bandwidth can be limited by providing FTP transfer or more priority can be given to database access over other features.
- **Efficient Use of Network Resources:** Information can be prepared using network analysis management and accounting tools to determine what the network is being used for and accordingly the traffic can be prioritised.
- **Customised Services:** Demarcated services are provided carefully to customers by the Internet Service Providers due to QoS.
- **Coexistence of mission-critical applications:** QoS technologies ascertain that WAN is effectively used by mission critical applications in the business and bandwidth, minimum delays are available to time sensitive multi media without interfering mission critical applications.

Answer: [c]- Improved services to specified flows

Module:4

Reference No:M4151

Question: Which of the following tool allots a specific amount of space to packets to handle traffic effectively?

- [a] Priority Queuing
- [b] Custom Queuing
- [c] Weighted Flow Queuing
- [d] FIFO, Basic store and forward capability

Module 4 – Congestion Management Tools

When the rate of traffic flowing through the network is higher than that allowed by the network resources, it leads to congestion. Congestion may occur when the switches in a network, having a limited buffer storage receive packets more than their capacity.

This problem is effectively dealt by network elements by using a queuing algorithm. The queuing algorithm sorts the traffic and then determines a method of prioritising it onto an output link. The queuing algorithm is a solution that is designed on the basis of problems specific to network. The queuing algorithm is effective only when there's congestion. In the absence of congestion all the packets are delivered directly to the interface.

Some of the queuing tools are as follows:

FIFO: Basic store-and-forward capability

When the network is congested, FIFO stores the packets and then sends the packets in the order of their arrival. This process continues until the network congestion is eased. FIFO some times comes as a default queuing algorithm and therefore does not require any configuring. But FIFO has its shortcomings:

- It does not formulate any decision about packet priority.
- Some sources can create long delays in transferring time-sensitive application traffic.FIFO cannot differentiate between high priority packets and low priority packets, and cannot decide on dropping the low priority packets.

PQ: Prioritising traffic

The PQ is designed to prioritise thus ensuring that important traffic is attended very quickly at every point. Priority queuing can be customised according to network protocol such as Internet Protocol, Apple Talk incoming interface, packet size, source/destination address and the like.

PQ classifies each packet in four queues on the basis of assigned priority. When the packets are being transmitted the algorithm gives more preference to higher priority queues over the low priority queues. The four queues are:

- High
- Medium
- Normal
- Low

This way PQ assures that mission-critical traffic traversing various WAN links gets priority treatment. An example is Oracle-based sales reporting which is transmitted ahead of other less-critical traffic.

CQ: Promised Bandwidth

Custom Queuing (CQ) permits various applications or organisations to allocate the network among applications with restricted minimum bandwidth requirements. The bandwidth is shared proportionally among the users and applications and guaranteed bandwidth is provided at congestion point. It specifies a certain amount of queue space to each class of packets and then services the queues in a round-robin fashion, thereby handling the traffic effectively.

Flow-Based WFQ: Creating Fairness Among Flows

In circumstances where it is desirable to provide a steady response time to heavy and light network users in the same way without any addition of excessive bandwidth, flow-based WFQ is employed. WFQ services fairly to each queue in terms of byte count. For example, if queue 1 has 100-byte packets and queue 2 has 50-byte packets, the WFQ algorithm will take two packets from queue 2 for every one packet from queue 1. This makes service fair for each queue- 100 bytes each time the queue is serviced. WFQ ensures that queues do not suffer due to lack of bandwidth and gives traffic a predictable service. This means low-volume traffic streams—which comprise the majority of traffic—receive increased service, transmitting the same number of bytes as high-volume streams. .

Answer: [b]- Custom Queuing

Module:4

Reference No:M4152

Question: A concept in geometry, that gives you the location of a point, given its distance from three other points is-

- [a] GPS
- [b] Trilateration
- [c] Pseudo random code
- [d] Satellite Signals

Module 4 – Global Positioning System (GPS) Receiver

GPS receiver is a device which tells you the exact location of itself. In other words a person having a GPS would know exactly where he is on the planet. It gives the position in the form of co ordinates for latitude, longitude and altitude. For a GPS to function, identifying a minimum of four satellites overhead is a must. This means that at least four satellites should be able to track it.

Working

The GPS uses the principle of **trilateration** to determine the location. For instance, if you are lost, and know that you are in a circle of 10kms from a pond (circle **a**), then you find that you are at milestone, which is at a distance of 11km of from the nearest town (circle **b**) and you 15km from another town (circle **c**). From these three points you can know your exact location which is the point of intersection of the three circles.

Trilateration is a geometric concept, which tells you the point, given its distance from three other points. This is basically two dimensional. The same principle is used in GPS, but in a three-dimensional space. GPS also uses spheres instead of circles. Therefore the GPS needs to know the distance from four satellites to know the exact location (the fourth satellite to give the information of altitude).

The GPS consists of 24 satellites, which orbit the earth. The GPS receiver gives the exact location in terms latitude, longitude and altitude anywhere on the Earth.

Measuring Distance: Radio signals sent out by the GPS satellites are detected by the GPS receiver. To know the distance of the satellite, the receiver measures the amount of time the signal takes to reach it from the satellite. Since we know that radio signals are electromagnetic waves which travel at the speed of light in vacuum (186,000 miles per second) we can find out the distance travelled by estimating the time taken to arrive at the receiver.

This can be easily determined if the exact time of signal leaving the satellite and reaching the receiver is known. Installing accurate and synchronised clocks in the satellites and receivers could do this.

The satellite transmits a long digital pattern called **pseudo random code**, as a part of its signal at a particular time. The receiver also begins to run the same digital pattern at the same time. When the signal reaches the receiver, its transmission pattern will lag behind the receiver's pattern. The length of the delay is equal to the time of the signal's travel. This time when multiplied with the speed of light gives the distance travelled by the signal.

Such level of accuracy is possible only with atomic clocks, which are required not only on the satellites but also on all the receivers. This could make them pretty costly.

To counter this problem, the receiver has a normal quartz clock. It calculates the exact time and location simultaneously and determines the intersection points of the four spheres as explained above. If the measurement were done incorrectly then the spheres would not intersect. Since the receiver makes all the calculations, the measurements obtained would be proportionately incorrect and by making distance adjustments the receiver can cause the four spheres to intersect at one point. Adjusting its clock to match with the measure of distance does this.

Since the earth atmosphere is not vacuum, it slows down the transmission of the signal. To counter this, a GPS receiver guesses the actual speed of the signal using complex mathematical models for a wide range of atmospheric conditions.

Determining The Satellites: To determine where the satellites are positioned, the receiver stores an index having the information of the position of every satellite at any given time. Any slight change of their position due to the pull of sun, moon or earth is constantly monitored and adjustments are transmitted to the receiver as a part of the satellites signals.

Applications

A receiver can be used for the following applications:

- Shows the exact position on the map at any particular location.
- It can trace the path moved across the map.
- The distance travelled.
- How long one has been travelling.
- The speed at which one is travelling.
- The estimated time of arrival to destination, if moving constantly at the same speed.

Answer: [a]- GPS

Module:4

Reference No:M4153

Question: Which of the following is incorrect with regard to IP multicasting?

- [a] It distributes large amounts of data.
- [b] It reduces the choking of bandwidth, due to high data traffic
- [c] It requires additional resources for efficient delivery of data
- [d] It is a group concept

Module 4 – IP Multicasting

The increased usage of Internet based applications, such as video conferencing, corporate communications, distance learning, distribution of software, stock quote and news has proportionately increased online traffic. In consequence, the bandwidth is getting choked because multiple streams of information that have to be transmitted. This problem can be efficiently dealt by using multicasting.

Multicasting helps in distributing large amounts of data better than existing ways of sending data, because it can broadcast the same message to many recipients simultaneously. It does not require separate connections

for each source-destination pair. Rather it shares the same source. This means that just one set of packets is transmitted. The IP multicast uses the available network bandwidth of any technology, without adding any extra load to source or destination. It delivers source traffic to multiple receivers

Routers enabled with Protocol Independent Multicast (PIM) and other protocols, which support multicasting, replicate multicast data packets. The source sends one copy of data for replication. Sometimes, the source may have to send an individual copy to different destinations through routers. High bandwidth applications such as MPEG (Motion Pictures Expert Group) video capture a large portion of network bandwidth for a single stream. If more than one receiver needs them, then again the only way to delivery is by using IP multicast packets.

Multicast group

Multicast is primarily a group concept. A group can be located in any part of the world, yet it can receive a specific data stream. Different groups are formed, depending on their addresses.

1. IP multicast addresses: Multicast addresses specify a group of IP hosts who want to receive traffic. When a host want to receive data that is being transmitted to a particular group, it must joins it using IGMP.
2. IP class D addresses: The IANA, Internet Assigned Numbers Authority is responsible for assigning IP multicast addresses. Groups are assigned the addresses in the range of 224.0.0.0 to 239.255.255.255.
3. Reserved link local addresses: Addresses are reserved from 224.0.0.0. to 224.0.0.255 to be used by the network protocols on the local network segment. Routers do not forward packets with these addresses. They therefore remain locally on a particular LAN segment. These addresses are used for automatic router discovery, and to communicate important routing information.
4. Globally scoped addresses: Addresses from 224.0.1.0 to 238.255.255.255 are referred to as globally scoped addresses. These are used to multicast data between organisations and over the Internet.
5. Limited scope addresses: These addresses range from 239.0.0.0 to 239.255.255.255, and contain,limited scope addresses or administratively scoped addresses. Routers do not allow multicast traffic in this range to move out of the user defined domain or Autonomous System (AS).

A host joins a multicast group, by sending out Internet Group Management Protocol (IGMP), which is then registered dynamically using LAN. An IGMP membership query is sent by the router periodically to verify whether at least one user on the subnet is interested in receiving traffic directed to the group. When there is no reply from the group, the router times out. and stops forwarding traffic to that group.

Answer: [c] Requires additional resources for efficient delivery of data

Module:4

Reference No:M4154

Question: Which of the following is NOT a Top-Level Domain (TLD)?

- [a] com
- [b] mil
- [c] net
- [d] co

Module 4 - Domain Naming Service (DNS)

The Domain Naming System is the world's biggest, most active and widely distributed database. It is responsible for converting IP addresses to domain names. Domain Name Services (DNS) is an application layer protocol that is part of the standard TCP/IP protocol suite.

On a network as vast as the Internet it would be impractical to identify each system solely by its numeric IP address. For example, the IP address of the server hosting the web site "www.themanagementor.com" is 202.140.141.11. Remembering the IP address of even a few web sites becomes highly difficult. So, every IP address is mapped to a unique name called the domain name.

The Internet's domain name servers (DNS) translate the human-readable domain name into the machine-readable IP address. During a day of browsing and e-mailing, one person can access the domain name servers hundreds of times. There is always a huge load on DNS servers since:

- There are billions of IP addresses currently in use, and most machines have a human-readable name as well.
- There are many billions of requests made from domain name servers every day. A single person can easily make a hundred or more DNS requests a day, and there are hundreds of millions of people and machines using the Internet every day.
- Domain names and IP addresses change daily.
- New domain names get created daily.
- Millions of people do the work to change and add domain names and IP addresses every day.

The DNS system is a database, and no other database on the planet gets this many requests. No other database on the planet has millions of people changing it every day, either. That is what makes the DNS system so unique!

To make a distinction among the category to which each of the web sites belong to and for administrative purposes, domain names have been assigned different extensions. The com, edu, org, net of these domain names are called the **top-level domain** or **first-level domain**. There are other several hundred top-level domain names, including gov, mil, and int, as well as unique two-letter combinations for every country. Within every top-level domain there is a huge list of **second-level domains**. For example, in the com first-level domain, there are many domains such as themanagementor, yahoo etc, each of which may have many sub domains like mail.themanagementor.com, mail.yahoo.com and so on. Sub domain names may go up to 127, although 3 is more common and four is rare. An example of a sub domain having 3 names is **bbc.co.uk**.

However, every name in the top-level domain must be unique, although the names in different top-level domains may be the same. For instance, www.themanagementor.com and www.themanagementor.org are two valid names and refer to different web sites.

Since all names in a given domain must be unique, there has to be a single entity that controls the list and ensures that there is no duplication of names. For example, the com domain cannot contain any duplicate names, and a company called Network Solutions is in charge of maintaining this list.

Answer: [d] co

Module:4

Reference No:M4155

Question: How is the DNS implemented on the client side?

- [a] Through "Binding"
- [b] Through "Resolver" programs
- [c] Through "Virtual hosting"
- [d] By registering with a "registrar" company

Module 4 – Domain Naming Service (DNS) – Part II

The Domain Naming System (DNS) is responsible for converting IP addresses to domain names. The previous article discussed the basic concept of how a DNS system works. When you register a domain name, it goes through one of several dozen "registrars" who work with Network Solutions to add names to the list.

However, if someone owns a top-level domain such as Microsoft.com, he is responsible for maintaining the database of all the sub-domains under the main domain. This makes the DNS database a distributed one.

Domain Name servers:

- Accept requests to convert domain names into IP addresses.
- They accept requests from other name servers to convert domain names into IP addresses.

When a request comes in, the DNS server does one of four things with it:

- It can answer the request with an IP address because it already knows the IP address for the domain.
- It can contact another name server and try to find the IP address for the name requested. It may have to do this multiple times.
- It can provide the requesting entity the IP address of another DNS server that contains more information about the requested domain.
- It can return an error message because the requested domain name is invalid or does not exist.

When a user types an URL into the browser, the browser converts the URL into an IP address by querying the DNS Server and then requests a Web page from the machine at that IP address. When connecting to the Internet, the ISP takes care of the DNS name resolution.

For instance, when a company XYZ wants to put up a web site, it first registers its name with the registrar. Then it finds a web hosting company and puts its web site on the hosting company's machines or puts the web site on its own servers. Then it has to include this domain name-IP address pair in the DNS server given by the hosting company or the ISP, i.e., when hosting a web site, the company should specify a name server that will resolve any requests. Only then can someone access the web site. However, a single machine can host many sites with a feature called "virtual hosting."

The domain name-IP address information has to be registered with the DNS name server. This is typically done by a technique called "binding." On the client side, DNS is implemented through the resolver. The resolver is not a program, but a library compiled into applications that need to know machine names. The resolver's function is to resolve user's queries. To do that, it queries a name server, which then returns either the requested information or a referral to another server.

In summary, the DNS system is responsible for the smooth working of the Internet, since it allows millions of computers to connect to each other without using complex numbers.

Answer: [b] Through "Resolver" programs

Module:4

Question: Which of the following is NOT a security option of Internet Information server 4.0?

- [a] All scripts and executable programs must be thoroughly tested for wrong input given with malicious intent
- [b] Enable Secure Sockets Layer (SSL)
- [c] Use NT File System (NTFS) instead of using File Allocation Table (FAT file system)
- [d] If multiple sites are being hosted using virtual directories, they have to be appropriately segregated

Module 4 – Internet Information Server Checklist

Internet Information Server (IIS) from Microsoft is an industrial strength web server for use by small businesses and very large corporations alike. It runs on the Windows NT Operating System, also from Microsoft.

To harden IIS from attacks, some settings have to be modified in the configuration. Since IIS and Windows NT are tightly integrated, it is necessary that some changes are made to the operating system as well, to ensure a more secure environment for running IIS.

The following questionnaire can be used to check whether all possible security options have been set or not.

Windows NT Checklist

1. Latest Service Pack and Hot-fixes applied
2. Use NT File System (NTFS) instead of using File Allocation Table (FAT file system)
3. Set NTFS Access Control Lists
4. Disallow the 8.3 file naming convention
5. The OS offers variable time to boot and can be set by the administrator. This must be set to zero seconds
6. The optional OS/2 Subsystem has to be removed
7. POSIX Emulator must be removed
8. File shares must be unshared and port 139 (file sharing) must be closed
9. Logging for success or failure of login attempts must be turned on
10. Do not display the last user who has logged on
11. When the logon box is displayed, a legal notice advising the user of the terms of using the system must be shown
12. The logon dialog box has a "shutdown" button that must be disallowed
13. The default account "guest" has to be removed
14. Create an account with administrator privileges, and remove all administrator privileges from the old "administrator" account. Most attacks start by assuming the user name of the root as "administrator" and can be prevented in this way
15. The administrator password must be very strong and follow best practices. Password crackers may be used to test the strength of the password
16. Disallow access to registry by normal users
17. Password for all users must have some minimum characters
18. Password aging must be turned on
- I. he option of accessing the server from any computer must be changed from the default "everyone" to authenticated users only
20. Disable NetBIOS from the "Network" option in the control panel
21. Turn off the IP routing feature

Internet Information Server 4.0 Check List

1. Run only the Internet services required and remove other services. FTP must be turned off compulsorily if not FTP service is being run
2. Authentication to access directories or files must be turned on
3. If multiple sites are being hosted using virtual directories, they have to be appropriately segregated
4. All scripts and programs that have executable content must be placed in a directory with "read" and "write" permissions turned off. Only execute permission must be given
5. All scripts and executable programs must be thoroughly tested for wrong input given with malicious intent
6. Enable Secure Sockets Layer (SSL)
7. Map Client Authentication Certificates to Windows NT Accounts
8. Enable logging of user requests to determine hacking attempts and also to find out statistics on the number and type of users visiting the site
9. The Index Server, which is part of the IIS installation, allows the web site to be searchable. Caution must be taken to see that the Indexing service indexes only appropriate content and does not throw up the entire source code of scripts and programs
10. IIS comes with some sample programs to test various features. Once the Server is running properly, all these sample applications must be removed, since many of them have serious security flaws

Answer: [c] Use NT File System (NTFS) instead of using File Allocation Table (FAT file system)

Module:4

Reference No:M4157

Question: In a thin client networking model

- [a] Database is available in server and application and the user interface is available on the client.
- [b] Database is available on the client; application is available on the server
- [c] Database and application are available on the server and user interface on client.
- [d] Database, application and user interface are available on server

Module 4 - Thin Client Network

Concept

The thin client-networking model is based on a centralised processing concept. In a traditional network, the database is located in the central server while the application and the user interface is available on the client that is used to process the data. As against this, in the thin client networking the application is also stored centrally and only the user interface is available in the client workstations. In such an environment all the applications are processed in a centralised server and the image is provided to the workstation or a thin client device. The clients are almost reduced to dumb terminals in this model of networking.

Components

As in any traditional network the components of thin client network are

1. Network Architecture
2. Server
3. Thin client device
4. Software

Network architecture: The thin client networks need a high bandwidth network as the server processes all the applications. Even small activities like mouse movements are sent from the server to the thin client. Hence a high Quality LAN is a must in a thin client model. Individual network capacities may depend on the user requirement but graphical applications generally consume high bandwidth and hence multimedia applications and those like CAD and CAM may not be suitable for a thin client environment.

Server: Presently two types of servers are used in a thin client network - windows based servers or UNIX servers.

Thin client device: Any device connected through the thin client network protocol (rules and standards prescribed for data communication and transmission between computer) can be called a thin client device. These correspond to the workstation (or now distinguished as fat client) in a traditional network or a client server environment. Easily distinguishable features between normal clients (that is fat clients) and a thin client is that, thin client does not have any hard drive or floppy drive. They have a minimum of applications, enough to run a PC or a desktop and user interface applications for the operations of the thin client. However even clients in a normal traditional network can be converted to thin clients.

Software: Most types can be utilised in a thin client environment. However graphic or multimedia software may not be ideal in a thin client-computing model.

Advantages of a thin client model

Simplicity of installation: Installation of a new user in a thin client is very simple. Since the thin client does not have or has minimal processing capabilities, installing a new user becomes simple. It can be installed instantly by just plugging the network cable into the network.

Security: As the processing is centralised, this networking model provides high levels of security for the data and information. Since all the applications are stored in the server it is not necessary to monitor the clients individually. And due to the absence of drives in the thin client, no data monitoring is required. High levels of security can be provided centrally by proper maintenance of the server centrally.

Flexibility: All up gradations to the software and applications can be made centrally. The network can also adopt any new technology centrally.

Maintenance: Any new client can be replaced immediately and the operations from that client will not be hampered. Replacement time can be reduced drastically.

The simple architecture of the thin client leaves little scope for system failures. In event of failure, replacement can be made instantly. Even the operations can be easily resumed in case of interruptions in the working of the client, for instance power failure.

Answer: [c] Database and application are available on the server and user interface on client.

Module:4

Reference No:M4158

Question: ----- is a component of virtual office.

- [a] Internet access
- [b] Cellular communications
- [c] Groupware
- [d] All of the above

Module 4 – Remote Accessibility-overview

The technological advancement in computing and communication has removed the locational barriers. This has ushered in the concept of virtual office -anywhere, anytime office - which is fast picking up.

Components

The components of a remote accessibility (virtual office) are)

1. Portable computer
2. Remote accessibility of data
3. Telecommunications and cellular communications
4. Mail systems
5. Internet Access
6. Groupware

Using the above components a virtual office or a virtual work location can be created. The work location can be practically created anywhere at homes, corporate offices, on flights.

The benefits of such a virtual network include increased output from employees due to flexible work hours, reduced costs to both employee and office. The costs of a workplace can be greatly reduced due to decrease in rental space, decrease in hardware costs and the like. The employees too can save on transportation costs to begin with.

Security

The security issues involved in a remote accessibility are

1. Hardware Security
2. Dial in protection
3. Information privacy
4. Information integrity
5. Threats through remote accessibility and internet access

Planning and Conducting Audit of remote work areas.

As in any other areas, the audit of remote accessibility (virtual office) includes both components of effective implementation and the system user's role.

The audit approach must include an understanding of the control environment. In this regard both technical security controls and the general controls should be considered. Like in any review, the auditor needs to determine the reliability of the control environment. The review process in particular should include the following components.

1. Organisational managements
2. Controls with regard to system and application programme changes
3. Network security controls including access controls
4. Database security controls including access controls
5. Risks associated with IT acquisition. The acquisition may include hardware, software and communication network.

Technical Issues

Access controls: As the virtual office provides remote access practically to anybody, access controls assume significance here. Access control mechanisms like encryption, passwords and PIN become the key technology components.

Virtual network: Another key element in the audit of virtual office is the network. Since interfaces involve various networks and use of various protocols, it adds complexity to security issues and the associated risks. These controls also need to be taken care of while auditing remote accessibility

Internet Access: Since the virtual office employs the medium of dial up Internet access, the associated Internet risks also crop up during the audit of virtual office. The control issues pertaining to these also need to be addressed by the auditor. Since virtual access is available to non-technical persons not familiar with communication risks, the risks are that much higher in a virtual audit.

Hence technical audit reviews need to be conducted in the early phase of the virtual audit. Some of the sample technical issues involved are addressing implementation of domain trust relationships in a group of systems like Windows NT, Netware and the like or the audit could address the controls with regard to Virtual Private Networks.

Answer: [d] All of the above

Module:4

Reference No:M4159

Question: A major problem in networking is the slow rate of data transfer. Which of the following would help counter this problem?

- [a] Data formatting
- [b] Decentralised control
- [c] Allocating adequate bandwidth
- [d] All of the above

Module 4 - Networking- problems and solutions

Introduction

Nowadays, with the increasing use of Internet, networking is expanding tremendously. At the same time the problems to control networks is also increasing. Currently network manager are facing two major problems:

- Managing increasing complexity of network.
- Efficiency of a system to search for relevant information.

Some of the problems related to inefficiency of the network elements to properly coordinate the data elements are:

1. **No control over bandwidth allocation:** Bandwidth is rate of data transfer over the network (in bits per second). Applications (photos, word document, video) need different bandwidth for transfer. Network should quickly allocate the necessary bandwidth for the application for successful transmission of data.
2. **Costly, slow administration and management:** In a decentralised network, managing network will get fragmented. Configuration management becomes very expensive. For example a software program is running on hundreds of machines and needs updating. If the process is not automated then we need to do updating on each machine and it will increase cost.

3. **Lack of consistent security:** By connecting different components together, the problem of security also increases. For example:
 - There should be only one password per entity.
 - Virus protection by using anti-virus packages.
4. **Lack of consistent network policy:** To synchronise the total network policy, there should be centralised network policy.
5. **No control over user:** Network cannot restrict user to access during critical situation. For example if some videoconferences is undergoing on net, then network cannot restrict user to use non-essential e-mails or search, until the necessary bandwidth had been released.
6. **Slow corporate response:** If the network is not responding to the queries at time, business may be lost. In this scenario if changes are to be made, they should be made quickly. Failing to do so will give advantage to competing organisations.
7. **Inaccurate data:** The customer's data is spread over decentralised database. Any change may not be reflected in other relevant database. It will lead to incorrect information.
8. **Unnecessary duplication of data:** Company have to incur cost for unnecessary duplication of records. Storing the data at a single place will not only reduce cost but also prevents inconsistent use of stale versions.
9. **Incompatible data format:** The data stored in different database will be in different format. Converting those formats of applications into readable format will increase the cost as well as errors in the application.
10. **Lack of personalisation:** When the customer places the order, it is important that all the information related with that customer is available to the respective applications at the time of entry. If it is not so then organisation may loose not only the sales but also the customer.

Measures to solve networking problem

1. **Fast corporate response:** Speed of Internet is mandatory in today's corporate environment. Quick integration of new technology into the network and ramping out old technology from the system is beneficial for organisation.
2. **Policy-based Enterprise network:** Appropriate policy is to be deployed for usage of bandwidth. For example if more bandwidth is needed for some important transmission, then web applications will be either slowed down or come to halt.
3. **Fast cost effective administration and management:** Centralised network management is more cost effective. Configuration management can be easily implemented and errors in a network can be easily identified and corrected.
4. **Consistent security policy:** It will allow all customers and employees to have their own password. Any incoming e-mail or file transfer is first scanned by anti virus package to avoid any malicious code to enter the machine.
5. **Logically compatible data formats:** It allows all the applications to have a single view of all the corporate data. It will reduce maintenance cost and errors.
6. **Customer personalisation:** If the organisation is able to logically relate all the information associated with a customer then it will allow organisation to give better service to customer and generate revenue.

Answer: [c] Allocating adequate bandwidth

Module:4

Reference No:M4160

Question: The communication between a single host and multiple receiver is :

- [a] Anycast
- [b] Multicast
- [c] Unicast
- [d] Dualcast

Module 4 – Internet Protocol v 6

Internet Protocol Version 6 (IPv6) is the latest Internet Protocols standard used across the world in TCP/IP based networks. This is going to replace the widely used IP v 4. The need for IPv6 arises due to lack of addressing. This is because of a number of large blocks of addresses being allotted to different government agencies and very large organisations. This would ultimately mean that after some time we would be running out of IP Addresses. To solve this problem we use the IPv6 protocol in our networks. This doesn't mean that IPv6 is a fitting super set of IPv4, instead it's a replacement for it.

The nodes, which uses either IPv6 or IPv4 have to have an implementation of both and should therefore implement both the protocols.

For IPv6 to forward a packet of IPv4, it treats IPv4 Internet work as a link layer. The IPv6 packets are encapsulated with that of an IPv4 header and sent from a reachable IPv4 source to an accessible IPv4 destination.

Presently the addressing is done in 32-bit address. With the implementation of IPv6 the addressing will be shifted to 128 bit addressing method.

Description Of IPv6 Packet Header

The IPv6 packet header consists of Version, Class, Flow label, Payload length, Hop limit, source address and destination address data and playfields.

Addressing Description

The IP v6 address is an eight part hex address separated by a colon ":" where each part n is an 16 bit number and is eight parts long. This gives a 128-bit address length.

n:n:n:n:n:n:n:n this is equal to 4digit hexadecimal integer.

Broadcasting Methods

The new methods in IPv6 are

- **Unicast:** In a unicast, packets are sent to a unicast address and are transported to the interface identified by that address. This is therefore a communication between single host and single receiver.
- **Multicast:** All the interface that have been identified by the address, receive the packet and is therefore a communication between a single host and multiple receiver.
- **Anycast:** A communication between a single sender and a list of addresses. In this, any packets sent to an anycast or list of addresses are transported to the nearest interface identified by that address.

Note: Decimal Number: The decimal numbers are base 10 numbers. The decimal system, is based on ten numbers: 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9. The next number in the sequence is a combination of two digits, where the second digit is multiplied by 10. 10 is equal to (1 X 10) + 0.

Hexadecimal Number: Similarly, hexadecimal numbers are base 16 numbers. Sixteen possible numbers may represent each digit or slot. Hexadecimal uses the first ten numbers of the decimal system: 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9. The number 10 has two digits so in hexadecimal it is represented by the letter A. The number 11, by B, 12 by C and so on.

Answer: [b] Multicast

Module:4

Reference No:M4161

Question: Which one of the statements is true with regard to a performance management?

- [a] Performance management includes only traffic analysis of the network.
- [b] Performance management involves setting of threshold limits for various database metrics.
- [c] Performance management involves configuring new components into the network.
- [d] All of the above

Module 4 – Network Performance Management

Definition

Network performance management is one of the five conceptual areas in the Open System Interconnection (OSI) model of the network management.

Network performance management refers to the effective and efficient utilisation of the network. One of the objectives of the network management is to measure and make all aspects of the network available to all users. The objective of the network performance is to ensure that performance of a network is at an acceptable level.

The procedure of performance involves the following aspects.

1. Quantifying
2. Measuring
3. Reporting
4. Controlling

of the utilisation and availability of all the components of the network. However the network has to be monitored as a whole and not as a summation of the performance of the individual components of the network.

The various factors involved in the performance management are

1. The quantum of data travelling across the various segments of the network.
2. The utilisation of various segments of the network
3. The responsiveness of physical topology to the traffic requirements.
4. Keeping track of utilisation of the bandwidth by users. This involves keeping track whether certain users are using more bandwidth than others.
5. The responsiveness of the system as a whole to the requests by each user
6. Keeping track of the users using large volume of resources and analysing the data that is being sent by such users.

Steps involved in implementation of network management

Performance management involves three main steps

- Capturing of data on variables of interest
- Analysing the data to determine baseline levels
- Determination of thresholds

Capturing of data on variables of interest .The activities involved in this stage are

1. Deciding the performance requirements.
2. Deciding the time intervals and the required data to be detained.
3. Capturing information for the decided database metrics and the measures. (Some of the metrics are network uptime, response time, application availabilities etc.)
4. Maintenance of the performance metrics.

Analysing the data: This includes network traffic analysis, trend analysis, protocol analysis, throughput analysis, and utilisation analysis.

Determinations of thresholds: Here the parameters of reporting are defined. The parameters include limits, granularity and the alarm rates. The objective of this activity is to set the limits beyond which the actions or activities are brought to notice and either analysed or rectified.

Performance management not only includes reactive measures but may also include proactive measures. This involves assessing the future needs for the network and the counteractive measures required to meet the future growth. Performance management also includes recommendations for future upgrades.

Since the current client server based networks are more dynamic in nature, analysing the path of a message becomes more difficult. Hence a huge volume of data regarding all components of the network needs to be taken.

Tools and techniques for performance management

Specific standards are available for monitoring the networks. Of the two, RMON (remote monitoring) and RMON2, the former deals with lower levels of OSI models. Here data can be collected from remote extensions and this includes traffic data of a segment, setting of thresholds and notification of changes in network behaviour. RMON2 deals with resources required to perform the application as a whole and not as individual devices. This is more useful for ensuring optimal use of the resources; redesign traffic flow and the like.

Separate standards are available for switched medias like ATM. These are AMON (ATM Monitoring).

One of the essential components of a performance management is SLA (Service Level Agreement). This is a contract, which defines the network services to be provided, and the acceptable level of performance.

Answer: [b] Performance management involves setting of threshold limits for various database metrics.

Module:4

Reference No:M4162

Question: Which of the following statements with regard to protocol is not true

- [a] Protocols are rules governing the exchange of data between two entities
- [b] Protocols can be utilised for troubleshooting the network problems.
- [c] Elements of protocol are syntax, semantics and timeliness
- [d] There may be different types of communications, but they all use same protocol

Module 3 – Protocol Analysers

Protocol analysers are devices, which provides information about conversations between two or more computer systems in a network. It also interprets (decodes) the data exchanged between 2 stations. Various protocol analysers are available in the market currently.

Protocols are basically rules governing the exchange of data between two entities. For information or data to be exchanged, there must be some convention, or in other words, they must speak the same language. These conventions are referred to as protocol. The elements of a protocol are

Syntax: This refers to data formats.

Semantics: This pertains to control information and error handling.

Timing: This refers to matching the speed of the data to be exchanged and sequencing of the data to be exchanged.

There are various types of protocols available for different types of communications. For instance TCP/IP is a protocol for Internet activities. This provides a rule or a protocol for communications in the Internet environment.

Protocol analysers are tools, which reveal exactly as to what is happening in the network or LAN. For instance if the TCP/IP sessions are hanging, it can point out clearly which system in the network has caused the problem and the last packet of information which failed to get transferred. If there is slow down in the network operations, the protocol analyser can indicate which system is responsible for this. It can show which system is waiting for information. In short protocol analysers can capture the data traffic. In other words, protocol analysers provide a device to monitor the health of a network and are best suited for troubleshooting the network problems.

There are basically 3 types of information about LAN traffic. They are

Statistics about data flow, station health and line errors: This information helps in identifying causes for a network problem or a load cause, resulting in slow down of the network. Additionally, if a new switch is to be added on to a network, the network statistics can show how best the new switch can be implemented into the system. If already the switches are installed, the protocol analyser can show whether the load is balanced evenly throughout the LAN.

Packet Capture and Decode: The LAN traffic is decoded into specific sub functions. This is useful for problem isolation in a LAN. Specific packet-by-packet conversion indicates the exact problem, cause and location. This indicates the exact events on the network in each workstation.

Trending Information: This helps in display of historical data in terms of days, months or even years. This information helps in indicating trend for any potential problem.

Some of the sample network troubleshooting applications that is helped by protocol analysers are as follows:

1. Hanging sessions: - The packet captures and decodes will show which system is hanging and failed to respond.
2. Problems in network printing

3. Failure to log in

Some of the applications of the protocol analysers are

1. Protocol statistics display which protocol is consuming more bandwidth
2. Station statistics indicate the traffic generated by each station. Therefore, it helps in answering the question that is using more bandwidth.
3. Frame errors will show which station is sending error packets so that it can be easily rectified.

Answer: [d] There may be different types of communications, but they all use same protocol

Module:4

Reference No:M4163

Question: Which of the following statements is true with regard to configuration management?

- [a] Configuration management involves tracking changes to the components of the system.
- [b] Configuration management includes only monitoring the hardware components of the network architecture.
- [c] Configuration management relates to only monitoring off end-items in a network system.
- [d] Configuration identification means identification of different components in a network.

Module 3 – Configuration management –overview

Concept

Configuration management implies monitoring the network and system configuration information so that changes in the hardware and software versions can be tracked. It also implies managing the effects of such versions on the network. Each network device contains a lot of version information associated with it. For instance a workstation could be configured in the following manner

Operating system version 3.2
TCP/IP software version 2
SNMP software version 4.0
X.25 software version 2.1
Netware software version 4.1

Objectives of a configuration management

1. Ensure disciplined systems development approach.
2. Monitor the changed status of the individual components by establishing a reporting mechanism for new components of configuration.
3. Provide a mechanism of control over the design, development, installation and support of individual components of network architecture.
4. Comply with international standards including the rules and regulations.

Components of a configuration management

There are 10 major components in any configuration management plan. They are

1. Documentation
2. Organisation

3. Configuration identification
4. Configuration Control
5. Configuration management status accounting
6. Suppliers controls
7. Program Phasing
8. Management
9. Configuration audits
10. Software Configuration

1. **Documentation:** This is a control mechanism for the records that are being generated and maintained for the project. A control record/database, which has reference to all other documentations/files, is created and maintained for a configuration management. The control document is used to monitor the documentation/information generated/stored as part of configuration management. This is akin to an index in any file.
2. **Organisation:** This component corresponds to the organisational responsibilities in a configuration management. This provides technical and administrative guidance to the project at different levels and activities.
3. **Configuration identification:** This serves the purpose of identification and maintenance of baselines for the components of a system. The baselines serve the purpose of providing the minimum requirements or a base for further system life cycle activity. The different types of baselines are design requirement baseline, component baseline, physical baseline build standard
4. **Configuration control:** This includes evaluation of all proposed changes to the individual components of the system. This involves co-ordinating change requests, proposals and their subsequent approval or disapproval. This includes reviewing and controlling changes according to set rules.
5. **Configuration management status accounting:** This implies recording the components of a configuration. This provides a document for containing information about fully approved drawings, changed proposals, and specifications of the components, the sub-components and the various associated components for all the sections of the system. This document states the status of each component, the baseline and the specifications.
6. **Suppliers Control:** This establishes the procedures for the control of the suppliers.
7. **Program Phasing:** This deals with various milestones and phases of the project. Procedures are established for monitoring the major milestones in a system project.
8. **Management:** This pertains to the overall management of the project configuration.
9. **Configuration audits:** This provides evidence whether the components of the system are as per the pre-determined standards.
10. **Software Specific configuration :** This deals with the configuration management of the software component of the system or network architecture.

Answer: [a] Configuration management involves tracking changes to the components of the system.

Module:4

Reference No:M4164

Question: Which of the following is most commonly used medium for Personal Area Network (PAN):

- [a] Lease lines.
- [b] Human body
- [c] Fiber optic cable
- [d] Radio waves

Module 3 – Personal Area Network (PAN)

Introduction

Thomas Zimmerman was the first to introduce the concept of Personal Area Network (PAN). PAN is a wireless communication device among others like laptops, PDAs, mobile phones, pagers and the like. PAN is also supported by Blue tooth technology. It eliminates the need for user specified commands, mouse, keyboard or voice for transferring data. PAN technology makes use of small stream of natural electric conductivity and human body as a medium (network) to transfer the data or information from one-person to another.

The human body too is a good conductor of electricity owing to the natural salinity (salt) level. PAN takes advantage of the same by generating external electric field that passes small amount of electric impulse through the body. This will carry the data from one place to another.

The intensity of electric current, which is used for this technology, is one-billionth part of an ampere i.e. one nano amp. This current is much lower than the natural current, existing in human body. This technology is also expected to gain popularity due to its tremendous speed of data transfer (400,000 bits per second), low power consumption and fewer expanses.

Working of PAN

It is based on seven-layer ISO [1] network model. In order to form a personal area network, PAN transmitters and PAN receivers are used to transfer data. The information is accurately transferred by microprocessor, which is usually the size of a deck of cards. A stream of electric current through human body then transmits the digitalised information. It is transmitted by physical contact of body like handshake (phenomenon is called linkup). In this process the electric circuit is completed and the data (phone numbers, e-mail Ids) from the sender is transferred to receiver laptops, mobiles or other wireless devices. After receiving the data, it can be used for various business or personal needs. In some cases individual's clothing also acts in the similar way. The low frequency (less than one megahertz) and control of electric signals do not allow data to move beyond the body. These characteristics plug the loopholes for security like eavesdropping (Intrusion of external party).

Applications of PAN

The major benefit of PAN is that it is wireless, which allows the user to use it anywhere and get the maximum advantage of e-commerce applications like vending, purchases, bidding and the like.

Although in current scenario, PAN technology is only a prototype, but their applications are unlimited. Some of the important implications are:

1. It transmits information between wireless devices carried by two individuals. For example electronic business cards swapped during handshake.
2. Assist individuals in exchanging personal information with wireless devices such as mobile phones, PDAs, pagers and the like.
3. It provides automation and security to the business transactions
4. Security policies of the corporate can automatically logon and logoff the user computer systems.
5. It even enables people to carry their medical information in digital form, which can be accessed in case of emergency.

[1] International Organisation for Standardisation.

Answer: [b] Human Body

Question: Which of the following is essential to understand the organisation's business risks relating to Router security?

- [a] Network Architecture
- [b] Network traffic management
- [c] Network security
- [d] Configuration process

Module 4 – Audit of Router Security

Router is an important networking device. It helps to route the data transmission and filters the packets according to different parameters like source address and destination. The following guidelines help the auditors to check the router security and its configuration.

Network architecture: The structure of the network and the role played by routers is to be clearly understood. The network-operating environment has to be clearly recognised in order to know the business risks related to the particular type of organisation. The following have to be observed to understand the network structure:

1. Network diagrams help to know the structural design of the routers and its nature and location.
2. The suitability of router in the existing environment.
3. Examine the role played by routers in network. Check whether they provide only connectivity or control also.
4. The role of routers in authentication and authorisation processes.
5. Change management, its approval procedure and monitoring process.

Network Traffic Management role: The basic duty of the routers is to manage the flow of traffic efficiently. There should be proper mechanisms to configure the routers, to ensure the correct direction of the traffic. To understand network traffic management, the following have to be considered:

1. The creation and maintenance procedures of routing tables.
2. Stability of the router tables. If liable to changes, an authorised person is to be designated to manage and control the changes.
3. Access tables have to be reviewed to know the access provided.
4. Network structure and routing tables are to be examined to verify the application of "least cost path routing" concept.

Network security: In case of routers being used for network security, examine its implementation and management to know the existence and effectiveness of the safeguards. Following have to be considered for this.

1. Control exercised over access passwords, changes to the network, authorisation and accountability for changes.
2. Access tables have to be examined to know the access path allowed and one used by network users.
3. Ensure that alternative access paths are prevented, if routers are used as significant security firewall.

Manageability: The configuration process of routers should be easy to manage. The tools available for easy management and its implementation have to be monitored. Thus,

1. Procedures for application to routers management have to be documented and reviewed.
2. Check with the network managers about the adequacy of tools available to manage the common risks.
3. Control over password by network manager to avoid unauthorised changes.

Recoverability: Important business processes are quite often supported by network. Its recoverability and components have to be considered while assessing the routers.

1. The capability of router configurations in reducing the disturbances in case of a failure.
2. Check with management, the existence of recovery plan and ensure proper updates. .
3. The tools used for router management are capable of reconfiguring the routers in case of failure.

Auditability: Required documents are available to review the Router Security and its configuration. Adequate records are maintained according to the needs of the organisation.

Answer: [a] Network Architecture

Module:4

Reference No:M4166

Question: Where organisation data is remotely accessed, the management should guard against information pilferage. For this purpose the management must ensure

- [a] Access through the remote device is based on password
- [b] Secure Socket Layer (SSL) is used for accessing the web site
- [c] Data that is being transmitted between the company and the end user is encrypted
- [d] All of the above

Module 4 – Mobile Device Wireless connectivity

Wireless connectivity provides an opportunity for remote users to stay in touch with the company despite the distance. This contributes to decentralisation thus helping the management in improving its productivity, customer satisfaction and reducing the operational costs.

Factors:

The factors that are to be considered by the management before it plans for a mobile wireless application are as under:

1. Application: The applications for which wireless connectivity is provided depends on
 - Flow of data in the application
 - Location of the data - whether it is stored in the system or on the server
 - Connectivity of the device with the application
2. Type of connection: Connection type will depend on the remote user's residence. The distance will determine the choice for PAN, LAN or WAN. If the user is within the radius of 100 feet, then PAN would be appropriate. For the distance up to a mile, LAN is suitable and beyond that a cellular network. The management should also contemplate on satellite connectivity if that is available.

3. Coverage: The coverage will depend on the location of the remote user. Connectivity can be within the company, region and country or at a global level. It should be ensured that the company has the appropriate link.
4. Throughput: The device/s to be used depends on the speed at which data should flow. There are several devices that are available with varying speeds. The speed of such devices is in kbps.
5. Security: When the access to the organisation data is from a remote place, data security is important. Following measures would help:
 - Access through the remote device based on a password
 - Secure Socket Layer (SSL) for accessing the web site
 - Encryption of the data that is transmitted between the company and the end user.
 - Installation of software to ensure that the company's information system is secure and that there are no threats of viruses.
6. Cost: The management before it decides on wireless application should decide upon the cost, since the benefits should outweigh the costs. Different providers charge differently. Packet based networks charge on the basis of data that is transmitted while some charge flat on monthly basis. If the connectivity needs are permanent and fixed, then WLAN technology can be used.
7. Power management: The power consumption of the device should be analysed and arrangement should be made for recharging the device.
8. Notification: The remote user needs to be notified on receipt of new information. The management should consider whether
 - The user can be notified when the device is off
 - Some other mechanism needs to be implemented say a pager or a cellular device
9. Services: The type of services that will be needed should be decided upon:
 - Web based application
 - E-mail
 - Thin client application access and the like

Answer: [d] All of the above

Module:4

Reference No:M4167

Question: Which of the following statement with regard to baseline management is true?

- [a] Baselines are not required for design specifications of a product.
- [b] Baselines refer to the performance standards for a component
- [c] Baselines once set cannot be modified in a configuration management
- [d] Baselines are set for all aspects of a product development/acquisition cycle.

Module 4 - Configuration Identification

Introduction

Configuration identification is a part of configuration management process. This refers to the activity of setting and managing baselines of a product development process. Once a product has been accepted by the

quality assurance team, the product drawings, code, tools, documentation, build and test scripts are base lined and stored.

Baselines are entities, which define the components of a system, subsystem or the system itself. Based on the phases in the system development activity different baselines are adopted. However the following types of baselines are considered necessary or constitute the basic data in a configuration management. They are

- Design requirements baseline
- Development component baseline
- Physical baseline build standard

Everything related to the product must be base lined. Even the configuration management data collected for the product development needs to be base lined. For instance, the change requests, service requests, issues, work orders all need to be base lined. This ensures that all development activities of a product are available for future reference on demand.

Baseline Management

The objectives of a baseline are as follows:

1. To provide a basis for the furtherance of a system development life cycle.
2. To provide a reference point and ensure trace ability in a configuration management
3. To control the configuration management.

Types of baselines

During the initial product development phase, when the product to be developed is identified and the designs fixed, the initial baselines are established. These baselines contain the system specification and the associated documents like drawings, tools for development and the like.

The components of the initial baselines are **functional baseline**, **physical baseline** and **product baseline**.

Physical baseline: The specifications of a product and the related drawing tree constitute the physical baseline of a product. This in turn serves as a starting point for the further phases in the project development that is during production and service operations of the system. This baseline will constitute the basis for any further change in the production process of a product.

Functional baseline: The detail system design/analysis including the prime item development, interface control document and equipment specifications constitute the functional baseline of the system. These need to be authenticated before being established as functional baselines.

Once the initial design and the specifications of the system are ready, then individual components are selected for development.

Product baseline: The form, fit, functional requirements, the acceptance test procedures are contained in a product baseline. It also contains the software product baseline, which prescribes the source code listings and design documentation of a product.

The design of the project and the related project document constitute the design requirement baseline.

The subsystem specifications, interface control drawings, software/interface requirements, assemblies,

installation drawings constitute the development component baseline.

Answer: [d] Baselines are set for all aspects of a product development/acquisition cycle.

Module:4

Reference No:M4168

Question: Which one of the following is true with regard to configuration status accounting?

- [a] Status accounting only involves a static representation of the components of the system configuration.
- [b] Status accounting includes a record of evolving changes to the components/product.
- [c] Status accounting does not involve maintaining the record of changes to drawings and specification to a product.
- [d] None of the above.

Module 4 – Configuration Management Status Accounting

Concept

Configuration management status accounting is an important element in the design of a configuration management plan. All development processes generate a huge amount of information. This information needs to be collected and accounted and utilised in the right manner. This process of recording and maintaining the configuration index of the project is termed as configuration management status accounting.

The configuration index/matrix

This forms the basic document for recording the individual products in a configuration. This document contains the complete drawings and the specification of the system.

It would not be practically viable to record each and every piece of the product. Any attempt to do this would shift the focus from developing a product to the recording process. A good configuration management design should devise strategies to develop a recording methodology, which seamlessly integrates into the development process or the configuration management process. Thus it should compliment the development process and not burden the development team with irrelevant responsibilities.

Components of status accounting

There are three standards that are maintained as part of the configuration management status accounting. They are:

1. Design standard
2. Actual build standard
3. Design build standard

Design Standard: The design standard defines what the component is, what is to be developed and contains a list of approved drawings, specification and the like. Each subsequent change to the baseline standards with their drawings is also incorporated following the approval procedures.

Actual Build Standard: This contains the actual hardware and software standards for the components. The bases for the hardware and software standards are the drawings and specifications in the design standard

above.

Design build standard: This is a document, which is a combination of the design standard and actual build standard. It is an evolving document, which records the designs and the development of the components.

The terminology adopted may vary from organisation to organisation. However the above standards are essential components or details that are required to be maintained on par with configuration status accounting.

Accounting Process

The initial drawings and the specifications of the project is the starting point for the configuration index/matrix. Then the fully approved changes to the drawings are accounted in the matrix. The flow of recording process is as follows:

1. The foremost task is to identify the issues. The issues could be from various sources, for instance from end users, development team, company employees, or even business partners. These issues could vary from inherent flaws in the technical design to the new features the user may require.
2. In the next step, the proposed changes are processed and approved. This process consists of preparation of change requests, change proposals, approval documentation and the like. These activities are duly recorded in the system to indicate the exact status of the project.
3. Once the changes are approved, the baseline documents are changed.
4. The changed baseline documents and the revised drawings and specification of the product are accounted for in the configuration matrix or the index.

Data Management

Certain administrative issues and protocols need to be followed while accounting changes or updating the configuration index. The objective behind the protocols is to maintain the integrity of the documents for the particular project or network system. And the records show the accurate status of the project.

Answer: [b] Status accounting includes a record of evolving changes to the components/product.

Module:4

Reference No:M4169

Question: In which of the following transmissions, is the communication channel disturbed by atmospheric conditions?

- [a] Twisted pair circuits.
- [b] Coaxial cable.
- [c] Optical fibre system.
- [d] Microwave transmission

Module 4 – Communication channels Part 1

In a network, data needs to be transmitted between different locations. There are a number of communication channels available for transmission of data. This article provides an overview of communication channels using

1. Telephone lines
2. Twisted pair (copper) circuits
3. Coaxial cable
4. Optical fibre system
5. Microwave transmission

Telephone lines: The telephone lines can be used to transmit data with the help of modems. The telephone line can either be leased or switched.

1. Leased line: Using a leased line, communication is possible only between two computers. The line is always open for communication between the two ends. But the line cannot be used for communication with any other computer. For example point of sale terminal. Such terminals require an open line for communication with the main computer.
2. Switched line: It is similar to a telephone operation. When the user wants to transmit data, it dials the telephone number of the receiving end. After transmission of data, the line is disconnected. Using this line it is possible to transmit data to any computer.

Twisted pair (copper) circuits: The circuit has two intertwining wires of which one wire carries electricity to the telephone or modem. The other wire carries electricity away from the telephone or modem. They are generally used for dedicated data networks, as they are inexpensive. Although the use of two wires reduces the chances of cross talk, they are easy to tap. With a speed of up to 4 Mbps, they are used for short distance.

Coaxial cable: Coaxial cables also use two wires but they have a higher capacity than twisted pairs. Coaxial cable consists of a protective jacket, conducting mesh, insulator and conducting core. It is widely available, used for high frequency, is immune to noise and has high usable bandwidth. Its speed is up to 10 Mbps. When compared to twisted pair, the coaxial cables are more difficult to tap and are expensive.

Optical fibre system: Optical fibre system consists of a transmitter and glass fibres. The glass fibers are about a diameter of a human hair. Data travels through this fibre in binary signals at a speed of light. A large amount of data can be transferred, when compared to coaxial cable of the same capacity, as they are lighter, thinner and stronger. They do not radiate energy or conduct electricity. They are free of cross connections and lightening induced interference.

Microwave transmission: Microwave transmission is transmission of data by line of sight carrier system. The transmission of data is similar to the transmission of radio and television signals. Instead of using cables they use antennas. The antennas are placed on top of buildings, or mountains or any such peak. The limited transmission range of the channel necessitates microwave signals for long distance through a chain of towers. The waves are affected by atmospheric conditions and solid objects as they travel by line of sight.

Answer: [d] Microwave transmission.

Module:4

Reference No:M4171

Question: The _____ component of LAN is used for communication between different networks.

- [a] Gateway
- [b] Network Interface Unit
- [c] Hub
- [d] File server

Module 4 – Components of LAN – Part 2

This is concluding part of the series on components of LAN. In the earlier article we discussed about workstation and file server. In this article we discuss about

- Gateways
- Network Interface Unit
- Hub

Gateway: Gateway is a node in the network point that is used for communication between different networks. It transfers bits between the different LANs. Both the networks need not have the same hardware features. It is possible to have a mainframe at one end and personal computers at the other end. When the hardware features are different at both the ends, a workstation may be designed to act as a gateway by attaching the network adapter cards of both the LANs. A server can also act as a gateway by installing the network adaptor cards to it.

Network Interface Unit: Network Interface Unit or the Network Interface Card (NIC) or Network Card of Network Adaptor is a combination of hardware and software. It is a computer circuit board. The computer can connect to the network only after the card is installed.

The card facilitates controlled communication across the network. The NIC need not be installed on all the computers. Some computers with inbuilt communication and networking need not have a card installed. They are equipped to perform all the network interface functions.

NIC is a collection of chips each designated for a particular function. The chips that form NIC are network bus drivers, communication controlled chips, RAM buffers and ROM. All the workstations on the network have the same type of cards. The server may have an additional ROM code for performing additional features.

The functions of NIC are

- To provide transmission and data control
- Format the data into manageable units
- Translate the data rate and protocols from the network communication medium to the workstation
- Provide address recognition capabilities

The user cannot visualise the NIC's operation. They would have no knowledge of transmission of data from one point to another. They simply specify the destination and the data is transmitted.

There are two types of NIC – the communication interface and host interface.

Communication interface: Communication interface performs all network oriented and transmission related functions. The function of communication interface can be broken into steps as under:

- To accept data from the workstation
- Buffer the data till a communication channel is free
- Transmit the data,
and vice versa when the data is received for a particular workstation.

Host interface: It performs computer specific functions. It is used for providing the connection between the communication interface and workstation's internal circuitry.

Hub: Hub is the place where data from different sources arrives for transmission to different destinations. It contains multiple ports. When data is received in one port it is copied on to the other ports, so that all the users on the network can have access to data.

Active hub: Active hub as the name suggests uses active devices for distribution of data. It can be connected to passive hub, file servers and additional active hub.

Passive hub: It is passive distribution of data. It covers very short distance. It cannot be connected to any active devices. .

Answer: [a] Gateway

Module:4

Reference No:M4172

Question: Which of the following is true in relation to the client/ server environment?

- [a] Client/ server is independent of hardware and software
- [b] There is one-to-one relationship between the client and the server
- [c] Data integrity is not maintained
- [d] Once the client/ server environment is set up it is not possible to alter them

Module 4 – Client/ server

Mainframe architecture that was being extensively used is now replaced with client/ server architecture.

What is client/ server?

Client/ server consists of a client and the server.

Client: Client is a PC or workstation in which applications run. The client has to rely on the server for resources and operations. The resources may be any data in the files or devices. An example of client is an e-mail client. E-mail client is an application that enables the user to send and receive e-mails.

Server: A server is a computer on the network, which manages the network resources. The resources may be files, devices and the like. They can be specially designed for a particular purpose such as file server for managing files or print servers for printer.

Though the client/ server concept usually applies to a network, it can also be used in relation to a single computer. In such a situation, client would mean an application making a request to another program and the server would mean the application that attends to the request. In some cases a client may request a server for some information that in turn will act as a client and another will act as server for the same information. Let us suppose you want to check your bank account from your computer. How does this happen in a client/ server environment?

1. An application of your computer i.e. the client will make a request to the server program in the bank.
2. The program on the server forwards your request to the client program in the bank, which in turn will send it to the database server.
3. The data base server retrieves the information and sends it to the client at the bank.
And vice versa till it reaches you.

Characteristics: The client server has the following characteristics:

1. Service: The server provides the services to the clients.
2. Shared resources: Server allows the sharing of the resources among several clients.
3. Asymmetrical protocols: Client/ server is based on many to one relationship. There may be many clients requesting the server for service. It is always the client, which requests for the service.
4. Transparency of locations: Server can reside on the same machine as the client or on a different machine.
5. Mix and match: There is no rigid specification for a client/ server. It can be created using any combination of hardware and software.
6. Message-based exchange: The client and server interact through message passing mechanism.
7. Encapsulation of services: Servers can be upgraded without affecting the client provided the message mechanism is not changed.
8. Scalability: Scalability can be horizontal or vertical. Horizontal is adding or removing a workstation, which has the affect of only a slight impact on their performance. Vertical is making changes in the performance of the server to a large extent.

9. Integrity: The data integrity is maintained as the data is maintained at a centralised place.

Answer: [a] Client/ server is independent of hardware and software

Module:4

Reference No:M4173

Question: The user account is created by the

[a] User

[b] Network administrator

[c] Security administrator

[d] Project in charge

Module 4 – User accounts

When you login to the network or on your personal system you cannot login unless you have your user account or you have a guest login. The user account grants you some privileges that allow access to the otherwise inaccessible areas.

User accounts:

User accounts contain the actions a user can perform. User accounts can be

1. On a computer that is a member of a network domain
2. On a computer that is a member of a workgroup or stand-alone computer

User account on a computer that is a member of a network domain:

Let us take an example. In a company there are many employees who would require the use of systems and access to information. All the users cannot just login. The network team who is in charge of the network would give access to the user by creating his user account. Then the user would be allowed to create files, folders, execute programs, change the password and the like.

Network administrator can only add users. When the user is added he can belong to only one group. It could be a department to which the user belongs or a temporary group for persons on temporary assignments. The user will have all the access rights given to the group. The rights can also be curtailed. But they cannot be extended to something which the group does not have access to. The administrator assigns a default password to the user which can be changed by him. The user should follow the password policy (which is discussed in a separate article) while changing his password.

User account on a computer that is a member of a workgroup or stand-alone computer:

The user accounts that are available in this type of set up are of three types

1. Administration
2. Limited accounts
3. Guest accounts

Computer administrator account: The computer administrator is a person who is entitled to add or remove programs, add or delete users, change other users account and permissions to make all the changes that are required. But he cannot change his own permissions, as there should be at least one computer administrator.

Limited account: Limited account user has restricted rights. Unlike computer administrator he cannot add or remove programs. He can only access them. His rights are limited to his own account i.e. he can change, create or delete his password. But he cannot delete his own account, as that is the task of the computer administrator.

Guest account: Guest account is used when the user has no user account. The guest user can have access to the programs that are already installed. He cannot make any changes.

Answer: [b] Network administrator

Module:4

Reference No:M4174

Question: The products of Internet Application Security (IAS) tools for e-Business applications are very popular due to which of the following aspect?

- [a] Standardisation
- [b] Automation
- [c] Optimisation
- [d] Customisation

Module 4 – Internet Application Security

Increasing use of applications in an e-Business needs a change in security requirements. As far now the security tools used for e-Business are:

- Intrusion detection system and firewalls
- Encryption standards
- Authentication techniques like Secure Socket Layer (SSL) and Public Key Interface (PKI)

But in an e-business environment, the integrity of interaction between the end user and the application should be ensured. Also the e-business environment and scope are expanding, which pose new security problems. Hence the security tools should be designed to cope with the current challenges of e-business security. In order to ensure this interaction, as intended by application developer is a great problem. This is due to following reasons:

1. Defects or errors in the design phase, implementation phase or in the testing phase of the codes developed for interaction.
2. Vendor products like web and application servers may not have fool-proof security
3. Drawbacks in the codes procured from external developers

A hacker gains access to the web application by making use of web browser and changing the Internet environment. A few technical loopholes that a hacker takes advantage of:

- **Parameter Tampering:** The accuracy of Common Gateway Interface (CGI), which is rooted in a hyperlink, is must. On failure of the same the system becomes vulnerable to hacker's attack.
- **Cookie Poisoning:** Cookies are used by web applications to save the data like user id and time stamp on client's machine. Since cookies lack security aspect, it is easy for hacker to modify the cookies by changing cookie file.
- **Stealth commanding:** Insecure commands like eval and system, when executed on web server, allows the hacker to attach Trojan horses in back of form submission. It will execute a malicious code on web server.
- **Configuration subversion:** Misconfiguration of application or web server is a common mistake, which authorises a person for directory browsing. Hackers can use this feature for browsing application's directories.

Measures to overcome security vulnerabilities

Manual application security is a practical solution to address all these problems. Some of these are:

- Secure code design: In order to design a secure application a specific proficiency is required. It also increases complexity, which leads to extended development time.
- Secure code implementation: The complexity of design makes the implementation difficult. In order to implement a secure application, one requires a defensive coding, which ensures that any implementation error will not result in any security threat.
- Testing for loopholes: Functionality tests are done to test the final application. Other than that, stress tests are also done. For example keeping the application in a hostile environment and exposing it to various attacks helps in detecting loopholes in the application.

Internet Application Security (IAS)

Companies involved in e-Business should explore usage of Internet applications security products to automate some of the security features. These tools should have application level security at the run time and implement it at every request. It should also be easily customisable for every application.

Advantages of Internet Application Security Tools

1. Current and forthcoming applications are secured instantly, even if the security aspect was not taken into consideration at the time of design and implementation phase.
2. Website administrator need not worry about constant patching and system configuration. Application servers and web servers are patched only when additional functionality is to be included.
3. Simpler applications can be created without worrying about security aspect.

Answer: [b] Automation

Module:4

Reference No:M4175

Question: In Wireless Application Protocol (WAP) technology, the data is transferred from source to destination via:

- [a] WAP gateways
- [b] WAP routers
- [c] Internet
- [d] Wireless devices

Module 4 – Wireless Application

Wireless technology plays a very important role in e-business strategies. Access to the Internet through wireless technology has increased the traffic on websites.

Wireless Application Protocol (WAP)

WAP is not a single protocol but it is a set of multiple protocols, which supports data formatting and transmission via wireless devices. It acts as a standard technology for distributed computing, cross platforms and the like. It enables user to communicate with Internet and telephone service on wireless devices like mobile phones, PDAs, Smart phones and the like. The use of different devices led to increased complexities in monitoring the website. Hence the need for various techniques like load testing and functional testing. Performance monitoring is done to fix performance bottlenecks, if any before the site is launched.

- **Load testing:** It is a type of stress testing, which is done by exposing the website to various user loads. It helps in identifying any loopholes and fixing them. In WAP-enabled service, the testing team should load test the Web servers and WAP gateways, since these are the most essential parts of WAP technology.
- **Functional testing:** It tests the content and business processes of the website so that the end-user can use the web application according to expectations. It ensures the correctness of web application on different wireless devices.
- **Performance monitoring:** Determining the performance of a website and analysing the problems before the user applies them real time. It keeps track of all the transactions in the web application and measures end-user response time.

Working of WAP

WAP technology is almost similar to Internet but the difference lies in low bandwidth, low potential to display the content, and low memory. The WAP client request is also same as Uniform Resource Locator (URL) concept on the web and is transmitted via WAP gateway. WAP gateway acts as a mediator between computing network (mostly TCP\IP) and "bearers" (responsible for carrying the data between the networks). It does the following :

- Processes request received from the client.
- Calls java servlets or CGI script
- Formats the data to be sent back to client for display or further processing.

This formatting of data is done by Wireless Markup Language (WML), which is based on Extensible Markup Language (XML). WML converts data into binary 0's and 1's due to low bandwidth, known as deck. The deck is so designed that it can display the information on the small display areas of wireless devices. It can manipulate the information via embedded WML script. Pros and cons of WAP

Pros

WAP helps in business applications by better communication with the vendors. WAP has the ability to build a single application, which is used by clients and is the only technology that supports mobile communication. Another advantage of WAP is that despite small display area, a well-formatted information does not give any problems while reading.

Cons

- It lacks graphical user interface (GUI).
- Normal HTTP content if sent directly to wireless devices will give a problem. HTTP content is formatted with graphics, which are not directly supported by WAP technology.

Answer: [a] WAP gateways

Module:4

Reference No:M4176

Question: To prevent database overload and server crash, which of the following events require monitoring?

- [a] Physical disk % disk time
- [b] Logical disk % disk time
- [c] Logical disk % free space
- [d] All of the above

Module 4 – Performance Monitoring Tools part 2

This is the second of a two part series on performance monitoring tools. The first part briefly discusses the entire process of performance monitoring. In this article we describe the hardware monitors of a computer system.

It is important that sufficient controls are in place to ensure that there are adequate inbuilt security mechanisms to safeguard the systems against any eventuality. And the objective here is to ensure not only the existence of security mechanism but also continuous functioning in an effective manner.

Several utility programmes are available, which assist the auditors in performance monitoring of the system. These may be very technical so the assistance of performance experts may be necessary to understand and analyze the data and information that is generated by these software.

The Process

Three main components are involved in any performance monitoring utility programmes. These soft wares are programmed to **log** any pre-decided **events**. These logged events can be viewed with the help of charts and graphs to analyze the data. And **alerts** can be set up when the logged events cross the **threshold** of pre-determined limit. This has been explained below with an example.

Assuming the objective of a company is to ensure that its database does crash due to overload, it will choose a method for monitoring the hard disk. It will select Logical disk % free space as an event to monitor the hard disk space. And also it can choose to monitor the memory available bytes counter to ensure that sufficient space is available in the computer.

And for an efficient management, the performance monitor will be set to a threshold of 10% free disk space. Each time the hard disk space goes below the level of 10 % the system will issue an alert.

Similarly these utility programmes are set up to provide information on various parameters of a computer system. Given below is a sample list

Objects	Processes/events	Explanation
Processor	% Idle time	This indicates the % of time the processor is idle during a given period of time
	% Interrupt time	This indicates the time the processor spends receiving and sending hardware interrupt
Logical Disk	Average number of disk read/transfer/write time	This indicates the average number of bytes that are transferred to or from the disk during read or write operation.
RAS port	Total number of serial overrun errors	This indicates the total number of serial overrun errors
	Frames per second	This indicates the number of frames transferred per second

There are 4 different ways of analyzing or viewing the data collected

Logs, Charts, Alerts, Reports

Answer: [c] Logical disk % free space

Module:4

Reference No:M4177

Question: One of the objectives for monitoring business uptime is

- [a] To improve the performance of the website
- [b] To increase redundant systems
- [c] To prevent the loss of revenue
- [d] None of the above

Module 4 - Business Uptime-Definition

The capability to carry out business even in the face of a partial or complete system failure and unexpected high demand is known as business uptime. The objectives of maintaining business uptime is to

1. Prevent loss of revenue.
2. Maintain brand reputation.

Causes of Downtime

There could be many reasons for downtime. They could include

Hardware failures- includes server hardware and network hardware

1. Operating system failures
2. Network failures- includes network software and traffic
3. Applications failure-platform software

Another major concern for failure is operation errors. These include human errors.

Maintaining Uptime-issues to be considered

Various issues need to be considered for maintaining uptime. These include

1. Identification of critical business functions.
2. For the critical business function identified, minimal services that need to be maintained even in case of downtime also need to be identified as well.
3. Which business function can be performed manually in the event of downtime?
4. The peak usage time of the website
5. The time taken to recover from system failure, switch to a backup or a contingency plan.

Another important factor that needs to be taken into consideration is that the downtime should not be apparent to the customer.

Techniques and tips for maintaining uptime

Building redundancies for the system is one way through which the site can achieve high uptime

What are redundant systems?

Redundant systems are extra systems that are maintained to be utilised only during the down time of website. In this method, data is simultaneously captured on multiple servers, and on Internet Service Providers. And also good contingency plan to recover from the down time is put in place. Some large companies have multiple ISPs, undertake data mirroring and clustering in order to achieve high uptime.

Redundant systems can be implemented by following a three-step process. It involves prioritising the critical functions of a website, modularising them, and segregating the critical functions.

Prioritising

This involves prioritising all the business services of a website. This activity can be divided into 2 parts

First-identification of all the business segments of the website

Second-categorising the business segments into critical and non-critical

Critical segments are those, which are essential and form the core of the operations like user logon, product catalogue, shopping cart etc.

Non-critical ones are those services that add functionalities and enhance the customer experience but are not essential to the operations of the business, for instance these include the ads, banners, online billing etc.

So, during peak times these non-critical services can be turned off to accommodate a large traffic.

Modularising

Once the task of prioritising is over, then both the critical and non-critical services can be moduled into different segments. This is done in order that during peak time non-essential modules can be completely switched off. For instance, the human resource functions can be grouped into a single module and be turned off during peak time if they are not critical to the operation of the website.

Segregating

After modularising, the critical modules can be implemented so that non-essential modules can be automatically turned off during peak loads. For instance, the administrator can suspend the implementation of the promotional functions during peak time.

Manual Fall back Processes

Also, to maintain a high business uptime, it is advisable to maintain a few manual alternatives so that customer servicing is not interrupted. For instance, the following manual alternatives can be implemented

1. Receiving orders by mail
2. Enabling payment through checks etc.

Answer: [c] To prevent the loss of revenue

Module:4

Reference No:M4178

Question: Which one of the statements is true with regard to problem management?

- [a] Troubleshooting is absolutely necessary for any problem
- [b] Problem management involves rectifying a system outage
- [c] A root cause analyses of all problems need to be done irrespective of business requirements.
- [d] All of the above

Module 4 - Problem management-procedures

Problem management-definition

The problem management function constitutes three important tasks

1. Putting back the systems that wear down to full functionality within minimum time frame
2. Analysis of the causes for the system disruptions
3. Communicating the cause of error to the team so to avoid the recurrence of the error.

Problems management -procedures

The problem management procedures involves 5 steps

1. Back up
2. Troubleshooting
3. Analysis of the problem
4. Resolution of the problem
5. Data collection

Backup

Data backups are an absolute necessity for any problem management procedures. In the event of any system outage the data loss can be reduced to a minimum. The level of the loss directly depends on the frequency of the backup.

Troubleshooting

The first question that needs to be decided is whether to trouble shoot a problem. This depends on the nature of the problem, the organisational issues, the criticality of the issue and other things. A trade off needs to be done between spending extensive time & resources for the troubleshooting of the problem and the business requirements. The recommended solution would be to collect the data of the problem and provide some intermediary solutions for restoring the systems to working.

Two issues needs to be tackled in the troubleshooting process

1. The problem management procedures should provide for training of the troubleshooting process.
2. A time frame needs to be set for the troubleshooting process. This is to ensure that long delays are not observed in restoring some mission critical systems, for instance the mail server etc.

Problem analysis

Before the problem is solved, an attempt needs to be done to analyse it. Problems usually fit into any one of the following categories-

Connectivity problems
Performance problems
Security problems
Data loss

Problem resolution

Once the problem has been analysed, the next step is to resolve it. Some of the common fixes for problems listed in the categories above could include-

Connectivity problems -Re-establishing channels, rebooting, resolving duplicate IP addresses etc.

Performance problems -Performance monitoring tools can be used to identify the location of the problem. These can locate system bottlenecks, suspending services that are causing the bottlenecks or stopping a non-essential service. Or ultimately re-boot the system.

Security Problems-re-set passwords and permissions

Data losses - restore data from the backup, correct hardware failures restore and re-build the system.

Persistent problems

If the problem cannot be solved after preliminary analysis, then a decision needs to be taken by the administrator whether to continue to analyse the problem, rebuild the operating system and restore the data from back up or not.

The situation could be difficult, but since the primary objective of problem management is to restore the system the second option is generally followed. However adequate documentation of the problem needs to be done before the system is restored.

Data collection

To identify chronic problems and prevent further recurrence of the problem it is always recommended to collect data about the problem that has occurred. The higher the quantum of data collected the better it is. The data could include

Problematic data
Performance monitor logs
Event Logs
Network monitor logs

Answer: [b] Problem management involves rectifying a system outage

Module:4

Reference No:M4179

Question: Event logging in the context of performance monitoring is

[a] One of the many tools available for performance monitoring

- [b] Refers to the recording of pre-decided activities of a system at pre-set intervals
- [c] Refers to the activity of monitoring the performance of a server
- [d] All of the above

Module 4 – Performance monitoring tools-Introduction

Performance monitoring tools help in analysing the efficiency of the operations of the system and detecting any suspicious behaviour. There are two ways of monitoring the system. Directly by monitoring specific events, or indirectly, by observing the status of server.

Every organisation needs to frame a security policy to determine the parameters of the monitoring activity. Within that security policy, certain monitoring targets need to be clearly indicated. The list of specific objectives that need to be defined before deciding on a monitoring tool are mentioned below:

Server performance- should the performance of the server be base lined? If so what are the various parameters that are going to be selected for performance, at what intervals will the data for the each parameter is collected/how often are baselines going to be set.

Objects-what are the objects that need to be monitored. They could be files, registries, kernels etc. There are a number of accesses that can be monitored for each class of an object. For instance for directories we can monitor the write, delete, modify and change access. In case of services, the start and stop accesses can be monitored.

Events-What are the events that need to be monitored? User right assigned, user right removed, audit policies changed, the operating system opening and shutting down etc are some of the common events that can be monitored.

Event log management – some of the common issues that need to be considered are -how is the event management going to be managed, whether customised logs are to be developed in-house or should a third party vendor package be used. What technologies are going to be utilised for performance monitoring? These pertinent issues need to be resolved.

And finally, the question of how much of the system's activities is going to be monitored? Because indiscreet monitoring may divert system resources that can otherwise be used in critical operations of the system.

Components of a performance monitor

The following constitute performance management architecture and is based on the windows performing architecture. Other platforms could use different terminology or may use a different approach to performance monitoring, but generally, the performance architecture could be in the following lines.

Event Logging- this indicates the recording of events in a system. One of the important aspects of event log management is to manage the size and overwrite policies of the log.

Actual Performance monitoring-here the various counters are determined for performance analysis. The four critical counters that are normally used in the system are

- CPU utilisation
- Memory Availability
- Disk system performance

Network bandwidth

Answer: [b] Refers to the recording of pre-decided activities of a system at pre-set intervals

Module:4

Reference No:M4181

Question: Which of the following is "TRUE' with regard to cryptography?

- [a] Cryptography modules should be tested before distribution
- [b] Users are not responsible for securing the keys
- [c] Cryptography should be limited to few applications
- [d] Lifetime of the keys should be limited to one year

Module 4 – Implementation issues for cryptography

Cryptography is used to secure data while it is transmitted. But if the cryptographic system is not implemented and managed properly it will create a security threat.

The security features are dealt under the following heads:

- General recommendations
- Key management - general
- Key distribution
- Key storage and destruction
- Key management facility/ certification authority
- Signature generation and verification

General recommendations

- Testing cryptographic modules before distribution
Cryptography modules help in providing cryptography services like signature generation and verification, encryption and the like. A cryptography system consists of several modules. If there is an error in the design of modules then the functioning of the entire system will be affected. The modules should be tested before implementation. The test should provide for comparing the results generated by implementation against the known result. This would help in detecting the flaws in the design. Also the tests should cover if the design conforms to all applicable standards viz. Data Encryption Standard (DES), Digital Signature Standard (DSS), Secure Hash Standard (SHS)
- Using cryptography services to a wide extent
Wherever sensitive information is transmitted, traditional security operations should be replaced with the cryptography system. This would reduce chances of forgery, reduce administrative time, reduce paper work and the like.
- Documentation and training to all users
All the users should be trained. The training should educate them of their responsibilities for the security of the system. The entire procedure of the system should be documented.

General key management

- Physical protection
The keys and their components stored in floppy disks, smart cards and the like (token) should be in a

secure place to prevent unauthorised users from accessing them. In addition to this, token should be kept in an envelope so that the owner can determine if any body has tried to tamper with it.

- Educating the users
Users should be aware of their responsibility for securing the keys. All users should be given a list of their responsibilities and liabilities. Users should give a declaration that they have read and will abide by their responsibilities.
- Timeout features
The cryptographic module should have a timeout feature where the system automatically gets logged off if it is left unattended for some time by the user. This helps in minimising unauthorised access to the system.

Key distribution

When a key is stored on the token, only its owner should be able to access it with the PIN (Personal Identification Number) that he possesses. This means that if a person has no PIN he cannot have access to the key. For this the security officer who generated the token and PIN should send the token and PINs in separate mails with a confirmation from the recipient.

Key storage and destruction

- Determination of the life of the keys
The lifetime of the keys should be determined before they are issued to different users. The lifetime should be determined by taking into account the roles and responsibilities of the user.
- To verify signatures and decryption the keys should be archived for a long time.
- The deactivated and revoked keys should be handled properly so that the data signed prior to the deactivation or revocation date can be verified.

Answer: [a] Cryptography modules should be tested before distribution

Module:4

Reference No:M4182

Question: _____ can be used for protection of central keys in a cryptography system.

- [a] Split knowledge
- [b] Delphi technique
- [c] Tabbing
- [d] Code comparison

Module 4 - Implementation issues for cryptography - Part 2

This is second and concluding part of the series on implementing issues of cryptography. In the earlier article we discussed the general recommendations, key management - general, key distribution and key storage and destruction.

In this article we deal with

- Key management facility/ certification authority
- Signature generation and verification

Key management facility/ certification authority

- Control over central or root keys
Sensitive applications require the use of the central or root keys. For example signing a central key database for its integrity and the like. If the keys are not secured then the entire application would be unsecure. These keys can be protected by either implementing split knowledge or dual control.

Split knowledge: Under this system, the key components are split and given to two or more persons. A part of the key with any person does not convey any idea about the original key. The key is formed only when all the parts are within the system.

Dual control: To protect sensitive information and functions, the key is under the control of two or more persons. The key can be used only when all the persons are present.

- Log: An automatic log should be maintained on the usage of the central keys.
- Encryption of sensitive data: All the individual records in the data that relates to the key should be encrypted. This would help in detecting if the data has been tampered.
- Compromise: A contingency plan should be prepared for dealing with compromise to the central key. It should state the actions to be taken in relation to encrypted data, system hardware and software, central keys, user keys and the like.
- Verification: Integrity of the code at the central key management site should be verified at regular intervals. Similarly generating the checksum should check the cryptographic module.
- Different keys for maximising scalability: Different central keys should be used for new systems and the backups of the central site.
- Migration: When the system is being migrated from prototype to live, the central keys should be changed. If this is not possible then the entire system of generation, distribution and storage of the central keys should be reviewed.
- Flexibility: The system should be flexible enough to allow for multiple central sites.

Signature generation and verification, encryption and decryption

- Encryption of data fields
Encryption should be limited to the sensitive fields. This would have an affect on the performance of the system.
- Protection of data prior to encryption
The data should be protected before the cryptography function is performed. Because if the data resides in the central database and has to be moved to the system for encryption, there is a possibility of the data being altered.
- Viewing the data
Users before signing and encrypting the data must view the contents properly.
- Re-signing of data
Resigning of data may be required when there is a change in organisational code and the like. The user before resigning must be able to view the contents and see the changes that have been made. A log should be maintained of all the data that has been resigned. The log should at least include the person who resigned along with the date of resignation.

Answer: [a] Split knowledge

Module:4

Reference No:M4183

Question: Which of the following functions does the client in a client/ server application provide?

[a] Providing connectivity

- [b] Remote Procedure Call
- [c] Job scheduling
- [d] Quality assurance

Module 4 -Functions of Client in a Client/ Server applications

Client/ server is the system architecture in which the system's functionality processing is divided between the client and the server. The client is a workstation at the front end and server is at back end where major processing functions are carried out.

The components of a client/ server are

1. Client
2. Server
3. Connectivity

Client in a client server application is a workstation. It provides the users with appropriate services such as computing, connectivity, database services and the relevant interfaces.

The functions of the client can be described under the various heads:

1. Role of client
2. Client services
3. Request for services
4. Dynamic Data Exchange (DDE)
5. Object Linking and Embedding (OLE)
6. CORBA (Common Object Request Broker Architecture)

Role of client:

The client requests the server for the services that are needed by the users. The services include

1. Presentation services using graphical user interface
2. Simultaneous executions of different functions using the windowing environment
3. Acting as a client and server when information and other logic of a request reside in the client itself

The client may use the same or different operating system from the server for providing basic services and network operating system interface.

Client services:

An ideal client/ server is one that is based on request-server discipline. When the client/ server is so designed the servers may change their operating system and hardware operations without altering the client application.

The client in a traditional client/ server environment operates only by sending and receiving input and output to the server. All the application logic is done at the server. The functionality of the client can be extended, by adding some of the processing functions at the client. For example, editing and help capabilities to name a few.

Request for service:

The client makes request for services to the server. Network Operating System (NOS) redirects the client service to the server operating system which may even be across LAN or WAN. For example say the local drives are A: and C: and the remote drives D:, E: and F:.

When there is any request for A: or C: the NOS redirects it the local file system. Request for other drives is passed on to the server operating system. The NOS at the client transfers the request using the Remote Procedure Call (RPC) and Application Program Interface (API) to the NOS server. NOS server executed the request and passes it to the application.

1. Remote Procedure Call (RPC): RPC provides for use of subroutines by different users. Subroutines are programs that are frequently used by different users or may be within the same application many times. Instead of writing the program each time it is required they be stored at a location and called for whenever they are required using RPC. RPC provides for a standard procedure in which the user must make the call. The call can be made and executed from processors running different operating system and using different hardware platforms.

Answer: [b] Remote Procedure Call

Module:4

Reference No:M4184

Question: In a client/ server environment _____ provides for sharing or communicating information between programs.

- [a] Dynamic data exchange
- [b] Object linking and embedding
- [c] Common object request broker architecture
- [d] None of the above

Module 4 - Functions of Client in a Client/ Server applications - Part 2

Client in a client server application is a single user workstation. It provides appropriate services such as computing, connectivity, database services and the relevant interfaces to the user.

The functions of the client can be described under the various heads:

1. Role of client
2. Client services
3. Request for services
4. Dynamic Data Exchange (DDE)
5. Object Linking and Embedding (OLE)
6. CORBA (Common Object Request Broker Architecture)

In part one we dealt with role of the client services, few of the request for service. In this article we deal with remaining functions under request for service, DDE, OLE, CORBA.

Request for service:

1. Fax/ print services: The client can execute a print request using the NOS even when the printer is busy. NOS redirect it to the print server queue manager. The client can view the status of his print request. Similarly the fax request is made and executed.
2. Window services: The programmers can write the application programs without any sensitivity to the windows. The application uses Graphical User Interface (GUI) to place the data on the virtual screen. Windowing service provides proper manipulation and placement of the application window. This facilitates the development of programs.
Besides that, windowing services provide the user with the facility to activate, view, move, resize or hide a particular window.
3. Remote boot services: The client may operate some applications without any local disk storage. For this purpose the workstation must have sufficient software burned into Erasable Programmable Read Only Memory (E-PROM). This starts the initial program load and holds the basic input/ output operation.
4. Other remote services: The NOS software provides for the remote execution of the application on the servers. With the appropriate architecture they can also provide mobile computing service facility.

5. **Utility services and other services:** The utility services that can be executed at the workstation are copy, move, edit, compare and help. They can be executed at the client workstation. The other services would include message services, network services, application services and database services.
1. **Message services:** Messages can be sent and received synchronously to/ from the network.
 2. **Network services:** The client along with the network and Application Program Interface (API) helps to create, send, receive and format network messages.
 3. **Application services:** Specialised services through API, embedded in a RPC can also be executed.
 4. **Database services:** Usually database requests are made using the SQL syntax. They can be run on different platforms. Other languages can be used but they may not provide the flexibility provided by SQL.

Dynamic Data Exchange: It provides for sharing or communicating of information between programs. In the client/ server model the application requesting the data is considered the client and application providing the data as the server. Either application can terminate the link.

Object Linking and Embedding (OLE): OLE is a standard that enables the linking of objects created in one application with the second application. These embedded objects when referred to by other applications retain their original format and links to the application that created them.

Common Object Request Broker Authentication (CORBA): CORBA architecture enables piece of program call object to communicate with one another. It is independent of the programming language and the operating system. .

Answer: [a] Dynamic Data Exchange

Module:4

Reference No:M4185

Question: Which of the following is used to receive and transmit the data in a satellite transmission?

- [a] Transponders
- [b] Beams of light
- [c] Mobile citizen band radio
- [d] Fixed citizen band radio

Module 4 - Communication channels - Part 2

This is the second and concluding part of the series on communication channels. In the earlier article we discussed about telephone lines, twisted (pair) cables, coaxial cables, optical fibre transmission, microwave transmission.

Infrared transmission: In infrared transmission, beams of light transmit data. It is optical in nature. The transmission is narrowband and through line of sight and hence an inexpensive way of transmission. But the range is limited. It is reasonably secure, unaffected by weather and artificial light.

Laser transmission: Here too, the transmission is through light and line of sight. Sensitive receiving equipment is used. It can be used for both narrowband and broadband. The distance of transmission can be increased through use of repeater or relay stations. It provides a secure means of data transmission.

Radio transmission: In radio transmission, mobile citizen band radio with a keypad and an unattended fixed (stationary) citizen band radio are used. Using these, it is possible for the user to dial through the telephone connected to the stationary radio. Once the person gets connected to the other end, a circuit is formed. Now

the persons can converse with each other as though they are on a telephone. The range of such equipment is about three miles. It is a transmission media devoid of any security features. They are more popular in United States where cabs, courier, and repair service providers usually use them.

Satellite transmission: The transmission between different earth stations is through a communication satellite. The earth station consists of a satellite dish, similar to an antenna and other communication equipment to transmit and receive data. The communication satellite use transponders for reception and transmission purposes. If an earth station wants to transmit data to another station it transmits the data to the satellite. The satellite accepts the data, amplifies it and then retransmits it to another earth station. They are used for both voice and data transmission.

Satellite transmission is through line of sight. It is affected by weather conditions. There are chances of voice echoing when there is a delay in transmission of the signal due to the extreme transmission length between the sender and receiver. The security is nil and it is provided through use of coding and decoding equipment.

Table showing the comparison between different communication channels

Medium	Range	Cost	Security	Advantages	Disadvantages
Copper circuit	Short distance	Low	Low	Easily installable Easy to modify Supports voice and data	Cross talk Noise Interference Easy to tap
Coaxial cable	Can be extended through use of repeaters	Varies with distance	Moderate	Easily installable	Expensive Not easy to modify
Fibre optic	Long distance	Expensive	High	Secure Non-interference No cross talk	Difficult to tap Expensive
Microwave	Long distance	Low to moderate	Moderate	Simple to install	Easy to tap Noise Interference
Infrared	Short distance	Inexpensive	Moderate	Simple to install	Sensitive to weather Line-to-sight
Laser	Depends on use of repeaters	Low to moderate	High	High security	Line-to-sight
Radio	Short distance	Low	Low	Cost is less	Easy to tap Noise Interference
Satellite	Long distance	Expensive	High with encoder	High bandwidth	Line-to-sight Weather sensitive Echo

Answer: [a] Transponders

Module:4

Reference No:M4186

Question: ----- is a component of a good problem management system?

- [a] Time bound schedules for problem resolution
- [b] Good co-ordination between the various roles involved in the function
- [c] Analysis of the trends of the problems diagnosed
- [d] All of the above

Module 4 – Problem management–best practices

Why do we need problem management?

Problem management helps in preventing discontinuity in the IT services of the business. An efficient problem resolution capability aids in building customer confidence in the business and helps to prevent or minimise any losses that is incurred or will be incurred due to system outages. Hence, with the increasing dependence of the business on the IT services for its operations, an efficient problem management procedure is pre-requisite for any large or medium sized IT department of organisations.

Problem management Service function

The problem management service of an IT organisation involves the following components

Identification of a problem -The problem could be originated either by a user, an application or an IT infrastructure component. Based on the contents of the call, it is classified into a problem, inquiry or a request. If it is a problem then the problem resolution process will be activated. Any problem resolution procedure should ideally go through the following steps

1. Identification of the type of the problem
2. Assessment of the business impact
3. Collection of information regarding the problem
4. Activating the resolution process.

Problem Management Organisational Issues

For successful problem management, various roles and responsibilities need to be assumed in the organisation. The various roles required are as follows

Management -the management has to actively involve itself in establishment, maintenance and continuous review of the problem management functions.

Problem resolver-one person in the organisation should be made responsible to bear the responsibility for resolving the problem. The person with this responsibility will need to have the required expertise and knowledge to solve the problems identified.

Problem Ownership- The responsibility related to this role is to ensure that the problem gets fixed within the set time frame and severity level.

Co-ordination-A high-level co-ordination is required between the various roles in the problem management service. The responsibility of this role is the collection of information to make it available to other roles in the problem management function.

Problem management function process

A good problem management system should provide for the following functions

- Problem recording
- Diagnosis of the problem
- Resolution

- Elimination of the problem
- Tracking of the status of the problem

Each problem should be assigned a severity level. This severity level will depend on the impact of the problem, criticality of the problem etc. Based on this severity level the time schedule of the problem resolution is set.

Documentation

Records of the problems diagnosed should be archived for a reasonable period to be used for analysis of future problems.

The information that would normally be recorded in any problem management systems is

- Problem code
- Severity level assigned
- Problem description
- Systems application involved
- Problem owner
- Resolution description
- Problem history
- Audit trail of the changes made as the problem resolution progresses

Problem management-proactive measures

A problem management should not only involve reactive measures but also involve some pro-active measures. Some of the pro-active measures include

- 1.Early warning from system alerts.
- 2.Periodic analysis of problems
- 3.User feedback information
- 4.Root causes analyses of a problem

Continuous monitoring of the problem statistics can be used for improving the efficiency of the problem resolution service.

Conclusions

Various tools can be developed to automate the problem management process. Problem analysis facilities can be inbuilt into applications. IT components could have inbuilt alert mechanisms with problem solving facilities etc

Answer: [d] All of the above

Module:4

Reference No:M4187

Question: Which of the following should form a part of the approach to framing the intranet security policy?

- [a] Identifying the resources to be protected
- [b] Designing the techniques for implementing the security
- [c] Performing penetration testing
- [d] Communication of the policy to all the employees

Module 4 – Intranet Security

Intranet is a technology that allows the company to create an internal community to facilitate communication within the organisation so that timely and cost effective information is made available for effective functioning of the company. It is based on

- Internet technology
- Web services
- TCP/IP and HTTP
- HTML publishing

Like any other environment, security is important in intranet environment also. Information should have integrity, reliability, availability and security. It should be ensured that the information is protected no matter where it is stored, where and through which communication channel it is transmitted. For this purpose the company must strengthen its network policy.

The first step in achieving this is to develop the network policy. The steps in designing the network policy are

- Network security planning: The extent of network security depends on the value of information posted in the network. If the intranet is used for posting some routine procedures and forms, which are not critical to the organisation, a very high level of security may not be needed. Hence it depends on whether the resources and information on the network is worth protecting. Network related problems should be identified before defining the policy. The policy should also define the services that users can access. . The policy should be acceptable to all the network users and administrators.
- Site security policy: A company can have multiple sites with each site having their own network. The network policy should encompass all the sites. The site security policy should be framed taking into consideration all the resources at the site. This includes, servers, workstations, connecting devices such as gateways, routers, bridges and repeaters, cables connecting the servers and workstations on software and application running on network, databases, information contained in files and folders.
- Approach to security policy: The cost of protecting the network against the threats should be less than cost of recovery if the company is affected by a security threat. The approach to security policy should identify
 - o Resources that should be protected
 - o Significance of the resources
 - o People from whom the resources should be protected
 - o Likelihood of the threats
 - o Measures to be taken to counteract the threat
 - o Keeping the policy current
- Risk analysis: Risk assessment is done to identify the risks that the resources of the company are exposed to. This helps in identifying the steps to be taken to protect them.

Techniques: The techniques of implementing intranet security are encryption and authentication. Authentication includes

- User to host authentication
- Host to host authentication

- User to user authentication
The techniques have been explained in detail in other articles.

Developing intranet security: Intranet security can be developed by deploying appropriate firewalls and configuring them accordingly. Different types of firewalls have been already explained in detail in other articles.

Implementing intranet security: The intranet security when implemented should encompass the following

- Physical and procedural control
- Network security
- Platform security through monitoring tools and the like
- Application security through implementing authentication mechanism and the like

The intranet security can be implemented through developing a policy (covered earlier in the article). The next step would be to configure systems in accordance with the security policy. The policy and the security procedures should be communicated to the users. The security environment should be regularly analysed for security breaches. When a breach arises the network team should take appropriate action.

Post implementation

- Post implementation, it is necessary to always ensure that the policy is current and update in accordance with the changes in the business activities.
- Even after security is implemented, there is a need for frequent assessment and analysis of risks and threats.
- Penetration testing should be taken to identify the unknown vulnerability points.
- External auditors should be appointed as their wide range of experience can help in identifying the vulnerabilities that the company may not be aware of. Internal auditing is valuable to the company but external auditing is a must.

Answer: [a] Identifying the resources to be protected

Module:4

Reference No:M4188

Question: In an Internet environment, ----- represents the activity of sending commands to other computers and receiving the output.

- [a] File Transfer Protocol
- [b] Gopher
- [c] Telnet
- [d] World wide Web

Module 4 – Intranet Concepts and Terms Background

The term Intranet generally refers to the application of various Internet technologies (especially the World Wide Web) to private corporate networks. The size of a corporate network can vary largely. Some of them are large with thousands of users. But even the largest of such network will conform only to a small-scale version of the technologies that are used for Internet.

The objective of this article is to introduce the readers to the basic terms and concepts that are used in the discussion of Internet and the web deployment issued for an Intranet. To start our discussion the article begins with a definition of what is Internet/internet.

Internet/internet

The internet (small i) is a network composed of small networks. An Internet (Capital I) is a larger version of the internet with millions of users and small networks connected to each other worldwide. From a small beginning wherein the network was used only by academicians and researchers, today virtually everybody in the world is using Internet. A variety of services are available today on the Internet ranging from E-mail, to the file transferring utilities and of course, the technology called the World Wide Web.

Internet/Intranet services

Some of the services that have been developed over the years for Internet/intranet users are given below

1. **File Transfer Protocol (FTP):** Transfers the files between computers
2. **Telnet:** This represents the activity of sending commands to other computers and receiving the output
3. **Gopher:** Files can be found by topic through this search engine. This is normally used with Telnet
4. **Wide Area Information Servers (WAIS):** A search engine through which files containing a particular text string could be found.
5. **News:** This lets users post, read and respond to messages posted by others.
6. **Mail:** A rule for programming electronic mail messages, and its transmission over the network
7. **World Wide Web:** A way to circulate pages of information which could be text, graphics, multimedia like sound and video clips and links to other pages.

Identifying Information: URLs

Uniform Resource Locator (URLs): This is a convention for describing file location and types. Meant for description of files on the server, it is platform independent. For each of the above-mentioned services, a variation of URL is followed. For instance

1. **ftp://server1/share1/dir1/file1.txt-:** This describes a text file called file 1 located on FTP server named server 1 in the directory /share/dir1
2. **file://server2/share2/dir2/file2.txt:** A text file called file 2 is located on server named server 2 in the directory /share/dir2
3. **http://website1/dir1/page1.htm:** A HTML file located on HTTP (web) server named website1, in the directory /dir1

Information Accessing: Browsers

Browser is the generic name for software whose main application is locating information or files. For instance, windows explorer is a file system browser. Either the browser itself will display the file or start another application, which will display the contents of the file.

For example, let's assume there is URL indicating a word document in a file server. When we select the URL, browser starts WORD to open and display that file. If the URL indicates a HTML file, then it would start a web browser.

Answer: [c] Telnet

Module:4

Reference No:M4189

Question: ----- is the communication channel between web server and web client

- [a] HTML
- [b] HTTP
- [c] TCP/IP
- [d] FTP

Module 4 - Intranet Concepts and Terms -part 2

Background

This is the second and concluding article of a two part series on Intranet Concepts and Terms. In the previous article, we had discussed some basic services provided by the Internet. In this article, we intend to describe in detail how the Internet services can be deployed on a corporate LAN.

Most of the services described in the previous article like file transferring, file locating are today available on PC networks. For example the windows explorer, windows file manager are similar to the FTP (file transfer protocol). The client/server software today has removed the need for Telnet. MS exchange provides services like corporate mail and news software.

The only exception is that the PCS do not have a native tool that is similar to the technology of World Wide Web. The World Wide Web technology has to be specifically deployed in the corporate network to build a intranet.

Intranet Web Creation

The topic, deploying World Wide Web software on a corporate LAN encompasses five major areas.

TCP/IP protocol

The first step in deploying an Intranet is configuring TCP/IP on the network computers. Through this protocol each device (node) on the network is assigned a TCP/IP configuration setting in the dotted-octet format including an IP address, a subnet mask that the node uses to identify nodes on other subnets, and default gateway to which the node sends frames. Instead of IP addresses the computers in a network can also be identified using either host names or NetBIOS names. In these cases, the host names and NetBIOS names are resolved to IP address using a separate service.

Web Server Software

The second step is the installation of web server software. Typically, HTTP (Hyper Text Transfer Protocol) is the communication medium between web server and client. HTTP is a convention for sending messages over the TCP/IP network protocol.

Web Client Software

The third step in the web deployment is the installation of web client software. The most important web client software is the browser. The browser is the communication medium between the web server and the web client. The HTTP is used to communicate to the server. Some of the popular browsers are Microsoft Internet Explorer, Netscape navigator and so on. They can read and display all documents written in the HTML.

Create the content

The next step is the creation of content. There are three ways to create content

1. Create a HTML page. This can be done using text editor, HTML programming guide or a HTML page-authoring tool.
2. Use tools to convert a existing document into a HTML document
3. Create a page with a link to a non-HTML document

Maintain Content

One of the major tasks in maintaining content is keeping track of links. This is especially important when adding new pages or deleting pages. Care should be taken to maintain the links contained in the deleted documents.

Answer: [b] HTTP

Module:4

Reference No:M4190

Question: Which of the following operations/ documents are not components of the control of operations management?

- [a] Processing standards
- [b] Processing manuals
- [c] Recruitment process
- [d] Service level agreements

Module 2 - Control objectives for implementation block

Operations management

Introduction

The IT function is a combination of various activities. All the activities should be performed for the completion of the entire IT function. Some of these activities are primary/ major while others are support activities. It is not possible to perform the primary/major tasks without the support activities.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To provide the support activities on continuous basis.	To ensure availability and integrity of IS operations through the support functions and their efficient and effective performance.	1. Processing standards 2. Processing manuals 3. Job scheduling 4. Log of processes 5. Interaction with change management and	• Data • Technology • Support • Human factor

		business continuity management personnel 6. Service level agreements 7. Automation of operations	

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **Operational procedures:** The management should define standard procedures for IT activities. The management should ensure that the IT staff understand the standard procedures and adhere to them. The standard procedures should be periodically tested and updated or changed when required.
- **Operations manual:** The standard procedures should be documented.
- **Job scheduling:** IT activities should be scheduled for proper utilisation of the assets and to meet the defined objectives as per the service level agreements. Any change or deviation from the schedule must be authorised by the appropriate personnel. There must be a procedure for identifying and investigating such deviations.
- **Continuity of operations:** Continuity of operations should be ensured when IT activities are carried out in shifts. A procedure should be defined for tendering the activity report to the next shift in charge.
- **Log maintenance:** The logs should be maintained for all activities in a sequence. This enables the review and restoration of activities when the systems fail.
- **Security over forms and other devices:** Appropriate physical controls should be defined for protecting the negotiable instruments such as cheques and other output devices that are used by the organisation. There should also be an effective control over their use.
- **Remote network:** Where organisation's network can be remotely accessed, IT managers should ensure that the access procedure is defined and implemented.

II. Operational Controls

The operational personnel should ensure that the above procedures are implemented. The concerned IT manager should approve of deviations, if any.

Answer: [c] Recruitment process

Module:4

Reference No:M4191

Question: Under which case/s do Intranet serve/s as effective networking tool/s?

- [a] In a distributed decision-making environment
- [b] Where heterogeneous applications are involved
- [c] In a centralised organisation
- [d] In a decentralised organisation

Module 4 – Checklist for Intranet features

Effective networking is necessary for information sharing and processing in a distributed decision-making environment. An intranet effectively coordinates the corporate activities. It can be defined as a company wide network that uses Internet technologies and several hardware and software platforms.

Employees possessing detailed knowledge about the company and organisational structure use the intranet. Therefore, they easily understand the terminology used. An intranet may simply contain company policies and employee details or it may include all other details about the company. Hence is it essential to evaluate its efficiency in facilitating users.

Features of an effective intranet system:

- 1. Shared access:** This is a common but important feature of the Intranet. Employees should not face any compatibility problems to access the information saved. Hence, the standard file format must be used to save documents. If any outside Web sites are linked to the intranet, they must be readily accessible. This saves time and resources.
- 2. Control over access:** Past and present employees may become potential trespassers of the corporate information contained in the intranet. Hence, proper security policies must be undertaken to protect human resource records, corporate communication and other important information. Password system and chronological levels of access to intranet serve as effective safeguarding measures.
- 3. Flexible organisation:** Control over content classification is essential for effective organisation of an intranet. For instance, if an intranet permits creation of several departments and sub-departments, security parameters can be established correctly.
- 4. Scheduling system:** All employees will have the same and correct information about meetings and events if a centralised scheduling system is maintained in the intranet. Further, employees can enjoy flexibility in setting their own meetings when the access to the scheduled system is controlled.
- 5. Message boards:** They help employees share their ideas, express views and overcome their frustrations. An intranet message board may help resolve matters under discussion between departments and peer groups, not otherwise possible in face-to-face discussions.
- 6. Address book:** Client, vendor and employee related information when stored in the company's intranet is easy to update. It also acts as an effective communication tool as the search criteria helps to send mass e-mails if batch e-mail functionality is implemented.
- 7. Search Engine:** An intranet search engine is essential to find the things quickly. It scans the intranet when a keyword is given in the text field and displays the results. Therefore, search engines must be easy to locate, access and use.
- 8. Task management:** An effective intranet eases task management. Managers can direct employees to do a particular task by merely assigning and prioritising the tasks.

9. Customised interface: A customised interface adds another minor feature, which displays the company's logo, name etc. It serves as an effective branding tool.

10. Individualisation: Employees of different categories who are responsible for various activities need a comfortable and convenient intranet. Hence, it should cater to individual user needs.

Answer: [a] In a distributed decision-making environment

Module:4

Reference No:M4193

Question: Which of the following is "FALSE" with regard to control objective of incident management?

[a] The incident resolving relates to following the prescribed procedure for standard operations.

[b] The incident should be communicated to appropriate personnel

[c] An audit trail should be maintained to record all changes made during the incident management.

[d] Incident management provides the procedure for identifying and resolving the incidents

Module 2 - Control objectives for implementation block

Problem management

Introduction

Problems and incident if not curtailed and managed properly would lead to compromising on security. The management should develop appropriate incident procedure to define, identify, resolve, escalate and report such incidents and ensuring that such incidents do not recur.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To define a procedure for identifying and resolving all the incidents.	To ensure availability of information by implementing incident management procedure and to ensure system effectiveness and efficiency.	1. Incident identification 2. Incident resolution 3. Reporting 4. Escalation 5. Vendor responsibility 6. Change management procedure 7. Emergency procedure	• Data • Technology • Support • Human factor

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls.

Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **Incident identification and reporting:** Incidents relate to any event that is not a part of the standard operating procedure. They may also include any problems or errors. The management should define a procedure for their identification, analysis and resolution. A periodical report should be generated for all the incidents and separate reports for all significant incidents.
- **Escalation:** An escalation procedure should be defined for escalating the incidents to higher authorities for a timely action to be taken. It should provide for setting up of priorities and documentation of the action taken. The escalation procedure should activate the business continuity plan where the circumstances so demand.
- **Audit trails:** The audit trails should be maintained to keep a track of all the changes made during the incident management. It should be possible to track the changes both forward and backward.
- **Emergency procedures:** In case of emergencies, the temporary authorisation granted should be properly documented and maintained in a standard form. The emergencies should be prioritised, approved by the IT managers and communicated to the security personnel. The authorisation must be revoked after completion of the emergency procedure.

II. Operational Controls

Incident management: The operations team should ensure that the procedures defined by the management are implemented. In certain cases it may have to violate the prescribed procedure. It should be ensured that all such violation are properly documented and approved by the IT managers.

Answer: [a] The incident resolving relates to following the prescribed procedure for standard operations.

Module:4

Reference No:M4194

Question: The control objective of the quality management is to ensure

- [a] Documentation of the test results as per the defined quality procedure
- [b] Customer satisfaction
- [c] Reporting of the quality assurance to the management
- [d] All of the above

Module 2 – Control objectives for planning block

Quality management 2

Introduction

The quality management of the IT function of the organisation should be clearly defined. It should be

consistent with the overall quality levels of the entire organisation functions. The quality levels for each stage of the system development life cycle process should be defined in clear and unambiguous terms.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To ensure that the IT functions are carried out by adhering to IT quality standards of the organisation and that the quality standards are continuously maintained.	To ensure effective and efficient IS system and to maintain the integrity and that reliability of the system is maintained through quality management.	1. Define quality levels 2. System Development Life Cycle (SDLC) 3. Quality plans 4. Responsibilities 5. Practices 6. Testing 7. Controls 8. Review 9. Report 10. Training 11. Industry standards	• Data • Technology • Support • Human factor

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **Acquisition of technology:** The management for all technologies acquired by the company should define a procurement and maintenance procedure. The procedure may include guidelines regarding
 - o Acquisition
 - o Testing
 - o Documentation
 - o Vendor selection
 - o Maintenance and the like
- **Relationship with the vendor:** To ensure that the management maintains cordial relations with the vendors and other parties, the agreement should be defined in clear and precise terms. The agreement should clearly state the management and the vendor's responsibility for acceptance of the technology, utilities, change process, standards and procedures to be followed.
- **Testing:** Proper testing should be done for both programs and systems. The SDLC process should define the procedure and the environment in which tests can be conducted, verification of the test result, documentation of the test. The test should be conducted at the time of development/

acquisition of the technology or when the technology is changed or modified. The process should also define the different tests that should be conducted before the technology is accepted e.g. pilot test

- **Documentation:** SDLC process should define the documentation standards for documenting the program and system development and modification process. The process should also provide for ensuring that the standards are being complied with.
- **Review:** The quality plan should provide for review of the entire SDLC process to assess the compliance of the process by the development team and to ensure that the objectives are achieved.
- **Quality measurement:** The management should define quality measurement unit and the process for measuring the performance.
- **Reports:** A report on the performance should be submitted to the user department and the IT management.

II. Operational Controls

Not applicable for this activity

Answer: [d] All of the above

Module:4

Reference No:M4196

Question: Which of the following data is processed and analysed to develop reports?

- [a] User ID
- [b] URL
- [c] Time Stamp
- [d] All the above

Module 2 - Control of Web-access resources

Access to Internet would help employees to work efficiently. At the same time, it can also lead to negative consequences when the employees misuse the facility to indulge in entertainment or malicious content. This has a bearing on the productivity and efficiency of employees and hence the organisation. Therefore configuration and control of Web-access resources is an essential duty of managers, human resource administrators and IT professionals.

Three steps are involved in Web-access control:

1. Defining policies and standards for effective usage of Web-access resources.
2. Establishing a reporting tool to monitor the Web usage.
3. Undertaking follow-up action

I. Policies and standards:

In order to have a proper control over Web-access resources, the policies and standards must be effective and consistent with the corporate culture. The prohibited as well as permissible web activities must be clearly stated. The established standards must be well documented and circulated across the organisation. They must be simple, measurable and easy to understand.

II. Reporting tool

A well-framed Web access reporting system helps the companies to effectively utilise the resources and avoid legal liabilities. The following are the essential requirements of any Web access reporting system:

1. Reporting tools must be consistent with the policies framed.
2. It should provide accurate information about web access.
3. Metrics explained in the reporting tools must be comparable to the standards developed in the policies.

Inbound activity and outbound activity are the two types of web activity reporting software. Inbound activity reporting software provides the details of users viz., suppliers, customers and any other third parties visiting a website (say the company's website). This kind of reporting helps companies to track the visitors and their frequency. On the other hand, outbound activity reporting software provides information on employees within the organisation accessing different web sites. Several users and several sites are involved in this activity. Therefore, outbound activity reporting software products need to be more sophisticated. These systems are not as easy as inbound activity software, to implement.

Outbound web-access reporting is required for control over Web resources. It records all the details pertaining to the visitors, which also includes the bandwidth consumed in the process and also identifies whether the visits are in compliance with the usage policy. Pre-existing log files, which contain electronic time-tagged logs to keep the complete record of visits, are used as primary source of raw data. The following data is analysed and processed to develop reports:

1. *User ID*: It is easy to understand
2. *URL: The name and type of the sites visited*: An appropriate categorisation of sites is required for an URL to be effective and identify the visited sites. Actual visits must be marked as acceptable or unacceptable according to the organisation's policy.
3. *Time-Stamp- that measures date, time and number of the hits*: Managers can ensure the optimal utilisation of productive sites by understanding the employees' level of activity. They can also identify the problematic areas.

III. Follow-up action:

Management evaluates the work force's activity through reporting system and takes necessary action to correct the situation if employees are involved in any malicious activity. It can modify the procedures or may take employee related actions like training, reassignment or termination of employment.

Answer: [d] All the above

Module:4

Reference No:M4197

Question: The overall objective of defining the technological infrastructure is to

- [a] To deploy the current technologies that are available
- [b] Deploying technologies that meet the business objectives
- [c] To set the technological standards
- [d] To define the migration procedure to be adopted when installing the new technology

Module 4 – Control objectives for planning block

Define the technological infrastructure

Introduction

The objectives of any IT organisation can be achieved through proper implementation of the technology. IT infrastructure plan should be framed which specifically states the purpose and expectation of acquiring and implementing such technology in clear specific terms.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To meet the business objectives by utilising the existing and available technology.	To ensure effectiveness and efficiency of the technologies that are available or to be acquired to meet the business needs.	1. Current technologies available 2. Available resources 3. Acquisition plans 4. Migration process 5. Third party relationships 6. Cost 7. Performance of resources	• Technology • Support

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **Planning:** Based on the long term and short terms plans of the IT functions a technology plan should be developed. The plan should include the following
 1. **Present architecture of the system** – The technology plan should consider the architecture of the present system before acquiring and implementing the new technology.
 2. **Criteria for selection of technologies** – The technologies that the organisation plans to deploy should be consistent with the overall objectives and should easily integrate with the existing systems.
 3. **Migration procedures** – The new technology when implemented should not affect the performance and functioning of the existing systems. The migration procedure must be defined which needs to be followed when installing the new technology.

- **Setting of standards:** The standards need to be set, based on the IT plans. The actual implementation and performance of the technology infrastructure should be measured against the set standards.
- **Acquisition plans:** The technology plan can be broken into hardware plan and software plan. The management whenever it proposes to acquire new hardware and software should ensure that the acquisition is based on the defined plans. The plans should include a guideline on
 1. Requirements of the end user
 2. Functionality
 3. Security features
 4. Vendor selection
 5. Installation process
 6. Documentation
 7. Training and the like
- **Technological obsolescence:** The plans should be evaluated on continuous basis to ensure that they are current and take into consideration the technological advancement, scalability, obsolescence and related matters.

Analyse future trends: The plans should have an inbuilt mechanism for taking into account the technological updates and the regulatory requirements so that the same can be taken into consideration when developing and making alterations to the plans.

Answer: [b] Deploying technologies that meet the business objectives

Module:4

Reference No:M4198

Question: Which of the following servers provide the business functionality required by a company?

- [a] File server
- [b] Application server
- [c] Database server
- [d] Communication server

Module 4 - Types of server in a client/ server application

Client/ server is an architecture in which the functionality and the processing is divided between the client (front end) and the server (back end).

A server consists of single or multiple processors with shared memory providing computing, connectivity, database service and relevant interfaces that address the business needs. The server has no special hardware requirements. The hardware of the server is based on the applications. Depending on the operating system that is used, it provides various different services. Often pre-emptive multitasking enables a high priority task to be executed, before a low priority task is processed. It ensures that no single application can take control of the resources of the server.

The different types of servers are:

- ☐ Application
- ☐ File
- ☐ Database
- ☐ Print/fax
- ☐ Image

- Communications
- Security

Application server: This type of server supports the operations of the client workstation by providing business functionality. The services can be extended to all or a few business functions. There can be multiple application servers to service the business needs. For example, for calculating the payroll, employee information can be handled by one server, gross pay calculated by another server, deductions by the third server and so on. The servers can run on different operating systems and different hardware platforms.

File server: The server manages free space in the storage area. It ensures fair allocation of memory, and supports the sharing of files across the network. It is a repository for documents, images, engineering drawing and any other data objects created by the user for sharing. It also provides access control and other security features that depend on the network operating system.

Database server: The client passes a request to the database server. The server then processes the request, instead of passing all the records to the client. It provides for efficient use of distributed processing power. It also provides decision support systems for ad hoc queries and flexible reports.

Print/ Fax servers: The server receives the document for printing from the client, queue, prioritises and executes it when the printer is free. It also provides for error recovery for jams and notifies operators of errors.

The fax server also provides similar functions. In addition, it also ensures that the fax is distributed when the communication charges are lower. Adding the fax card to the server also provides the compression and decompression facility.

Communication server: It takes care of communication over the wide area network, and supports different protocols. **Security server:** Security is provided at the server by restricting access to software and data. Usually, the user login is the primary threat to security. Even the LAN server can be used to implement the integrated Response Access/ Control Facility (RACF) security.

Answer: [b] Application server

Module:4

Reference No:M4199

Question: The computer requires an external serial connector to communicate with the outside world. Which of the following components is not used for such communication?

- [a] Serial port
- [b] RS 232C connector
- [c] Asynchronous communication port/adaptor
- [d] None of the above

Module 4 – Communication Hardware

Communication hardware is required for data transfer between computers. In this article, we discuss the communication hardware requirement for microcomputers. Usually, microcomputers use telephone lines (adapters and modems) for communication.

Communication adapter

Data flows between computers in the form of bits. The transmission of bits is possible in two ways – serial

and parallel. In serial data transmission, the flow of data is in a series. In parallel transmission, the eight bits that form the character travel simultaneously in a separate wire. This method cannot be used, when communication is over telephone lines.

The computer requires an external serial connector to communicate with the outside world. The following components are used:

- Serial port
- RS 232C connector
- Asynchronous communication port/adaptor

Serial port is the connector through which data enters and departs.

RS 232C is a standard that specifies how the pins in the connector are wired and which pin performs which function.

Asynchronous port supports the transfer of data in bytes.

The communication adapter is a circuit board, which can be built into the computer, or it may be an optional circuit board. It has 25 pins. Each pin carries signals defined in an internationally accepted standard. Its functions are as follows:

- It handles the transfer of data between the computer and telephone line
- It reads and writes data to and from the buffer that exists in RAM
- It signals the CPU when the buffer needs to be refilled or emptied
- It formats the data, adds start and stop bits and parity bits when transmitting the data
- It removes the start and stop bits and parity bits when receiving the data
- It controls the communication rate

Acoustic couplers and Modems

The information is stored in the computer in the digital form, while information is transmitted through the telephone in analog form. The modem is used to convert digital signals into analog signals and vice versa. It is connected to the communication adapter at one end, and to the telephone line at the other end. (Modem types and functions s has been covered in another article).

The functions of the acoustic coupler are similar to that of a modem. It can be used to link the telephone to computer terminals and fax machines. It has two openings to accommodate the earpiece and microphone of the telephone handset. The speed of the coupler is 300 or 1200 baud.

The advantages of using acoustic couplers are: they are cheap and permit the use to standard telephones for transmission. But the major drawback is that they are very slow, and there are chances of loud background noises causing disturbances.

.Answer: [d] None of the above

Module:4

Reference No:M4200

Question: Which of the following is not an approach to network traffic measurement?

- [a] Hardware and software approach
- [b] Passive and active approach

- [c] Top to bottom approach
- [d] On-line and Off-line approach

Module 4 - Network Traffic Measurement Part 1

Network Traffic measurement plays a very important role in the design, testing and evaluation of applications that have to communicate over a network. By employing the appropriate hardware and software, any one can completely rebuild an Internet-based application.

Network Traffic Measurement: How-to

There are different approaches and techniques for measuring traffic that are discussed below.

Hardware and software approaches

Measuring Network Traffic can be accomplished in two ways- using hardware tools or software tools. Each has its own advantages and disadvantages.

Hardware-based measurement tools are called "network traffic analysers" and are devices that can collect and analyse network traffic. Such a network consists of various interface devices and each of them requires monitoring. This in turn may require a number of analysers and hence the costs may be prohibitive.

Software tools rely on operating system communications with network interfaces. Therefore, a low-end computer can be converted to run the measurement tool exclusively. This approach is cheaper, but may not offer sophisticated protocol analysis capabilities.

Internet traffic can be measured, by an efficient mechanism. When a client requests a web page or a resource through a Web Server, the Web server records all information such as IP address of the client, the date and time of request and the like in logs. Analysing these logs can generate the required information on the type and location of network traffic, eliminating the need to capture low-level packet data.

Passive and Active approaches

In the passive approach, a "monitor" is used to observe all traffic in the network without adding any of its packets to the network. This reduces the workload on the network due to the monitor and helps in accurately determining the network traffic. Almost all network traffic measuring tools adopt the passive approach.

In contrast, an active measurement device injects packets into the network and studies the response of the network to understand the network characteristics. For example, the "ping" command sends packets to a specified destination and measures the time taken to get a reply from the destination system. The time between sending and receiving can be used to gain an understanding of the amount of traffic in the network.

Another similar utility is the "traceroute", which reveals the path taken by packets to reach a specified destination.

On-line and Off-line approaches

Traffic measurement and display can be real-time, i.e., the measurement device displays traffic information "live". Such an approach is termed as "On-line measurement". This is more popular among hardware network analysers.

Another approach is to simply log all information when the device is connected to the network and then disconnect the device. Thereafter, the logs can be analysed exhaustively.

When network time is precious, it is better to use the second approach since all analysis can be done at

leisure.

Answer: [c] Top to bottom approach

Module:4

Reference No:M4201

Question: Which of the following is not a use of network traffic measurement?

- [a] Monitoring the performance of the network
- [b] To find out the efficiency and effectiveness of an application or protocol
- [c] To determine if the applications are running correctly and according to predetermined standards
- [d] None of the above

Module 4 – Network Traffic Measurement Part 2

Network Traffic measurement plays a very important role in the design, testing and evaluation of applications that have to communicate over a network. By employing the appropriate hardware and software, one can completely rebuild an Internet-based application.

Network Traffic Measurement: How-to

In part 1 we covered

- Hardware and software approach
- Passive and active approach
- On-line and Off-line approach

In this article we cover the other approaches.

LAN and WAN approaches

The factors favourable to LAN traffic measurements are:

They are strictly controlled and properly demarcated and hence getting permission for traffic measurement is easy.

Ethernet protocol that is commonly used in LANs is a "broadcast" protocol, which means that any packet is routed to all computers in the network. This makes it easier to monitor network traffic from any computer on the network.

With increased use of the Internet, traffic measurement was extended to WANs, where local administrators have no control as also the many security and privacy issues. The solution here is to deploy the measurement device at the point of interface between the organisation and the Internet.

Layer approach

Traffic can be captured at different layers of the ISO model, for instance at the Network Layer or the Transport layer. Many hardware traffic analysers can operate on a multi-layer approach. However, different network interface cards are required for different types of network connections. For example, an ATM-based network requires an interface different from Ethernet networks. However, analysis of the traffic data may be performed at a higher level or layer and hence can be independent of the type of network used.

The uses of network traffic measurement are:

1. **Network monitoring:** Network performance can be affected substantially even if one device in the network is not functioning properly. If the device is a router, a bridge or a gateway, then problem becomes serious.
Causes of such malfunctioning can range from incorrect addresses, incorrect packet sizes to hacker attacks. During such situations, traffic measurements can help network administrators to pinpoint the errant system and take corrective measurements.
2. **Application debugging:** Network applications have to be debugged, upgraded or modified frequently. Traffic measurement allows application developers to determine if the applications are running correctly and according to predefined standards. Further, upgraded applications must also comfortably work and communicate with previous versions.
3. **Workload Characterisation:** Workload characterisation analyses statistical data and generates important properties of a network application or a protocol. Traffic measurements can be used as input data to such characterisation processes, since knowledge of properties can help improve the protocols and applications.
4. **Operational Efficiency:** Network Traffic measurements can help find out the efficiency and effectiveness of an application or protocol. Analysing traffic logs can pinpoint the source of a bottleneck, if any and help develop better versions.

Answer: [d] None of the above

Module:4

Reference No:M4202

Question: Which of the following is neither an essential nor desirable aspect in evaluating an URL control list?

- [a] 100% accuracy
- [b] Easy downloading process
- [c] URL categories
- [d] Post-sales support options

Module 4 - Web filtering - URL Control List

Control of Web access resources is essential to enhance the productivity and efficiency of employees. Web filtering is one way to effectively control web access. A well-implemented Web filtering product restrains employees from accessing undesired and malicious content. It in turn creates a healthy working environment. Hence, it is essential to select an effective Web filtering solution.

The process

The web filtering process catches the web browser's request and evaluates whether the requested page falls within the organisation's web access policy before allowing, denying, or delaying the access. The software needs to ask for the adequacy of the page each time the browser requests. Therefore, the programme should understand the organisational rules and web pages. Nevertheless, it is not possible to have knowledge of thousands of millions of web pages and scan them in real time.

The dynamic content scanners promise to provide an effective web-filtering service but their accuracy, scalability and performance is limited. For example, they can only analyse a text, not pictures and graphics. Also they may have difficulty with foreign languages.

Web filtering products with URL control lists

Alternatively, Web filtering products that utilise URL control lists are considered as better products. In a pre-categorised URL control list approach, URLs are categorised into different types after analysing the content of different Web sites manually. Then they are made available at the customer site for web filtering. Whenever a user makes the request, his URL address is compared against the URL control list available in the local site. Finally, a filtering policy is employed to allow, deny or delay the access.

The following aspects must be considered while comparing one URL control list with another: -

1. **Accuracy:** - 100% accuracy of the control list is neither essential nor desirable in the corporate world. Corporate users are aware of the policies and hence, organisations need not spend excessively on 100% accurate lists to spread the policies across the organisation.
2. **Bigger lists:** - A lengthy control list may include maximum number of sites but it also consumes space on the hard drive and computer memory, time for downloading and searching.
3. **Minimal categories:** - Having fewer URL categories is an effective way of filtering lest the categories should confuse the users.
4. **Scope for suggestions:** - Control lists must provide for e-mail sites and Web-site tools to enable independent parties to submit voluntary suggestions.
5. **Easy check of URLs:** - Companies should be able to easily locate a particular URL (like their own company's site) in the control list.
6. **Update and downloading:** - Continuous updation of control lists is essential in the changing Internet era. The downloading process must be quick and preferably completed during off hours.
7. **Technical differences in database design:** - Technical design affects the speed with which the filtering engine is being searched. Hence, the new software should improve the company's performance and minimise the search time.
8. **Preventing control breaks:** - The URL filtering tool must be capable of preventing the clever ones to break the controls.
9. **Price factor:** - The subscription price (which may be based on per-user, per-server or categories), annual support fees, and cost of switch over to another service must be checked.
10. **Post-sales support options:** - Post sales supporting options must be verified before purchasing the software product.

Answer: [a] 100% accuracy

Module:4

Reference No:M4203

Question: In the case of technological infrastructure, the audit working guideline should provide for the test of which of the following?

- [a] Modifications made to technology plans to reflect the cost and identified risks
- [b] Communication of the management's policies on internal controls
- [c] Compliance with the segregation of duties principle
- [d] Provision of a security review for all IT functions

Module 4- Audit working guideline

Defining the technological infrastructure

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Define the technological infrastructure	1. Planning 2. Setting of standards 3. Acquisition plans 4. Technological obsolescence 5. Analyse future trends	Not applicable for this activity

Audit Process

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. CEO 2. COO 3. CFO 4. CIO 5. IT steering committee member 6. IT management	1. Policies and procedures 2. Roles and responsibilities 3. Business objectives 4. IT objectives 5. Technology acquisition plans 6. Technology plans 7. Technology guidelines 8. Reports and minutes of steering committee meetings

Preliminary analysis

The next step is analyse the effectiveness of the control measures adopted and the degree of reliability that can be placed on the control measures. This can be done through ensuring that

1. Technology plan
 - Is updated based on a defined process
 - Considers the cost of implementing plans
 - Takes into account risk factors
 - Approval of all updations by the concerned personnel
 - Is based on the long and short term IT plans
2. Processes exists to assess the status of the technology in the organisation

3. Technology plans allow evaluation of the available technology and its integration with the organisation's technology when required
4. Impact of technology on the organisation's environment and working
5. IT policies evaluate the plan for contingencies
6. Technology acquisition plans are based on overall technology plans
7. Technological guidelines exist for all technology components

Tests of controls

A clear picture of the functioning of the controls can be gained by

- Obtaining evidences
- Reviewing the deliverables

Tests: The following tests have to be done, before an opinion is formed on the functioning of IT tasks in the organisation.

1. Management awareness and use of IT plans
2. Modifications made to the technology plans to reflect the cost and identified risks
3. Consistency between technology and IT long term and short term plans
4. Incorporation of the appropriate current technologies with the existing technologies implemented in the organisation
5. Assessment of contingency requirements and its inclusion in the technology plans
6. Physical environment of the IT department accommodates new technology acquired as per plan along with the existing technology
7. Consistency between acquisition and IT long range and short range plans
8. Technology plan emphasis on the use of current and new technology
9. Technology guidelines are defined properly
10. Access levels are in accordance with security levels

Tests should be performed to ensure that the above identified control measures are taken in the preliminary analysis section

Substantive Testing

This step is undertaken so as to substantiate the auditor's view of controls objectives either not being met or not existing. The control weaknesses observed and its impact will have to be documented. In order to further substantiate the viewpoint comparative benchmarks from similar organisation, industries can be identified.

Identification of shortfalls

The auditor should identify:

- Failure to identify contingency aspects
- Inconsistency between technology acquisition plans and IT plans
- Inconsistency between technology acquisition plans and the IT guidelines
- Non-inclusion of main elements in the data dictionary, redundancy in the dictionary and data syntax rules
- Failure to restrict access to sensitive data as per the defined security level

Answer: [a] Modifications made to technology plans to reflect the cost and identified risks

Module:4**Reference No:M4204**

Question: With regard to auditing quality management in IT implementation, to ensure that Quality standards are in tandem with changing environment the auditor should verify that

- [a] The SDLC process is regularly reviewed by management
- [b] Co-ordination exists between users and developer
- [c] Involvement of all categories of the users
- [d] All of the above

Module 4- Audit working guideline**Quality management****Table of applicability**

For IT task	Control objectives	
	Management controls	Operational controls
Quality management	1. Planning 2. Quality compliance procedure 3. In-house development of the technology 4. Acquisition of technology 5. Relationship with the vendor 6. Testing 7. Documentation 8. Review 9. Quality measurement 10. Reports	Not applicable for this activity

Audit Process

The Audit process has been covered in two parts. In the first part, the preliminary understanding and analysis have been covered. In the second part, the test of controls and substantive testing have been dealt with. This article is first in the two-part series.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. CEO 2. CIO 3. Organisation's quality assurance department	1. Quality assurance, system development, system documentation policies and procedures

representative 4. IT function's quality assurance department representative 5. Security management representative 6. Steering committee members 7. IT function representative 8. Owners/users	2. Planning & steering roles and responsibilities 3. Organisation and IT function quality manual: 4. IT objectives 5. Long term plans of IT function and the organisation 6. Minutes of SDLC review meetings 7. Minutes and reports of IT steering committee meeting 8. Minutes of quality committee meetings 9. Configuration management 10. Job responsibilities of key personnel/senior management

Preliminary analysis

The next step is analyse the effectiveness of the control measures adopted and the degree of reliability that can be placed on the control measures. This can be done through ensuring that quality plan/procedure of the IT function consists of /provides for the following details

1. Compliance with organisation's long term and short term plans
2. A standard approach, which is applicable to all IT activities project or otherwise, communicated and understood by all personnel of the organisation.
3. A comprehensive approach to the quality assurance activities which prescribes the scope, timing and quality assurance activities to be performed
4. Assurance for adherence to organisation's IT standards, policies and procedures
5. The SDLC methodology adopted by the organisation provides for a complete and detailed approach for both system acquisition and in-house development. The methodology should define the various stages and ensure that project is checked and authorised at each milestone. It should be flexible, scalable and suitable to all types of changes. It should provide for the conditions required while dealing with third party transactions. It should provide for detailed documentation that is current and clear. It should ensure that all projects are tested at each relevant stage.
6. The quality assurance approach adopted by the management should ideally have following components
 - Ensure that all new or changed existing systems are reviewed for adherence to the SDLC approach by the organisation
 - Ensure that system implementation complies with organisation's standards and IT long and short term plans
 - Provision of appropriate report to the management and follow up of the same
7. The quality assurance approach should also ensure that SDLC approach is reviewed by management for changes/developments, existence of different levels of controls appropriate to the size of the project, involvement of related and affected departments, co-ordination and communication between IT staff and users.

Answer: [a] The SDLC process is regularly reviewed by management

Question: With regard to auditing quality management in IT implementation, to ensure that Quality process ensure adherence to the SDLC methodology the auditor needs to

- [a] Ensure compliance of the quality process with the technological framework prescribed by SDLC methodology
- [b] Review the quality assurance post implementation review reports
- [c] Ensure the existence of adequate Programme and system testing documentation
- [d] All of the above

Module 4- Audit working guideline

Quality management-2

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Quality management	1. Planning 2. Quality compliance procedure 3. In-house development of the technology 4. Acquisition of technology 5. Relationship with the vendor 6. Testing 7. Documentation 8. Review 9. Quality measurement 10. Reports	Not applicable for this activity

Audit Process

The Audit process has been covered in two parts. In the first part, the preliminary understanding and analysis have been covered. In the second part, the test of controls and substantive testing have been dealt with. This article is second in the two-part series.

Tests of controls

A clear picture of the functioning of the controls can be gained by

- Obtaining evidences
- Reviewing the deliverables

Tests: The following tests have to be done, before an opinion is formed on the functioning of IT tasks in the organisation.

1. Ensure that following documents are used as inputs for developing a quality plan

- Organisations long term and short term plans
 - IT long term and short term plans
 - Organisation's quality plans and procedures
 - Change management plan
2. The IT plan has the following components
 - The benchmark level of service
 - Error tolerance levels
 - Definition of statistics to be collected to measure performance
 3. To ascertain the compilation of quality plans and procedures by the staff
 4. SDLC methodology ensures
 - Existence of adequate controls
 - Communication to all relevant employees
 - User approval and sign-off
 - Provision for change management
 - Provision for adequate configuration management
 - Review of test results
 - Adequate problem management
 - Quality assurance review for post-implementation
 - Involvement of users
 5. Auditor should also ensure that quality assurance review reports are communicated to the management and the remedial actions are undertaken by them.

Substantive Testing

This step is undertaken so as to substantiate the auditor's view of controls objectives either not being met or not existing. The control weaknesses observed and its impact will have to be documented. In order to further substantiate the viewpoint

1. Comparative benchmarks from similar organisation, industries can be identified.
2. Review of sample projects to ensure
 - The compilation of SDLC methodology
 - The adequacy of the methodology
 - Satisfactory completion of development
 - Acquisition of approvals and sign-offs
 - Compliance with technological framework
 - Conduct of quality assurance review
 - Adequacy of project documentation
 - Adequacy of testing procedures and the related documentation
 - Adequacy of post implementation review process

Identification of shortfalls

The auditor should identify

- Quality plans that do not meet long term and short term plans
- In appropriate SDLC methodology

- Lack of communication and co-ordination
- Non-adherence to SDLC methodology
- Non-existence or inadequate testing and related documentation
- Non-Performance of post implementation quality reviews
- Non-action by management on the quality review reports

Answer: [b] Review the quality assurance post implementation review reports

Module:4

Reference No:M4206

Question: A cookie gets data from

- [a] Whatever the user enters from the console on a web page
- [b] What the web server sends to the web browser
- [c] User application programs
- [d] The operating system and the web browser used at the client end

Module 4- COOKIES- PART I

Definition: A piece of information that is stored in the computer's hard disk by a website is known as cookie. The web servers use these in order to identify the user. The purpose of a cookie is to save technical information in memory for future reference. Such information is stored at the client side. The data entered by the user while visiting various websites (say for example, name, interests and other user-specific information) is the basis of information to the cookies.

The term cookies originated from objects in UNIX, known as magic cookies. Magic cookies are tokens put together with the user's program that keep changing as and when the working environment of the user changes.

How do cookies work?

Cookies are attached to the HTML pages that move between the client and the web servers. The cookies work on a two-stage process. The web browser stores the cookie in a special cookie list or directory in the user's machine without his awareness, in the first stage. In the next stage these stored cookies are conveyed to the Web Server.

Facts and myths about cookies:

- **Myth 1:** Cookies are programs, which can attack the hard drive of the machine of the user.
Fact: Cookie is not a program code. It's merely a brief piece of information usually in the form of text files for technical use by the web server. Hence cookies cause no problem to the user's machine.
- **Myth 2:** Cookies can trace intimate details like the user's credit card number, bank account number, computer passwords and the like.
Fact: Cookie is not an executable program. It gets data from what the web server sends to the web browser, nothing more.

What kind of information does the cookie store then?

Any request from the client to the server includes IP address, type of browser and the operating system of the client. This information is stored in the cookie by the web browser. Whenever the user tries to access the same server again, this information is passed on to the server along with the request, so that the server identifies the user and sends the page requested by the user. The cookies are sent back to the servers that originally sent them to the user's browser and eventually stored it in the user's machine, and not to anyone else.

In practise, adding a line of text along with the Header in the HTML document generates a cookie. The syntax in the document to enable cookies is:

Set-Cookie: <name =value>; expires = <date>; path = <path>; domain = <domain_name>; secure

The strings within <> are set by the server.

Attributes of the cookie:

- The '**name=value**' part store the information that the web server passes to the client when a page is requested by the user.
 - **Date** is an attribute that sets the time limit until which the cookie can be stored in the user's system. Setting it to a relapsed date deletes the cookie. Similarly a cookie set to an approaching date can be stored for future. Such cookies are known as persistent cookies. If the date attribute is left empty, the cookie though stored in the memory gets deleted the moment the communication session ends.
 - **Domain_name**: Address of the sender of the cookie (the web server) is stored in the **domain_name**. The default value of the **domain_name** is the address of the server that sets the cookie.
 - **Path**: **Path** is an attribute for matching the **domain_name** and the path. Unless the two match the cookie is not sent.
 - **Secure**: This allows the cookie to be sent only if the channel used for sending the cookies is safe.
- Cookies-Part II deals with how cookies are used by various websites and how safe are cookies from catching viruses.

Answer: [b] The data in cookies are the ones sent by the web server to the browser. It does not get information from any other source which is why they cannot access intimate user related information like passwords, credit card numbers and the like.

Module:4

Reference No:M4207

Question: Physical Layer

- [a] Refers to physical components like cable, wires and the like used in communication
- [b] Specifies the protocol for physical requirements of communications
- [c] Refers to physical addressing of each workstation in a LAN
- [d] Is in charge of flow control

Module 4- The Physical Layer

The physical layer is the lowest layer of the ISO-OSI reference model. The key function of the Physical Layer is to transmit raw-bits (i.e. where incoming and outgoing entities are in the form of a '0' or a '1'). It converts the frames into raw bits and sends them over a communication channel. It provides electro-mechanical support to the physical medium. Thus, physical layer shouldn't be confused with the physical media like wires and cables. It is a combination of both hardware and software programming, which includes hardware design like electrical and mechanical interfaces and software implementations (say what voltage would represent a '1' or a '0'). The physical layer protocols define the physical requirements like electrical, mechanical and so on, in order to trigger, preserve and switch off a physical link between two workstations. It also specifies cards, NIC attachments to hardware, and techniques to transfer bit stream to cable. **NIC** (Network Interface Card) is an electronic circuit board that connects individual workstations to the network. It is exclusively devised for LAN connections.

The various kinds of cables and circuits used for communication in the physical layer include open wire circuits, twisted pair cables, fibre optical cables, coaxial cables and the like.

Signalling of bits: The physical layer specifies as to how a bit is expressed in form of voltage, phase, frequency, or phase. Some of the major schemes employed for the purpose comprise the following:

- ☐ Pulse signalling
- ☐ Edge / phase signalling
- ☐ Level signalling

Pulse signalling (Return-to-Zero) is a type of transmission in which each bit of zero or one is represented by the presence or absence of a pulse. Typically, the presence of a pulse signifies a '1' and the absence of a pulse represents a '0'. In return-to-zero, the state of the signal is represented on the basis of the voltage during the first half of the pulse. The pulse comes back to zero in the second half (resting phase). Generally, zero volts represent a resting state.

Edge signalling / phase signalling as the name suggests, is a type of data transmission in which, the shift of a pulse from rising edge to low or from falling edge to high determines a '0' or '1' respectively, i.e. the edge of a pulse determines the value of the bit. This type of data transfer is also known as Manchester encoding.

Level signalling uses the level of the pulse, i.e. a high or low for a '1' or '0' respectively. Typically a less positive or a more negative voltage is used for symbolising a '0', while a more positive or less negative level signifies a '1'. This is also known as non-return-to-zero.

Timing the bits: Communication can be of two types - synchronous and asynchronous. *Synchronous* systems have all the events coordinated with a timing device or a clock, i.e. every transition in the signal coincides with the clock. *Asynchronous* systems are not timed. The occurrences in these systems are not coordinated with time.

The physical layer is set to synchronous mode for demarcation so as to prevent the overlap a bit with other bits. Timing also involves verification of the raw-bits received using CRC (Cyclic Redundancy Check). It not only determines the number of errors present in the transmission, but corrects them as well.

Answer: [b] Specifies the protocol for physical requirements of communications

Explanation: The physical layer is a combination of hardware and software that specifies the physical requisites for communication. While a physical layer does comprise physical components like cables, wires it does not solely refer to it.

Module:4

Reference No:M4208

Question: Which one of the following is absent in the TCP/IP reference Model?

- [a] Presentation Layer
- [b] Host-to-network Layer
- [c] Transport Layer
- [d] Application Layer

Module 4- TCP Vs OSI- A Comparison

The two reference models, namely the TCP/IP and the ISO-OSI both share a number of similarities and differences. Despite the differences, implementation of one of the protocols does not conflict the standards of the other. This is because both these reference models were developed at the same time. In other words, they are complimentary. The two layers can be different with respect to

- ☐ The number of independent Layers in each of these models
- ☐ The services and protocols offered by the two models
- ☐ The functionalities of the two
- ☐ The mode of transmission used by both

The major differences are confined to the layers above the Transport Layer (Layer 4) and the Network Layer (layer 3). The fundamental requirements of the TCP/IP reference model like dynamic routing, packet switching, universal connectivity and connectionless protocols is the basis of these differences.

Differences in the number of layers of the two:

The OSI reference model has seven independent layers while there are only four layers in the TCP/IP reference model. The Session Layer and the Presentation Layer precede the Application Layer of the OSI model, while in TCP both these (the session layer and the presentation layer) are combined into an Application Layer. Further, the two separate layers, namely the Datalink Layer and Physical Layer of the OSI model are merged into one layer known as the Host-to-Network Layer in TCP model.

The diagram below shows how the two layers differ in their layered architecture:

OSI Reference Model	TCP/IP Reference Model
APPLICATION LAYER	APPLICATION LAYER
PRESENTATION LAYER	Not present
SESSION LAYER	
TRANSPORT LAYER	TRANSPORT LAYER
NETWORK LAYER	INTERNET LAYER
DATALINK LAYER	HOST-TO-NETWORK LAYER
PHYSICAL LAYER	

PHYSICAL LAYER

Differences in the services and protocols of each layer:

The services in the TCP/IP are not very clearly defined unlike those in the OSI Model. In the OSI Model, protocols are encapsulated and can be replaced with technological advancement.

Physical and the Datalink Layer:

- In case of a TCP/IP model, the Physical and Datalink Layers are merged into one, namely the host-to-network layer.
 - o In OSI, the standards for the physical medium of transmission, protocols for transmission of data packets from host to host are clearly defined. While, in TCP/IP, there is no clear mention of how the transmission takes place. It just says that the host has to get connected to the Internet using some Internet protocol (this protocol is not defined clearly).
- In fact the host-to-network layer of the TCP/IP model is just an interface (a conceptual layer) that lies between the network and the datalink layers.

Network Layer:

- The Network Layer of the OSI model deals with the routing of the data packets and establishing the physical connection between two workstations, using protocols ES-IS. In TCP/IP, it is known as the Internet Layer, which uses an IP (Internet Protocol) to route the data packets from source to destination. This is not a dependable method, since the order of receipt of packets may vary and at times may get lost in transmission

Transport and Application Layer:

Both the models share similar protocols in the Transport Layer and the Application Layer.

Answer: [a] Presentation Layer

Question: Which of the following functions is true of the Presentation Layer?

- [a] Interacts with the user
- [b] Attempts to merge two incompatible machines
- [c] Helps in writing application programs
- [d] Makes end to end data transfer independent of machine compatibility

Module 4- THE PRESENTATION LAYER of the OSI Reference model

The Presentation Layer converts data in an appropriate form using a variety of coding methods, and provides readability from one application layer (sender) to another application layer (recipient). For e.g. conversion of a simple stream of text into a pop up menu with the newly entered text and things alike, is done by the presentation layer. The Presentation Layer ensures that the information is passed in an appropriate form to the recipient.

The chief functions of the Presentation Layer involves

- Transforming data into a form that can be accepted by the Application Layer
- Formatting and encrypting the data which is sent to the recipient across the network irrespective of the compatibility between various machines
- Making the transfer of data from one end to the other independent of the differences in the format data and its representation

A Presentation Layer can be broadly viewed as an intermediate layer flanked by the Application Layer (that accepts inputs regardless of the varying data representations) and the Session Layer (that actually takes input from the Presentation Layer prior to establishing the connection).

The programs running in the Presentation Layer chiefly adhere to the following:

- Data Representation (i.e. the format of data that is entered at the user end or transferred to the end user, namely ASCII, Binary or Postscript)
- Compatibility with the recipient's workstation (i.e. with the operating system at the user-end)
- Data encapsulation in form of "envelopes" for transmission of data across the network

The Presentation establishes a common format for representing data, images, motion pictures, and sounds for proper communication between two incompatible computers. For this reason, the Presentation Layer is also known as the *syntax layer*. This is accomplished by proper data conversion schemes using data compression and encryption. *Conversion schemes* make possible exchange of information between two machines with varying data and text representation. Some examples of standard data representation schemes are ASCII, EBCDIC and the like. Prior to the transfer of information, data is first compressed or encrypted, which is then decompressed or deciphered at the recipient end. Some of the examples of standard compression implementations include the MPEG (Motion Picture Experts Group) and QuickTime. GIF (Graphics Interchange Format) and JPEG (Joint Photographic Experts Group) are standards for graphic coding and compression.

HTTP- An illustration of program functioning in the Presentation Layer:

The most popular instance of a program, which strictly adheres to the Presentation Layer of the OSI reference model, is the HTTP (Hypertext Transfer Protocol). This protocol is generally included in the operating system. HTTP can be thought of as a messenger, between the web browser and the web server. It conveys what the web browser takes in from the user in standardised form to the web server. It specifies a set of rules that govern the standards of exchange of text and images between two ends. Upon receiving the information, the web server sends a notification with a MIME (Multipurpose Internet Mail

Extension) header, indicating the file type namely, text, audio or video. This helps to determine the system compatibility of the recipient and accordingly convey the message.

Answer: [d] Makes end to end data transfer independent of machine compatibility

Explanation: The Presentation Layer standardises the input/output forms to and from the user in order make data transfer across the network independent of machine compatibility.

Module:4

Reference No:M4210

Question: A session is

- [a] A link between two network nodes
- [b] Series of transmissions without any disconnection
- [c] A specific connection place in a system
- [d] Bi-directional dataflow between two network nodes

Module 4- The session layer--- An association between the endpoints of communication

The start off: The 5th layer of the ISO-OSI reference model, commonly known as the Port Layer governs and maintains the connection between two end points. A **connection** builds the communication link between two points. A series of inter-related connection-oriented transmissions without termination of the connection is known as a **session**. The duration of sessions may however vary. Thus, while some may last only till the message reaches the other end, others are long enough to support bi-directional transfer of information. More precisely, the Session Layer actually supports the Presentation Layer by creating, maintaining and terminating a connection.

In Web applications, each session is linked to a port. A **port** is a specific connection either physical (in case of computer and telecommunication devices) or logical (in programming especially used in the Internet). In this context port refers to a logical connection or a number, which is associated with some application program running at the application layer.

Establishing connections, maintaining them, synchronising communications, managing dialogues and terminating them are the chief functions of the Session Layer.

How the sessions are governed

To start with, the connection is established between two ends after authenticating the users at both the ends. Then the roles of the protocols of this layer and the type of communication (connectionless or otherwise) is determined. The sender and the recipient are identified by data transfer and dialogue control. The data transfer and dialogue controls also specify whether it is necessary for the recipient to acknowledge the receipt of data or not.

Transmission modes: The three fundamental modes of transmission in any layer viz., *simplex communications* (unidirectional data flow), *half-duplex communications* (bi-directional data flow, one way at a time) and *full-duplex communications* (simultaneous bi-directional dataflow). The Session Layer uses half-duplex mode.

Examples of Session Layer implementations and services:

The services and protocols defined for the Session Layer include RPC (Remote Procedure Call), SQL (Structured Query Language) and SCP (Serial Communications Protocol).

RPC or Remote Procedure Protocol also known as the function call or subroutine call is a protocol that uses a client /server model to request a service from an application loaded in a remote computer without getting into the intricacies of the network. The requesting program functions as a client while the service providing program serves as a server.

SQL or the Structured Query Language is a user-interactive programming language that enables a user to access information from the existing database for data updates or for manipulation. It is both an ANSI and ISO standard. The queries given by the user are taken as command (of accepted standards) that aid in insertion, deletion and updating of data from the database.

A Communication Protocol establishes a set of rules governing the rate of flow of data between two terminals and the mode of transmission (i.e. whether it is half-duplex or full-duplex).

SCP or the Serial Communications Protocol governs the communication between two machines that are pre-configured to communicate with each other. A relevant example in this context will be an Internet cable connection for the computer. In this case the service provider's server responds to the requests and delivers them to the Internet and vice versa.

Answer: [b] Series of transmissions without any disconnection

Module:4

Reference No:M4211

Question: File transfer is

- [a] An Application program
- [b] One of the functions of the Application Layer
- [c] A protocol of the Application Layer
- [d] A web application

Module 4- THE APPLICATION LAYER of OSI Reference model

Introduction: The Application Layer is the most layer of the ISO-OSI reference model. This is the layer that interacts with the end-user directly. The Application Layer facilitates the application programs to run at the user end thereby making communication possible between any two ends. It is not the application program though. In fact it provides an environment for the application programs to run on a machine.

Application Program is the software that enables the user to perform a specific function or at times facilitate devising new application programs. Some of the examples of application programs are text editors, database programs, word processors, and development tools like paint, drawing and image editing programs. An application program uses the system programs of the computer like operating programs, compilers and the like in order to make possible for the user to interact with other machines in the network.

What exactly the Application Layer does? There are countless computer terminals in the world that are incompatible with each other, which might lead to a disfigured view of a program running on different terminals. For example the screen of a text editor might shrink or expand according to the size of the monitor of the terminal, which in turn would pose a problem in viewing it. An incongruity among various workstations calls for a universal platform that can map these application programs onto all the real terminals across the globe. The Application Layer provides this platform wherein users at all terminals view the same representation regardless of their mutual incompatibility. In gist, the Application Layer acts as an interface between what the user sees on the screen and the background work.

Another key function of the Application Layer is file transfer. This includes handling transfer of files with different naming conventions, varying file organisation, different text lines' representation and the like.

The protocols in the Application Layer should conform to the following functions:

- ☐ Identification and authentication of the receiver and sender of the information
- ☐ Ensuring the presence of resources necessary for the communication
- ☐ Maintenance of data integrity and privacy at both the ends
- ☐ Establishing protocols and data syntax at the application level

Application Layer Implementations:

The various kinds of application programs (services) run on the application layer are electronic mails, newsgroups, web applications and network management. Some of the examples of these programs include Telnet, File Transfer Protocol (FTP), Network Filing systems (NFS) and so on. **Telnet** is a software that allows a user to log on to a remote machine connected to a network and access data, interactive environments and libraries stored in that machine. FTP is an application that enables transfer of files to a workstation from an FTP (downloading) server or vice versa (uploading). The user has to log on to the FTP server in order to transfer the files. NFS is a Client / Server application devised by Sun Microsystems. It facilitates accessing shared files through an interface (Virtual File System).

Answer: [b] One of the functions of the Application Layer

Explanation: Often confused with File Transfer Protocol (the FTP which is an application program run on the application layer), is just a function of the application layer. It is different from FTP.

Module:4

Reference No:M4212

Question: Which of the following is not a function of the Datalink Layer?

- [a] Controlling the data flow
- [b] Transmitting raw bits over the communication channel
- [c] Error control
- [d] Framing

Module 4- The Datalink Layer- Layer 2 of ISO-OSI reference model

The Datalink Layer connects the Network Layer (that switches data packets along appropriate paths / routers) and the Physical Layer (the lowest layer of the OSI). The Datalink Layer acts as an interface between the two, and oversees that there is an error-free transmission of Data packets from the Physical Layer to the Network Layer. The activities of the Datalink Layer include assembling the raw bits received from the Physical Layer into frames, managing and controlling the errors during data transmission and regulating the rate of flow of data.

At this layer, the data encoding and decoding takes place. The IEEE-802 LAN standard has specified two sub layers of the Datalink Layer viz.,

- Media Access Control (MAC) Layer
- Logical Link Control (LLC) Layer

The Protocols defined in the Datalink layer specify features of different networks taking into consideration the modes of physical addressing, flow control, ordering of data frames and information related to errors in transmission.

The Media Access Control (MAC) Layer: The Media Access Control (MAC) Layer specifies protocols for physical addressing. It takes care of the data framing function of the Datalink Layer.

It uses a MAC address in order to connect every computer in the network. **MAC address** is a unique number stored in each computer's hardware that gives each computer's address in a LAN (unclear; pl rephrase I had left address with MAC, so it looks unclear). When a computer is connected to the Internet, the IP address maps itself with the physical address in LAN. One of the protocols that works in the MAC layer is Ethernet (a ic already covered in one of the articles).

The Logical Link control (LLC) Layer: The Logical Link Control (LLC) Layer is in charge of Data flow and error control. Theoretically the LLC is above the MAC Layer in the Datalink Layer. It servers both connection-oriented and connectionless transmissions.

In connectionless services the receiver receives no acknowledgement due to which transmission is faster. This kind of transmission is usually implemented at this layer only, since the upper layers of the OSI have their own error checking and control.

In connection-oriented services, the receipt of each message is duly acknowledged. Due to this, the transmission is slower as compared to the connectionless connection.

Flow Control: Many times the rate of transmission of data from the sender exceeds the processing limits of the recipient. This leads to loss of data packets during the transmission. To manage the rate of flow of data to the devices without losing or re-transmitting (to transmit only the amount of data that can be handled by the device) is known as **flow control**.

Flow Control can be implemented either by hardware flow control or by software flow control.

Error detection: The Datalink Layer through error-detection evaluates each transmission across a wire to assure that the data transfer is error free. For this it makes use of a pre-calculated value named CRC (Cyclic Redundancy Check). The Datalink Layer only detects the error present in the transmission. It does not carry out error recovery.

Answer: [b] Transmitting raw bits over the communication channel

Explanation: Transmitting raw bits over the communication channel is a function of the physical layer. The Datalink Layer just assembles the raw-bits received from the Physical Layer and checks for any errors present therein.

Module:4

Reference No:M4213

Question: Cookies can prove to be a nuisance by

- [a] Passing on viruses to the client's system
- [b] Passing information about user's preferences to shopping sites
- [c] Passing valuable information such as user's credit card number to the web server
- [d] Being persistent in the system

Module 4- COOKIES PART -II

A piece of information that is stored in the computer's hard disk by a website is known as cookie. The web servers use these in order to identify the user.

COOKIES-part I discusses in detail on what cookies are and how they are enabled.

How cookies are employed by various web sites:

- The shopping sites use cookies in order to maintain a record of the user and his shopping cart. A cookie with an ID number (for the shopping cart) is sent to the user when he visits the site for the first time. For every new item selected by the user, the tag attached to the cookie records the new addition. When the shopping is complete, the list of items stored in the tag assists the 'checkout' page in listing all the items selected by the user. This way the listing by the checkout page is done easily in one go, thereby saving time. Otherwise the user has to remember all the items he wants to buy and then list them out separately in the end of his shopping.
- Cookies are also employed for creating customised web pages for the user. Every time the user specifies his preferences for the customised web page, a cookie is sent to the web server. Thus when the user logs in the next time the web server recognises the user and sends the customised web page. In the absence of cookies, the web server would have to identify the user every time he logs in and has to save the customised settings as many times.
- Cookies are also put to use in advertising. A marketing site that serves many clients uses cookies to keep track of user's browsing preferences in its client sites. The website attaches a URL tag (that advertises

one of its clients) to the cookie). This tag appears at the user end every time the user views any site containing a product of the client site.

Keeping track of persistent cookies:

Cookies set to a future date (described in part I of cookies) are known as persistent cookies. The location of these cookies depends on the type of browser. For e.g. If the client uses Microsoft's Internet Explorer, then these cookies are stored in a separate folder under Windows named 'cookies'. Netscape Navigator stores cookies in one single text file named as 'cookies.txt'.

The user can delete these files if he considers them to be useless.

How to stop the browser from accepting cookies: Simply by changing browser options, one can prevent the browser from accepting cookies. In Internet Explorer clicking the 'Disable all cookie use' option will stop the system from accepting cookies.

Using cookie-blocking software: Cookies can be blocked 'cookie-blocking' software. All the user needs to do is mentioning the name of sites, which he feels can send him cookies.

How safe are cookies from virus?

A cookie being a text file cannot be of any threat to the system. Since virus is an executable program, the cookie files also have to be executable in order to damage a system. But even if the cookie is executable it cannot infect a system unless the user runs it, which is a remote chance as passing on an executable program to a text file is highly improbable.

Thus, cookies in general are not capable of damaging the computer. The only downside of cookies is that they send information about the users to web servers thereby making the users a victim of various companies who try to lure them into buying their products.

Answer: [b] Passing information about user's preferences to shopping sites

Explanation: By passing user preferences to the shopping sites makes him a victim of advertisements of different companies or products that in a way becomes a nuisance for the user. Persistent cookies can be deleted if the user chooses to.

Module:4

Reference No:M4215

Question: Which of the following is not an advantage of Virtual Private Networks (VPN)?

- [a] Low capital requirement
- [b] High pay-back period
- [c] Less expensive than leased line networks
- [d] More flexible than WAN technology

Module 4- Virtual Private Networks for Branch Networking

Banks have several choices like a central data base server or a distributed network for implementing branch networking. They may choose to use the secure conventional WAN technology. However, it may require efficient infrastructure facilities like power, bandwidth and communications.

VPN (Virtual Private Networks)

Banks also have to meet the expectations of different categories of customers. In addition, short and long term objectives, project costs, ROI, competitors, and the customer base need to be looked into. Integration of the network with the strategic objectives of bank need to be clearly understood before the generic

architecture for the networking is planned. In this scenario, banks may tend to adopt Internet technology for their applications. The result is the development of VPN (Virtual Private Networks).

In a Virtual Private Network, a private network is executed over a public facility like an Internet service provider or an ATM network. Different types of VPNs are available. Remote access VPN with client- initiated tunnel is best suited for the banking environment.

A tunnel is used between a server and a remote client. It is a secured communication medium. It ensures the authentication of users, and supports data encryption, address management and multiple protocols.

VPN provides the following advantages: -

- Less expensive than leased line networks
- Low capital requirement
- Low pay back period
- More flexible than the traditional WAN technology. There exists an alternate pipe if any Internet link fails.
- Allows the management to concentrate on core business objectives by saving time otherwise spent in operating the corporate network.

Security aspect

Security of VPNs is an important issue. They must be protected against unauthorised access to prevent the leakage of confidential data. Proper controls like encryption, authentication and access controls must be placed. Tunnels, encryption, packet authentication, user authentication, auditing, firewalls and intrusion detection systems are some of the essential elements, which a VPN security solution must have. These protect the VPN at different levels.

Additional security measures

Additional security measures include assigning a user ID and password to the cyber account holder and the use of multiple servers. Multiple servers provide consistency in operations in case one site is attacked by hackers. Customer's photographs and signatures should be stored in the central database, to serve as an effective control for customer identification. In this way, customer and branch staff can perform the transaction simultaneously.

This facility also enables the customer to check his account statement and payment details from home. The customer can also make transfers from his savings account to his checking account to ensure control over cheque payments. The cyber branch facility provides scope for multi-branch banking.

VPN applications in the banking scenario

In the first phase of application, customers are allowed to make transactions related to cash and transfers at the branch. In the second phase, customers can make online transfers between accounts. In the third phase, business concerns are also involved in money transfers. They can make transfers from the business house.

A VPN is not the only alternative for banks for branch networking. Banks have to evaluate the alternatives available and select one, which is best suited for their requirements.

Answer: [b] High pay-back period

Question: Which of the following statement is "FALSE" with regard to Incident management?

- [a] Identification of incident
- [b] Prioritisation of the incidents and their documentation
- [c] Escalation of all the problems to senior management
- [d] All of the above

Module 4 – Audit working guideline

Problems/ incident management Part 1

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Incident management	1. Incident identification and reporting 2. Escalation 3. Audit trails 4. Emergency procedures	Not applicable for this activity

Audit Process

The audit process has been covered in two parts. This article is the first part, and deals with a preliminary understanding and analysis of the process.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. Operations team 2. Help desk 3. Support team 4. Application support team 5. Users	1. List of facilities used for incident management 2. List of people involved in incident management 3. Policies and procedures regarding • Identification • Recording • Resolving • Escalation • Reporting of incidents 4. Details of • Incident reported

	• Date of occurrence • Date of escalation, if any • Date of resolution • Time within which the problem was required to be resolved 5. Details of vital applications for resolution by the senior management 6. Methodology for ascertaining whether that the problems are identified, resolved and reported

Preliminary analysis

The next step is to analyse the effectiveness of the control measures adopted, and their reliability. This can be done by ensuring that the following are in place:

- Process to identify, record, resolve and report all the operations that are not part of the standard operations
- Process of incident management for
 - o Defining the problems
 - o Recording, and resolving them
 - o Generating reports for vital applications and reporting them
 - o Prioritising incidents based on risk
 - o Documenting the priorities and its approval by the senior management
 - o Determining the access controls for information generated from incident management
 - o Distributing the information on need to know basis
 - o Analysing the trends of incidents to reduce the turnaround and to maximise the use of resources
 - o Escalating the problems to appropriate personnel
 - o Evaluating the incident management process by the management at regular intervals to increase its effectiveness and efficiency
 - o Audit trails
 - o Coordinating and integrating the incident management with configuration management system and its staff
 - o Emergency handling procedure that provides for
 - Use of standard forms for documenting the access to facilities
 - Management approval
 - Communication of the changes to the security
 - Termination of the access after a defined period

The next articles focuses on test of controls and substantive testing.

Answer: [c] Escalation of all the problems to senior management

Module:4

Reference No:M4217

Question: In order to assess the weaknesses in incident management the auditor should identify

- [a] Whether operational levels are communicated to the appropriate personnel
- [b] Incidents that are not resolved as per the defined process
- [c] Projects that are not adequately tested
- [d] Failure in identifying and recording the costs

Module 4 – Audit working guideline

Problems/ incident management Part 1

Table of applicability

For IT task	Control objectives	
Incident management	Management controls	Operational controls
	1. Incident identification and reporting 2. Escalation 3. Audit trails 4. Emergency procedures	Not applicable for this activity

Audit Process

Audit process has been covered in two parts. In the first part the preliminary understanding and the preliminary analysis has been covered. In the second part the test of controls and substantive testing has been covered. This is the second article.

Tests of controls

A clear picture of the functioning of the controls can be gained by

- Obtaining evidences
- Reviewing the deliverables

Tests: The following tests have to be done, before an opinion is formed on the functioning of IT tasks in the organisation.

- Process exists for identification of incidents
- Problems that are highly critical and hence of high priority should be escalated to senior management
- Problems with vital applications are escalated to senior management
- Reports generated provide information that is accurate
- Reports are distributed to the required personnel
- Action is taken based on the reports
- Satisfaction of the users
- Personnel interviews to determine the awareness and understanding of incident management process

Tests should be performed to ensure that the identified control measures in the preliminary analysis section are functioning as desired.

Substantive testing

This step is undertaken so as to substantiate the auditor's view of control objectives either not being met or not existing. The control weaknesses observed and its impact will have to be documented. In order to further substantiate the viewpoint select few of the incidents that have been reported.

- Ensure that the incident management have been recorded and appropriate procedures have been followed.
- Test whether all the changes and resolutions were tracked.
- Also ascertain that:
 - o Incidents related to vital applications were escalated to senior management
 - o Incidents were prioritised
 - o Incidents were reported to the required personnel
 - o Process was reviewed at periodical intervals to increase its effectiveness and efficiency

Identification of shortcomings

The auditor should identify:

- Incidents that were that were not identified by the incident management process
- Identification of the problems as per the defined by the process but its resolution was not as per the defined process
- Variances between the actual implementation for incident management and the defined process
- Dissatisfaction of the users
- Lack of communication of incidents and resolution
- Lack of integration of incident management with the configuration management

Answer: [b] Incidents that are not resolved as per the defined process

Module:4

Reference No:M4218

Question: A preliminary understanding of the operation management procedure can be obtained, by ensuring documentation of:

- [a] Operator instructions
- [b] Job scheduling
- [c] Performance standards
- [d] All of the above

Module 4 – Audit working guideline

Operations Management- 1

Table of applicability

For IT task	Control objectives	
Operation Management	Management controls	Operational controls
	1. Operational procedures 2. Operations manual 3. Job scheduling 4. Continuity of operations 5. Log maintenance 6. Security over forms and other devices 7. Remote network	Not applicable for this activity

Audit Process

The audit process has been covered in two parts. This article is the first part, and deals with a preliminary understanding and analysis of the process.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. IT management 2. Operations management 3. IT users 4. Third party service providers 5. Hardware and software contractors.	1. Policies and procedures of the organisation with respect to ▪ IT procedures ▪ Position and role of IT in the organisational goals and objectives 2. IT policies and procedures with respect to ▪ Roles of operation ▪ Operator instructions ▪ Performance standards ▪ Job scheduling ▪ Job rotation ▪ Service level agreements ▪ Continuity planning ▪ Remote operations 3. General operational instructions for ▪ Start up and shut down ▪ Emergency and abnormal situational procedures ▪ Problem management and escalation procedures ▪ Physical and logical security ▪ Service level agreements ▪ Log maintenance 4. Sample instructions for applications with regard to ▪ Schedules ▪ Input, processing time ▪ Handling error messages ▪ Problem escalation instructions ▪ Abnormal ending instructions· Restarting· Off-site file maintenance

Preliminary analysis

The next step is to analyse the effectiveness of the control measures adopted, and their reliability. This can be done by ensuring that the following exist

1. Control measures that ensure completion of all processes, restarts, cold starts and recoveries

2. Sufficient procedural instructions to regulate initial programme load and shut down the applications/systems
3. Statistics that establish the successful compliance with all requirements.
4. Principles of segregation of duties between the functions of testing, development of programmes/ maintenance of production libraries and change control procedures for programme movement
5. A system for collecting the Performance statistics for the following activities. (The list given below is only an indicative and not a comprehensive list)
 - Utilisation of hardware and peripherals capacity
 - Hardware and peripheral capacity
 - Performance of hardware and peripherals
 - Performance and utilisation of memory
 - Performance and utilisation of telecommunication media and other equipment.
6. Statistics to collect information regarding the extent to which the applications match the performance levels, internal standards and commitments of service level agreements
7. Logs for periodic maintenance and review
8. Proof that all equipments are being maintained appropriately
9. Evidence that jobs are being rotated especially for operators etc.

The next article focuses on the second part - the test of controls and substantive testing.

Answer: [d] All of the above

Module:4

Reference No:M4219

Question: Which one of the following activities should be performed for auditing operations management to substantiate the control procedures?

- [a] Review of sample IT manuals
- [b] Examination of start-up procedures
- [c] Examination of schedule of processing
- [d] All of the above

Module 4 - Audit working guideline

Operations Management- 2

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Operation Management	1. Operational procedures 2. Operations manual 3. Job scheduling 4. Continuity of operations 5. Log maintenance 6. Security over forms and other	Not applicable for this activity

	devices 7. Remote network	

Audit Process

The audit process has been covered in two parts. The first part covered a preliminary understanding and analysis of the process. This article is the second part, and focuses on the test of controls and substantive testing.

Tests of controls

A clear picture of the functioning of controls can be gained by:

- Obtaining evidence
- Reviewing the deliverables

Tests: Before taking a stand on the functioning of IT tasks in the organisation, the auditor should check whether the employees have been informed and made aware of the operations instructions regarding

1. The operational responsibilities of individual staff members.
2. Performance standards with regard to vendor performance, organisational policies and procedures and service level agreements.
3. Emergency procedures with details of start and shut down procedures.
4. Log requirements and review by management
5. Problem escalation instructions
6. Shift change procedures and details and between shift responsibilities
7. Communication between remote facilities and central processing facilities

Tests should be performed to ensure that control measures identified in the preliminary analysis are functioning as desired.

Substantive testing

This step is undertaken to substantiate the auditor's viewpoint that control objectives are either not being met, or do not exist. The shortcomings in controls and its consequences also should be documented. He should:

1. Compare operational performance statistics to comparative benchmarks from similar organisation and industries, internal, organisational standards and best practices.
2. Review samples of IT manuals to ascertain whether they meet the organisational policies and procedures
3. Examine the start- up and shut down procedure documentation and instances to ascertain if they are tested and updated on a regular basis.
4. Examine the schedule of processing to determine the adequacy and ensure whether the schedule is being adhered to.

Identifying shortcomings

The auditor should identify:

- Selected users and ascertain the adequacy of the normal ongoing procedures/activities and service level agreements
- A sample of abnormal ends and determine ways to resolve problems that caused the abnormal ends
- Sample logs and review them for accuracy, performance trends and review of management for the problem resolution process and evaluation of the problem escalation procedures
- Users for determining the commitment to the service level agreements.
- Whether preventive maintenance procedures were performed on all equipments as per the vendor requirements.

Answer: [d] All of the above

Module:4

Reference No:M4220

Question: FTP is more reliable than HTTP because

- [a] It uses separate channels for data transmission and flow control
- [b] It transfers data from the web server
- [c] It transfers data from the file server
- [d] It copies files to the user's hard disk in the destination specified by the user

Module 4 – A comparison between HTTP and FTP

Introduction

FTP (File Transfer Protocol) and HTTP (Hypertext Transfer Protocol) are used at the Application level of a network. Both of them use the protocols specified in the Internet layer of TCP/IP. The fundamental difference in both the protocols lies in the fact that FTP specifies protocols for *file transfer* while HTTP sets rules for exchanging files across a network. The differences between the two, merits and demerits of each of these protocols are discussed below:

- **Protocol Definition:** File Transfer Protocol establishes a set of rules that govern the transmission of files (downloading or uploading) from the network (i.e. from a computer that acts as a server in the Internet) to individual workstations (i.e. to the users' machines). While on the other hand, HTTP lays the protocols for displaying files (E.g. image files, text files and the like) to the user.
- **Working:** When FTP appears in the URL, it can be inferred that the user is getting connected to a *File Server*. A *file server* is a dedicated computer that stores files (or programs) that can be downloaded by the user (and does no other function). When the URL displays HTTP, it indicates that the user is getting connected to the *Web Server*. A *web server* is a program that uses the client/server model and sends the files for displaying a web page on the user's browser. It is in charge of handling user requests for viewing web pages (that include the content to be displayed, the format in which it is displayed and so on). In other words, a web server handles the file server and controls the functions of the file server (i.e. a web server handles user requests in a much more broader sense). Some examples of web servers include Microsoft's IIS and Novell's Netware.
- Prior to any file transfer (using FTP), the user has to log on to the file server. While, no login is required for an HTTP.
- **Mode of transfer:** HTTP is unidirectional, while FTP is bi-directional. The user's workstation acts as an HTTP client and sends request to the web browser for viewing a web page. The server sends the response and the page is transferred to the user's browser. While in case of FTP, the file requested by the client

(the user) is copied to the hard disk of the user's workstation. In other words, files, programs, or images are in fact downloaded (i.e. transferred from web server to the user's terminal or uploaded (i.e. transferred from the user's machine to the web server). Thus, it can be observed that there is a two-way communication between (i.e. to and fro the web server and the user's terminal).

- HTTP files (usually the web pages) aren't stored (copied) permanently in the hard disk of the user's terminal (unless and otherwise exclusively saved by the user). But in FTP, for every file transferred it is saved in the user's hard disk, in the destination specified by the user.
- *Reliability*: FTP is a better protocol in terms of reliability and performance. HTTP does not check for errors in transmission or for loss of data packets during the transmission. In other words, HTTP doesn't guarantee accurate transmission of data, which is likely to cause serious problem in transferring large files. On the contrary, an FTP uses two channels for transmission one for data and the other for flow control. This makes the data transmission infallible.

Answer: [a] It uses separate channels for data transmission and flow control

Module:4

Reference No:M4221

Question: Which of the following is not a field present in SDLC (Synchronous Data Link Control) data frame?

- [a] Flag
- [b] Data field
- [c] FCS (Frame Check Sequence) field
- [d] Link access Control field

Module 4 – Synchronous Data Link Control

Introduction: Synchronous Datalink Control Protocol (SDLC) is a protocol defined for Layer-2 (the data link layer) of the OSI reference model. One of its popular derivatives is the HDLC (High level Datalink Control protocol). IBM developed SDLC for implementing it in the mainframe networks. SDLC works in only the Normal Response mode (unlike the HDLC which works in three modes; in all other respects SDLC is similar to HDLC), i.e. it recognises only primary station -secondary station network model. In fact, in a mainframes network, the host machine acts as the primary station and all the work stations connected to it act as secondary stations. Hence, the SDLC was designed specifically for functioning in a primary station -secondary station model. Other derivatives of SDLC include LAPB (Link Access Procedure) and LAPB (Link access Procedure, Balanced).

SDLC Configurations:

SDLC can be employed in point-to-point and multipoint links with half / full-duplex operations. It is implemented in two kinds of stations namely- *primary station* and *secondary station*.

Primary stations have full control on the secondary stations in data transmission, data reception, error recovery and flow control. Secondary stations simply operate under the commands of the primary station. SDLC specifies four configurations using primary and secondary stations:

- *Point-to-point*: This type of configuration employs only one primary and one secondary station, the secondary station responding to the requests of the primary station. A client server model can be thought of as a point-to-point configuration.
- *Multipoint*: A multipoint configuration is implemented with one primary station and many secondary stations.
- *Loop*: In a loop, the primary station is connected to the first and the last secondary stations. The secondary stations in-between are linked to one another and they respond through one another as and

when the stations connected directly to the primary station respond to the requests (of the primary station).

- *Hub go-ahead:* A hub go-ahead configuration consists of an inbound and an outbound channel. The primary station transmits using the outbound channel, while the secondary stations use inbound channel.

SDLC frame:

A typical SDLC data frame is conceptually organised as follows:

FLAG	ADDRESS	CONTROL	INFORMATION / DATA	FCS	FLAG

- *Flag:* Every data frame begins and terminates with a flag. Flag keeps a link/ session alive. During transmission a station always checks for a flag so as to check whether the communication session is active or not. A flag starts and ends the error checking procedure during transmission.
- *Address:* The address field identifies the station (whether primary or secondary) that sends a data frame. In fact, an SDLC frame stores the address of the secondary station and the source / the destination (as the case may be) is taken to be the primary station. So it doesn't specifically mention the address of a primary station.
- *Control:* The control field specifies the mode of communication process and its control. It includes commands and functions to handle flow control and error detection/recovery. The three different formats used by the control field are-
 - Information transfer format (performs error control and bit flow control operations)
 - Supervisory format (used for acknowledging the receipt of an information)
 - Unnumbered format (used for connection and disconnection of communication session)
- *Information/Data:* The data field as the name suggests, contains the actual information to be transmitted across a communication channel.
- *FCS (Frame Check Sequence) field:* This is the last but one field and is succeeded by the flag. It is used for error detection (using Cyclic Redundancy Check-CRC). If the value calculated from CRC corresponds exactly to the actual value sent, then the transmission is declared to be an error-free transmission.

Answer: [d] Link access Control field

Module:4

Reference No:M4222

Question: The basic function of the network layer is

- [a] Selection of paths or routers for data transfer
- [b] Breaking the Network in to subnets
- [c] Determining the IP
- [d] To take in user input and transfer to the transport layer

Module 4 - The Network Layer-the control of subnet operations

An Overview: The Network Layer (the third layer of the IOS-OSI reference model) connects the Transport Layer and the Datalink Layer. This is where the decisions regarding choice of path is made. The Network layer is responsible for managing the operations of the subnet. A **subnet** is a part of the complete network that shares the same address component. To make data transfer secure and efficient a network is segmented into subnets. Usually subnet connects all the machines that are located within a short radius say for instance, in one building or a campus. The Internet is a collection of these kinds of subnets. The Network layer

administers the communication path through which the data packet has to be routed. This involves all the processes related to selection and routing of messages before they are sent to their respective destinations.

Why a Network Layer? The Network Layer is primarily involved in decision making, for selecting the route and paths to be taken to transfer the data, in the absence of which the network cannot synchronise the sending and receiving pace. This decision is based on communication rates, bandwidth, parity rates and the continuity of the connection.

The Network Layer keeps a tab on the addresses of the workstations in the vicinity. The Network Layer then attaches the correct address to the datagram / packet and selects the route for sending them. It also determines the beginning of each communication session.

The Network Layer also manages the number of packets that reach a particular destination at one particular time in order to check overcrowding of the path due to uncontrolled flow of packets.

The Network Layer maintains this check by using the software that counts the number of packets sent by each source and the ones that are actually received. Thus any mismatch in the number of packets at the sender's or at the receiver's end would show the number of packets lost on the way.

During the transit, the packets have to pass through various networks and hence heterogeneous addressing schemes and standards for packet sizes. It is the task of the Network Layer to resolve any problems arising therein.

Network Layer services and protocols:

The two types of Network Layer services include *Connectionless Network Service (CLNS)* and the *Connection-Oriented Network Service (CONS)*.

IP is a Network Layer Protocol that defines exactly how data is transmitted from one computer to the other. Every computer in the network is given a unique address known as the IP address. When a message is sent from one computer to the other in the Internet, it gets divided into smaller packets each bearing the IP address. It is with this address, the packets get transmitted across the network. Other protocols include IPX- a Novell Protocol and DDP (a Datagram Delivery Protocol)- an Apple Protocol

Answer: [a] Selection of paths or routers for data transfer

The Network Layer takes decision regarding which paths or routers are to be selected and which not. IP or Internet Protocol is just one of the protocols in the Network Layer.

Module:4

Reference No:M4223

Question: Which of the following is not a function of the Transport Layer?

- [a] To interact with the user
- [b] Maintenance of data integrity
- [c] Connection and disconnection of intermediate virtual circuits
- [d] Breaking the Session Layer datagrams

Module 4 – The Transport Layer-“peer to peer” communication

The chief purpose of a layered architecture (like the one specified in OSI) is to simplify communication between two remote terminals regardless of the mutual compatibility in a complex network frame. In support of this, the fourth layer of the ISO-OSI reference model, i.e. the Transport Layer's primary function is to establish a “*peer to peer*” communication. A “*peer to peer*” communication is the transfer of data between two similar protocols implemented in equivalent layers of two workstations. In peer-to-peer communication, the party at each end has the same abilities and both can set up the connection. Usually a peer-to-peer communication is established by granting both, the client and the server capacities. Thus, the Transport

Layer offers transparent data transfer between the two end-users with the help of the services from the Network Layer below.

Functions: The chief functions of the Transport Layer involve segmenting and assembling the applications from the upper layers, transferring these segments from one end to the other, setting up and managing the procedures at both the network ends and providing recovery from errors. It offers dependability of data transfer and integrity. The processes involved in accomplishing these comprise the following:

- Data multiplexing from the applications received from upper layers
- Maintenance of data integrity using flow-control techniques
- Connecting and disconnecting virtual circuits that might have been set up during the communication process
- Data encapsulation (covering up the irrelevant data from the upper layers)
- Segmenting the Session Layer datagrams

The working: The Transport Layer's chief function i.e. end-to-end communication is accomplished by using two protocols -

- The Transmission Control Protocol (TCP)
- The User Datagram Protocol (UDP)

The Transport Layer serves for both connection-oriented and connectionless transmission modes.

In case of a connection-mode, the information at the recipient reaches in form of small segments / packets (instead of the complete file as a whole). A **packet** / datagram refers to a single part of data that is transferred from one end to the other in a network. Whenever a file is sent across a network, the Transport Layer breaks it into a number of segments which are passed on to different routers. These are finally collected and assembled back into its original form by the Transport Layer at the receiving end. This task of the breaking up of information into packets and then reassembling them is governed by the TCP (Transport Control Protocol). The TCP is a connection-oriented protocol, i.e. it will ensure despatch and receipt of the data packets during the life of the connection after the connection is set up.

On the other hand the UDP (User Datagram Protocol) is a connection-less protocol. It uses one-to-many transmissions and it does not guarantee a reliable data transfer mechanism. It obtains the message from the application and adds the addresses of the source and the destination. This is passed on to the Network Layer, which is encapsulated in to an IP Datagram for delivering it to the destination. There is no acknowledgment for the receipt of the message at the destination end, unlike the TCP.

Answer: [a] To interact with the user

Module:4

Reference No:M4224

Question: Which of the following is not an operation mode specified for HDLC (High level Data Link Control)?

- [a] Normal response mode
- [b] Unbalanced mode
- [c] Asynchronous response mode
- [d] Asynchronous balanced mode

Module 4 - HDLC- High level Data Link Control

Introduction

High level Data Link Control (HDLC) is a data link protocol that functions in layer-2 (i.e. the datalink layer) of the OSI reference model. HDLC is chiefly concerned with flow control. The popularity of HDLC arises from

the fact that it supports both half-duplex and full-duplex data communication in all kinds of channels (namely switched, non-switched point-to-point and multi-point networks). HDLC allows synchronous data transmission and uses distinct bit patterns for controlling the data and representing them, which reduces errors. HDLC organises data in to separate units known as data frames. An HDLC frame depends on the physical layer for clocking and synchronising the bits transmitted and received at two ends of a communication channel.

HDLC Stations

Three stations have been specified by HDLC

- **Primary Station:** A primary station is used as a controlling station in a communication channel, i.e. a primary station controls all other stations (the secondary stations) in a link. A primary station also manages data flow in a communication channel and is responsible for error recovery in the datalink layer.
- **Secondary Station:** A secondary station is under the control of a primary station. It doesn't have the direct power to control a link. It gets invoked only when the primary station request for a data frame. In other words a secondary station only responds to the requests of a primary station.
- **Combined Station:** An arrangement of a primary station and a secondary station is known as a combined station. A combined station is capable of transmitting and receiving data on its own (without being under an external control).

HDLC Configurations

Three types of configurations specified by HDLC are:

- **Unbalanced Configuration:** An unbalanced configuration is composed of a primary station and one or more secondary stations. It is known as an unbalanced station since a single station (i.e. the primary station) controls more than one station (secondary stations). An unbalanced configuration uses either full/half duplex operation or point-to-point /multi-point networks.

The following figure illustrates an unbalanced configuration:

Balanced configuration: An HDLC link composed of two or more combined stations is known as a balanced configuration. Each of these combined stations in a balanced configuration can control both sending and receiving data without depending on an external control, which is why such type of configuration is known as a balanced configuration. A balanced configuration can be used for half / full duplex operation or point-to-point networks.

The following diagram illustrates a balanced configuration:

Symmetrical station: A symmetric station comprises two independent point-to-point unbalanced station configurations. In this type of configuration each station is logically distinguished as a primary and secondary station (i.e. no separate primary or secondary station exists, every station acts both as a primary and a secondary station). This type of configuration is not popular and is less in use.

HDLC Operation modes

Three operation modes specified for HDLC are:

- **Normal Response Mode (NRM):** As the name suggests this mode is the usual mode of data transfer between a primary and a secondary station, in which the secondary station is fully controlled by the primary station. This is to say that in a normal response mode, a secondary station transmits if and only if the primary station gives it the permission to do so. This mode is employed in unbalanced configurations of multi-point links where the primary station controls the link. The limitation of this mode is that with every data frame the secondary station has to send an acknowledgement frame too

(so as to indicate the receipt of permission from the primary station). This increases the number of data frames in a link, thereby jamming the link.

- ***Asynchronous Response Mode (ARM)***: In ARM, the secondary station does not require an explicit permission from the primary station, i.e. a secondary station need not send acknowledgment frames along with the information frames. This reduces the burden on a link and hence is used in point-to-point links. Error recovery, connection and disconnection of a session still remain the responsibility of the primary station.
- ***Asynchronous Balanced Mode (ABM)***: In ABM, none of the stations require permission for any kind of data transfer. This mode is used in combined station configurations where each station is independent in transmitting and receiving data.

Answer: [b] Unbalanced mode

Module:4

Reference No:M4226

Question: Location of network controllers, cables and videos are evaluated to ensure:

- [a] Dial-up security
- [b] Physical security
- [c] Performance integrity
- [d] Logical security

Module 4 - Internal Control Assessment for Networking - I

This article highlights the use of Networking audit and the Internal Control Questionnaire (ICQ) to review preliminary data.

Audit of Networking

Before undertaking networking audit an auditor should gather and understand all the necessary information. This includes network diagram, hardware configuration diagram showing servers, network topology, workstations, bridges, repeaters, protocol converters, details of hardware and software inventory and communications gear.

An auditor must examine the standards, policies and procedures of the organisation, details of vendors and his representatives and the contingency plans in place. He should also obtain and evaluate the sample reports for monitoring firewall and security violation, details of service level agreements and network services.

Internal Control Questionnaire

The ultimate objective of the networking audit is network security. Network security may be affected by faults, negligence on the part of third parties or through misrouted messages. Therefore, an auditor must suggest the preventive and detective controls. The network administrator or the area manager must fill the IQC. The following must be evaluated to review the preliminary data.

1. ***General***: Check the availability of documentation procedures for network usage, which detail data network equipment, protocols and gateways to various networks. Details of network vendors, their liability and responsibility also have to be checked. Network diagram, access policy and access codes for external parties must be evaluated.

2. *Performance integrity*: Ensure the existence of specific terminal within the online system to monitor the activity. Examine whether the network personnel have reviewed the new applications to assess their effect on the systems in use. Performance of the hardware against the vendor specifications and services provided by vendors need to be evaluated. Check whether corrective actions have been taken for network hardware failures.
3. *Dial-up security*: Check the authorised users' list and evaluate the confidentiality provisions for telephone numbers. Check the frequency of changing the dial-up numbers. Telephone numbers must be taken out of the modems to circumvent access to the dial-in numbers. Ensure that the access to dial up facilities is authorised. Examine whether the users are disconnected in case of improper log-off.
4. *Physical security*: Ensure the security of physical environment by evaluating the location of network controllers, cables and videos etc. Check the availability and access to test equipment.
5. *Logical security*: The passwords, user codes and authorisation of access must be identified. Ensure that only authorised personnel have access to network software and storage buffers. Further, there must be proper controls over processing of sensitive information and the same must be routed to the authorised printers.
6. *Employee Knowledge*: Employee awareness about the policies and procedures of corporate networking must be evaluated and their efficiency in using the software and hardware must be tested. Employees dealing with networks must be well aware of the security aspects, control methods and the subsequent vulnerabilities. Also review the existence of disciplinary actions for violation of security guidelines.

The next article will discuss ICQ for specific areas of Networking.

Answer: [b] Physical security

Module:4

Reference No:M4228

Question: For ensuring accurate selection of polariser, the receiver is provided with

- [a] The exact polariser used by the sender
- [b] The key
- [c] The polarisation scheme used by the sender
- [d] An intrusion detector

Module 4 - Quantum Cryptography

The concept

Quantum physics or the quantum theory forms the basic building blocks of *quantum cryptography*. Unlike the traditional approach to cryptography that applies mathematical concepts for encryption and decryption of data, the working of quantum cryptography is based on the *Heisenberg's principle of uncertainty*. Quantum cryptography makes use of the inherent properties of individual particles of light (photon) in building a cryptosystem. This is because, measuring a quantum state without disturbing it is not possible. Thus, any kind of eavesdropping would create disturbance in the communication channel and hence can be detected. This way, quantum cryptography provides more security as compared to a traditional cryptosystem.

The working principle

Quantum cryptography uses the smallest existing particle photon for transmitting data in encrypted or decrypted form. The sender initiates a communication by sending the key (i.e. the mode of encryption) to the receiver. A key is sent as a stream of photons using a distinct scheme of orientation for each photo known as *polarisation*. The two basic types of polarisation schemes are rectilinear (up/down & left/right) and diagonal

(upleft/rightdown & upright/leftdown). A filter that allows only photons with a specific polarisation to pass through (known as a *polariser*) is added in the communication channel.

An illustration:

Let us suppose, that two people wish to communicate and the message is sent in one of the polarisations. On receiving the photon key, the receiver determines the polariser chosen for each photon (by the sender while sending the key). But the receiver is liable to make a wrong selection. Hence, along with the key, the receiver is provided with the information about the polarisation scheme used for sending the key. Polarisation scheme here refers to rectilinear or diagonal, without explicit mention of left/right, up/down, upleft/rightdown and the like. Thus, the wrong selections made by the receiver are discarded. This way half of the photon bits arrive intact to the receiver. Hence, for transmitting n bits of information $2n$ bits have to be transmitted in the key.

Safeguard against eavesdropping

Eavesdropping in the communication process can be detected and avoided in two ways as discussed below:

- Firstly, if the voyeur taps the message transmitted through the communication link, he would make the same errors in determining the correct polariser used for encrypting each photon. Moreover, the eavesdropper would be devoid of any information about the polarisation scheme employed for the photons (unlike the authenticated receiver). Thus, interpretation of the key will become totally useless. This way, quantum cryptography averts the problem of eavesdropping.
- In addition to this, quantum cryptography offers an inherent security measure the intrusion detection. Divulging any sort of snooping in the transmission is known as intrusion detection. If an eavesdropper overhears the information (key), and tries transforming it, then the incongruity between the receivers' transmission and the eavesdroppers' transmission is revealed (as according to Heisenberg's uncertainty principle no change in a photon polarisation can go unnoticed). Thus, quantum cryptography, due to the innate particle properties proves to be an infallible cryptosystem.

Practical implementation of Quantum Cryptography

Fibre optic cables are used for photon transmission in real transmissions. These cables have far-fetched pure optic properties that ensure error-free transmission. Nevertheless implementation of quantum cryptography over large distances still needs to be researched.

Answer: [b] polarisation scheme used by the sender

Explanation: Polarisation scheme i.e. rectilinear or diagonal should not be confused with the different kinds of polarizers like left/right, up/down. Upright/ leftdown or upleft/ rightdown.

Module:4

Reference No:M4229

Question: ECC (Elliptic Curve Cryptography) is an ideal cryptosystem for mobile applications because

- [a] It integrates elliptic curve theory with encryption
- [b] It provides an easy mechanism for key generation using a simple ellipse equation
- [c] The keys are of shorter bit-lengths, as compared to the ones generated by traditional schemes
- [d] It is a less expensive method of encryption

Module 4 – Elliptic Curve Cryptography (ECC)

Definition

Elliptical curve cryptography is a form of cryptosystem that employs public key encryption by applying elliptic curve theory. Elliptic curve theory allows the user to expand the key using detailed mathematical descriptions or formulae. ECC is an eye-catching public key cryptosystem since many small keys can be generated (resulting in faster computations) using the elliptic curve equation.

Elliptic curve equation: Simple bi-variant (having two variables say, x and y) functions that generate ellipses are referred to as elliptic curves. These are produced by joining all the points generated by the equation of the ellipse (or the elliptic function). Elliptic curve cryptography is just one of the implementations of the elliptic curve theory.

The properties of an elliptic curve are employed for generating the keys in ECC. This proves to be a better method as compared to the traditional approach to key generation using exponentiation (product) or discrete logarithm (inverse of exponentiation) of prime numbers. Exponentiation is less complicated as compared to discrete logarithm, but is an expensive option. Since, the conception of elliptic curve theory dates back to many years, it can be used with almost all the public key encryptions without disrupting the existing methods of encryption or decryption.

Implementing ECC

As explained above, properties of an ellipse equation basically govern elliptic curve cryptography. An equation using a set of values (used by the two members involved in the communication) is generated. Subsequent points on the curve are derived from the points of intersection with the coordinate axes (the X and Y axis). This way, even by knowing the curve, a third person (an eavesdropper) cannot intercept the data transmitted between the two users, as any alterations in the curve will only result in a new curve, not the original values used by the two communicators. This is because elliptic curves have a property of being generated in a simple fashion but to obtain the values back from the equation is as difficult.

In gist, ECC integrates basic number theory, polynomial algebra, and elliptic curve functions for generating code for key.

Merits of ECC

- Typically, ECC can generate a 164-bit key, which is as large as 1024-bit for a traditional approach, there providing security even under low computer power and battery usage. Hence, ECC is an ideal encryption system for mobile applications (where the devices are compact in terms of size and power resource usage).
- Since ECC is based on properties of a particular equation of ellipse, any alteration (like say for example, multiplication, exponentiation and the like) will merely generate another curve; the original curve will not be revealed, even if the result is known. Thus, it provides a foolproof security measure for data transmission systems.
- ECC is based on the properties of ellipses, which is a well-conceived and researched field in mathematics. This makes the key generation method uncomplicated and easily handled cryptosystem; but at the same time the inherent properties of an ellipse make ECC an unbreakable encryption system.

Answer: [c] The keys with shorter bit-lengths, as compared to the ones generated by traditional schemes

Explanation: Since mobile applications are run in smaller / compact devices like cellular phones and pagers keys of shorter bit lengths are ideal for executing them.

Question: Security checks are more at the network level in order to

- [a] Reduce complexities for the users and makes them more receptive to the security checks
- [b] Manage and handle passwords more efficiently
- [c] Avoid password loss
- [d] Prevent illegitimate users from logging in

Module 4 - Security Issues in Client/Server architecture- I

An overview of the client/server architecture

In client/server architecture, the tasks and roles of a system are divided between two workstations- one the user's PC (or the client PC) and the Database Server (workstation that is linked to all other clients in the network and processes requests from them). The three chief building blocks of client/server architecture are the client, the server and the interface between them to connect the client and the server. In fact all the functions such as data management and business rules are shared between the two ends.

Usually implementation of security in a client/server model is neglected, since the profits on the costs are not returned directly. Moreover, the buyers are often unaware of the intricate security issues that threaten a system.

Susceptibility of a client/server system

The distribution of client/server architecture over an extensive area makes it vulnerable. It is exposed to system damages due to viruses, misuses, physical tampering and the like, than a centralised computer system

The chief security issues in client/server architecture include:

- Security at the client end
- User awareness about security measures
- Security of network interface between client and the server
- Server security

Security issues at the client side:

The chief loopholes in the client side are:

- *At the physical level:* Clients from various sites/locations connect to the servers for accessing data. Physical security issues include implementation of disk drive locks, diskless workstations and refraining from installing unauthenticated software.
- *At the OS (Operating System) level:* The operating system of a workstation poses a greater risk than the physical level since a corrupt data could be easily passed on to the entire network. Mostly, the OS is not capable of distinguishing an intruder from an authorised user. It simply takes for granted that the person who switches on the machine is its owner and offers no resistance to unauthorised access of all the files (including the configuration files) in the system. Hence, selection of a suitable operating system (ones which offer facilities like user authentication and restricted access) plays an important role in securing the connection at the OS level.

User awareness in security measures

In order to ensure an infallible security system it is essential to block all loopholes at the user level. Thus, the security concern at the user level includes:

- Making the user aware of the risks that the system faces if they fail to comply with the security measures imposed by the company

- Thwarting illegitimate access to distributed systems (implementing client/server architecture)
- Handling and managing passwords that involves preventing passwords from getting lost, employing schemes to recover lost passwords and ensuring that proper passwords (those that cannot be guessed easily) are chosen by the users
- Incorporating as many security checks as possible at the network level and limiting the complexities of security measures at the user level so that users grow more receptive to these procedures and abide by them dedicatedly.

The next part of the article discusses the security issues at the server side and at the network level (or the interface between client and the server).

Answer: [a] Reduce complexities for the users and make them more receptive to the security checks

Explanation: Since more number of security checks at the user end makes the work of user cumbersome and makes him prone to committing errors in logging in, it is wiser to incorporate as many security measures as possible at the network level as machines (i.e. the network interface) are believed to be less fallible.

Module:4

Reference No:M4231

Question: Which of the following is not a key security issue pertaining to the network level?

- [a] User identification and authentication
- [b] Establishing conditional access to data
- [c] Implementation of audit services
- [d] Maintaining data privacy and integrity

Module 4 – Security Issues in Client/Server architecture- II

Client/server security takes into consideration user's logical and physical security needs from both the sides- server and the client. Thus, the chief security issues concerning client/server architecture can be segregated under the following levels:

- Security at the client end
- User awareness about security measures
- Security of network interface between client and the server
- Server security

Security issues pertaining to the client side and user's involvement in implementing them is discussed in the first part of this article.

Security issues in the network (interface between the client and the server)

The interface between the client and the server is often prone to attacks from intruders. The chief security issues at the network level can be enumerated as follows:

- *Eavesdropping:* Often vital information packets are hacked from an unprotected connection. These data packets might contain key information about the company like passwords, intricate details of the company, loopholes that could be exploited to break the system, and the like.
- *Loopholes in encryptions:* Encryption solves the problem of unauthorised intrusion. The only setback in this approach is that some network OS does not encrypt the information till the user is authenticated (i.e. the user is able to decrypt the message). To counter the problem, these systems adopt re-usable

passwords for authorising the users. This facilitates an intruder to obtain the login and password by closely monitoring the network. The problem of hacking is worsened by employing re-usable passwords since these passwords allow access to all the servers in the network through a single login, thereby making the job of an eavesdropper even more easier in keeping watch on the network activities.

Thus the key issues of security at the network level are:

- Implementation of proper identification and authorisation processes
- Employing reliable discretion control on the part of the network to give conditional access to data
- Implementing audit services

Security issues at the Server end

Usually servers face security threats due to the following reasons:

- *Negligence at server centre:* Usually servers are kept in an open unprotected environment, making it impossible to lock them. This type of arrangements lack physical security implemented by locking the equipment and cabling into place. In fact only authorised personnel should supervise the servers. The chief security issues at this level include protection of servers through filters, locking facilities for machines cables and the like.
- *Lack of proper power supply:* Often lack of uninterrupted power supply for the servers lead to loss of data, thereby leading to disruption of functioning of the system. Hence, servers should be equipped with unfailing power supply and back up facility. A proper back up facility allows the server to shut down properly during power failures thereby protecting the data.
- *Virus threats:* Unplanned and lack of proper monitoring in system upgrades leads to installation of corrupted software. Hence, PC-based servers should have an active anti-virus programs enabled.
- *Data privacy:* At times, intruders somehow make it to the servers breaking all security checks at the client and the network level. In such circumstances, it becomes the server's responsibility to check access to vital data. Thus, to ensure privacy of data the server should implement security checks by incorporating data encryption and passwords. Data integrity at the server level is maintained by restricting data modification only to authorised users. This will check data manipulation by intruders.

Answer: [d] Maintaining data privacy and integrity

Explanation: Data privacy and integrity is managed and handled by the server. Checking for unauthenticated data modifications or manipulations is the server's responsibility.

Module:4

Reference No:M4234

Question: Which of the following is not true of application gateway?

- [a] Traffic control is application specific in the case of an application gateway
- [b] An application gateway allows a direct connection between the client and the server
- [c] An application gateway has access to application data
- [d] An application gateway software is capable of extracting user specific information

Module 4 - Stateful inspection firewalls vs. application gateways

An overview on firewall classification

Firewalls are classified on the basis of how they handle the network traffic. The two major types of firewalls are packet filter firewalls and application/proxy firewalls or application gateways. These firewalls differ in the way they block or allow data packets pass through the network. Packet filter firewalls are again classified

into router packet filter firewalls and stateful inspection firewalls.

Difference in working principle and the technology involved

In packet filter firewalls, the data packets are allowed after checking the TCP address on the header of the data packets. Also they are blocked if the address differs from that mentioned in the acceptable format (i.e. the standard format configured at the time of setting up the firewall). Both route packet firewall and stateful inspection filter firewalls control network traffic on the basis of the IP address (the address of the source and the destination mentioned in the header of the data packet). They differ in that a stateful inspection firewall (as the name suggests) also peruses contents of a data packet apart from checking the IP address.

Application gateways or proxies break the connection between a client and the server and simulate a client / server program that behaves as a client and a server at the client end and the server end respectively. In fact the proxy checks for any discrepancies in the data packets and thereby blocks with its own discretion without letting the actual client and the server come in contact with each other.

This article discusses the differences between the working of packet filter firewalls and application gateways and their features.

A Comparative study of firewall types

- *Message blocking scheme employed:* Packet filters allows all those messages whose IP addresses (specified in the header) conform to the acceptable address format specified while configuring the firewall rules, thereby blocking only those having improper address formats. An application gateway, on the other hand, has access to the application data of the data packet and discards any unidentifiable data packet, i.e. applications that do not conform to approve Internet application protocols. Thus, application gateways are more reliable than the packet filters.
- *User identification scheme:* Since application gateway software has access to application data of the data packets, it is capable of extracting user specific information like user names, login IDs etc. and employing them in controlling the data packet transfer between two communication points. It can for instance, block a message from say messages sent from a particular user name. This reduces the complexities involved in employing different levels of security checks at the login level. Packet filters do not support user authentication. Even if they do, they do so by specially incorporating a scheme using additional services and protocols. Thus the whole process is cumbersome.
- *Traffic control:* Packet filter traffic controls are not application specific, like network traffic control schemes. Application gateways can enforce restrictions on the execution of certain application programs like downloading files with specific content from a site.
- *Portability:* Application gateways are portable and extensible allowing for further upgrades, unlike packet filter firewalls.

Answer: [b] An application gateway allows a direct connection between the client and the server

Module:4

Reference No:M4235

Question: Session hijacking refers to

- [a] Specifying the exact routing of the datagram in a particular communication session
- [b] Forceful unauthenticated takeover of an active communication session
- [c] A hit and trial method for hacking the password for user authentication
- [d] Strategic algorithm for revealing the password to gain unauthorised access to a private network

Module 4 - Session Hijacking

Session hijacking, also referred to as TCP session hijacking is one of the most widespread methods of obtaining unauthorised access to private web servers. In session hijacking, an unauthorised user takes over the TCP session between two workstations and eventually gains complete control over the computer itself. The user intrudes a web application session by *brute force cracking* also known as reverse-engineered authentication while the genuine user is still logged into the application. A brute force cracking refers to hacking the passwords for user authentication through a hit and trial method. The user employs extensive search for the correct password instead of using strategic algorithms for decoding the password. Once the password is hacked, the system is eventually brought under the control of the intruder. Gaining forceful control over a communication session after obtaining the password and acquiring authentication is called *session hijacking*.

Different schemes employed for session hijacking

Some of the popular ways in which a session can be hijacked are:

- **Using source-routed IP packets:** Source routing is a technique through which a sender can mention the data transmission path through which the data packet is to be sent across a network. In other words, instead of specifying all the possible routes for sending the message and leaving the routing decision on the router, the user specifies the exact route for sending the datagram. Since the exact path of routing is known it can gain access to a conversation between already logged-in users. This way the IP packets are intercepted before it reaches the destination and eventually, the session continues with the intruder as one of the communicating end points.
- **Blind hijacking:** This procedure is adopted when source routing is turned off. Blind hijacking is a hit and trial method, whereby the hacker tries guessing the users' responses. The hacker can thus communicate with one of the users asking them to set a common password for network access from elsewhere. However, the intruder cannot get replies from the logged in user. He simply guesses the responses, which is why it is known as a blind hijacking.
- **Inline sniffing:** In this process the intruder can remain in an intermediate point (between the two end points of communication) and closely observe the ongoing conversation between the two parties.

An illustration of potential vulnerability for session hijacking

At times, an intruder comes across active sessions between a genuine customer and a bank, which could become a potential exploit. The attacker may employ the brute force technique to acquire a sequential list of URLs for online transaction with the bank. When he discovers the exact URL he can paste it in his browser and sign a self-cheque. After signing the cheque, he can shop in an online shopping mall and spend the money before the genuine owner of the money becomes aware of the withdrawal.

Preventive measures

Session hijacking can be thwarted by the following measures:

- Successful active communication sessions to a particular IP address should be avoided as far as possible.
- Every user should be re-authenticated before crucial actions for e.g. online withdrawal, money transfer etc.

Answer: [b] Forceful unauthenticated takeover of an active communication session

Module:4

Reference No:M4236

Question: Network access point (NAP) refers to

- [a] A public communication network facility managed by various Internet service providers
- [b] A set of protocols governing the exchange of information between two endpoints
- [c] A particular route chosen by the protocol for routing the network traffic
- [d] A common network server that controls the routing decisions of all the ISPs

Module 4 – Network access point (NAP)

Definition

A network access point is a public communication network facility that is utilised by various Internet service providers (or ISPs) for establishing a peer-to-peer connection in the communication interface. In other words, network access points connect the Internet frameworks owned by different ISPs across the world. Various Internet service providers across the globe subscribe to these access points. Network access providers are primary building blocks in the internetworking. These access points make routing decisions i.e. they control the information traffic and determine how the traffic is to be routed.

Conception

The concept of network access points was first conceived in 1994. In fact these access points were new additions in the already existing Internet framework. The concept of implementing network access points emerged from the need to efficiently manage information traffic with the increase in network users. The most striking feature of network access point is that they make routing decisions without employing routers for routing the information traffic in the communication channel. Network access points act in layer two of the ISO-OSI reference model.

Working

Network access points do not employ routers for routing the network traffic. Instead network access protocols are attached to edge routers. These edge routers are governed by BGP (or Broad Gateway Protocol). *Broad Gateway Protocol* governs the exchange of the routing information between two gateway hosts in a communication channel. It usually governs networks with autonomous / independent systems. The routing table lists the name of all the known routes (along with its cost) and the best among them is chosen by the NAP. Thus, the network access points are capable of channelising the traffic without implementing routers.

An illustration of how NAPs work

Let us suppose that a user belonging to a particular area (controlled by a particular ISP) wishes to access a website (the traffic of which is controlled by another company). In such a case, the two ISPs have to be linked by a common interface. A network access point provides the interface. This network access point provides the switching facility and establishes a connection between the networks of the two different ISPs.

Why a network access point?

Instead of managing Internet connections privately, network access points provide the means of bringing the whole Internet framework (of the world) under one roof. The connections in the whole world will be managed by a cooperative effort from all the Internet service providers across the globe. The main advantage of using NAPs is reduction in cost. Since a major part of the communication mesh is managed by a cooperative effort from various ISPs, individual cost in establishing and maintaining a number of new connections, additional equipments, and overhead involved in administering the network is greatly reduced. Another advantage is that the efficiency of managing the network increases, as the load to be managed is reduced. NAPs connect endpoints of networks using various meshes. This increases the flexibility in networking.

Answer: [a] A public communication network facility managed by various Internet service providers

Module:4

Reference No:M4237

Question: Which of the following is the main objective in the audit programme of private key encryption?

- [a] To determine the existence of appropriate infrastructure and administration controls over selection and maintenance of private key encryption
- [b] To determine the accuracy of controls over key generation, distribution, maintenance and termination
- [c] To ensure that the key selection process considers the organisational security needs and the cost benefits of the tools
- [d] All the above

Module 4 – Audit programme for private key encryption -2

Definition

A Cryptographic technique based either on public keys or a private key is the primary security tool in e-commerce. Cryptography provides data security in public networks. The present article dwells on the audit programme and internal control questionnaire for private key encryption to evaluate the controls.

Objectives of audit programme

- To determine the existence of appropriate infrastructure and administration controls over selection and maintenance of private key encryption.
- To determine the accuracy of controls over key generation, distribution, maintenance and termination.
- To ensure that the key selection process considers the organisational security needs and the cost benefits of the tools.

Audit programme: Auditor has to perform the following to achieve the above objectives

Preliminary review: Before commencing the audit, an auditor should determine whether the corrections made in the previous audit are complete. Observations made in the previous audits must be cleared and E-commerce requirements must be clearly defined in the business objectives. The information architecture model must consider the business needs and e-commerce requirements. Auditor must confirm that the data is identified as an asset. They must examine the efficiency, integrity, reliability, availability and confidentiality of the information. Also they must check whether the need for encryption and acceptable risk levels are identified.

Ensure that the present hardware infrastructure is in accordance with the e-commerce plan and data requirements. If not, check the existence of planning initiatives for the acquisition of necessary tools. Then he should get all the required documentation pertaining to organisational chart, data classification policy, architecture model for information, encryption tool specification and network infrastructure. Further an auditor should understand the acquisition procedures for infrastructure software and examine the maintenance records of encryption tools.

Planning: This involves:

Examining the responsibilities of different personnel of the security department in security and encryption processes.

- Identifying the data requirements and regulatory requirements for encryption.
- Identifying the current risk level and compare with the acceptable risk level.
- Evaluating the decision-making process and selection process for tools and ensure its compliance with the present technologies.

The auditor must ensure the existence of private key management procedures with a detailed description about its development, implementation and termination.

Purchase, execution and maintenance of encryption:

This involves:

- Verifying the procedures for purchase and implementation process of encryption tools.
- Ensuring that they meet the desired requirements.
- Examining the access controls and change control processes over encryption tools.
- Evaluating the efficiency of encryption output and determining its conformity with the organisational policies.

Encryption keys:

This involves:

- Checking the appropriateness of access to keys.
- Evaluating the distribution, maintenance and termination processes for keys. Auditor should ensure that proper controls exist over encryption keys.

Answer: [d] All the above

Module:4

Reference No:M4238

Question: In which of the following terms routers prove to be better than bridges?

- [a] Fault detection and isolation
- [b] Installation and configuration
- [c] Relocating workstation within the network
- [d] None of the above

Module 4 – Comparison between routers and bridges

Bridges and routers- definition

Bridge is a device that transfers messages between LANs using the same protocol. It can be thought of as a device that decides whether a particular message is to be sent within the LAN or to an interconnected LAN. Routers are devices that establish the next destination for the data packets. In other words, it decides on the path to be taken for sending a data packet to its destination. Thus, basically both bridges and routers integrate networks and internetworks thereby simplifying the task of connecting networks together.

Differences between routers and bridges

Bridges and routers differ in their working approaches and individual merits and demerits which has been discussed below:

- Installing a bridge is simpler as compared to a router. This is because, routers are dependant on protocols and hence require separate software packages that support individual protocols in which the routers run. This makes installation and configuration of a router complicated. On the other hand, bridges connect networks working in different protocols without requiring any supplementary software package. This is because, bridges are implemented below the network layer in the OSI reference model, thus freeing the network layer from the intricacies involved in the lower level protocols.
- Routers make use of redundant paths in a network for dividing certain applications so as to reduce the load on the network. Thus, routers make optimum utilisation of the available bandwidths. Bridges are not

capable of using redundant paths in a network and hence are not capable of splitting up the load on the network.

- All the intermediate network segments in a bridge have the same network address. Thus, conceptually a bridge can be viewed as a single network and any workstation is portable within the bridge. Routers implement end-to-end communication system i.e. each segment in the network has a different network address. Thus, for traversing the network, permission has to be sought from the network administrator so as to relocate a workstation to another location.
- Bridges are not capable of preventing "*broadcast storms*". A broadcast storm occurs when a data packet is sent more number of times than it should have been. This leads to clogging of the bandwidth eventually making the whole network malfunction. While on the other hand, routers are very effective in working against broadcast storms. Routers incorporate a firewall between the sub-networks, which shields the broadcast storms from affecting the entire network.
- Routers support any kind of network ology and hence make a network extendible while bridges lack flexibility in establishing connections. Some of the applications that make use of bridges for execution often disrupt the functioning of other applications (the incompatible ones).
- Routers can differentiate between different paths in terms of cost, bandwidth and the like, and hence prove to be better decision makers in terms of path selections. In fact routers can make use of all active paths. Thus, in terms of flexibility, routers are more adaptable as compared to bridges.
- Fault isolation is literally impossible in networks implementing bridges. Bridges are conceptually single networks (i.e. have same network address throughout the network). This makes detecting a fault and isolating it from the rest of the system especially in distributed networks unfeasible. Routers, inherently by design have different network addresses for different network segments. This enhances the chances for fault detection and isolation.

Answer: [a] In fault detection and isolation

Module:4

Reference No:M4239

Question: Which of the following is not a function of Metropolitan Networks (MANs)?

- [a] Providing end-to-end security
- [b] Convergence of data/video/audio
- [c] Providing connectivity to vast areas e.g. a country, continent and the like
- [d] Routing data traffic from LANs to WANs or to other LANs in the same metro region

Module 4 – Metropolitan Area Networks (MANs)

Introduction

Definition: Metropolitan Area Networks (MAN) is a set of networks that connect a vast area, typically a metro region. In fact it is a distinct network that belongs to a single network operator or service provider. It provides access and services to a metro region. Conceptually MAN comprises a group of networks that work collectively in order to connect smaller network installations in a metro region.

How MANs differ from LANs and WANs

LANs (Local Area Networks) and WANs (Wide Area Networks) are defined in terms of their locale (i.e. the extent of spread of network). While, MANs are defined in terms of both distance (the border or vastness) and functions. The limits of LAN is defined by the boundary of an organisation (known as an '*enterprise edge*') and the limit of WAN known as '*edge*' is defined by vast network stretches. This may comprise many Points of Presence (POPs) and other installations spreading across a vast locale e.g. a country, continents and the like. In terms of vastness, LANs are smaller as compared to MANS and typically span less than two kilometres. In contrast, MANS stretch upto 150 kilometres. WANs are larger than MANs in terms of span, typically stretching above 150 kilometres in area.

Purpose of MANs

Traffic Explosion: Constant increase in data traffic in communication network channels has given way for increased bandwidth in Local Area Networks and Wide Area Networks. As a result, managing and controlling huge bulk of data across LANs and WANs becomes a challenging task. Hence, MANs are implemented to manage data flow across the networks and route them so as to avoid information congestion. Thus, MANs typically, route the traffic in transmission from LANs to WANs or to other LANs stretching within the same metro region.

Some of the key functions performed by MANs are as enumerated below:

- MANs support applications and services run in large networks like WANs, nested LANs and the like. MANs direct the information flow from one LAN to other in the same metropolitan region or from a LAN to a WAN.
- MANs provide secure access to users in vast distributed structures of network.
- Since individual service providers offer MANs, these are always designed with competitive features like implementing integration of voice, video and other forms of data into the same channel, combining bandwidth of data and network control.

Key requirements for Metropolitan Area Networks

Ideally, a MAN should conform to the following:

- It should provide end-to-end security, which is usually implemented using Virtual Private Networks (VPNS), VLANs and the like.
- It should be capable of integrating different forms of information like voice, images, text etc. so as to transmit different forms of data through same communication channel. This feature is known as data convergence.
- Since MANs are privately owned, it should support usage-based billing (i.e. charges on the basis of utilisation of the network) for bringing about flexibility in business models.
- MANs should be flexible and have enhanced network management systems (i.e. it should be flexible and capable of controlling abrupt fluctuations in data traffic).

Answer: [c] Providing connectivity to vast areas e.g. a country, continent and the like.

Explanation: Large networks like the ones connecting countries, continents etc. are known as Wide Area Networks (WANs). MANs are smaller as compared to WANs in terms of span.

Module:4

Reference No:M4240

Question: Broadcast storms in communication channels occur mainly due to

- [a] Sending the same broadcast packet more number of times than it should be
- [b] Increase in the hop count
- [c] Improper routing decisions
- [d] Lesser bandwidth of the communication channel

Module 4 – Broadcast storms

Definition

Broadcast storms refer to occurrence of bandwidth congestion when a broadcast packet (or a data packet) is sent more number of times in a network than it should have been. Eventually, a large part of channel bandwidth is consumed, thereby increasing network traffic.

Why does it occur?

An information packet called broadcast message is sent to a common IP address, thereby reaching all the communication points in a channel. In other words broadcast messages are received by every member in the network irrespective of his IP address. E.g. e-mails distribution, message distribution and the like. At times when a broadcast packet is sent in a network, it goes unattended due to the presence of electrical noise in the network. Since every router in the network receives the broadcast message, each one of them starts sending the broadcast packets successively. Consequently, every data packet (broadcast packet) is duplicated as each router in the network sends the broadcast packet. Now, when *hop count* (i.e. the number of communication points or legs in a network that is traversed by a data packet before reaching the destination) reaches zero, it indicates the completion of data transfer from one end to the other. And hence the broadcast dies out, but eventually would have used more bandwidth than it should have for broadcasting a particular message.

Role of routers in preventing broadcast storms

Routers adopt a three-step process to avoid broadcast storms

- *First step:* In the first step known as the *reverse path forwarding*, the routers ensure that broadcast packets are forwarded only if they receive the data packets in the *primary interface*. When a router chooses to send the broadcast message through the same channel through which it receives the message, it is known as a primary interface. The messages received through all other interfaces are omitted (i.e. considered as duplicate messages). Thus, the router sends the broadcast message only once irrespective of the number of times it receives them. This significantly reduces the number of broadcast messages thereby reducing the storms if not completely eliminating them. The reduction depends upon the way routers make the selection of primary interface.
- *Second step:* Broadcast storms are completely eliminated if it is ensured that all the parallel routers send the broadcast messages through the same primary interface. This kind of uniform selection is implemented by selecting the interface with the lowest MAC (Media Access Control) address as the primary interface. In other words the first interface is always taken as the primary interface. This will force every router to choose the same interface (i.e. the first communication interface) as its primary interface that will guarantee elimination of a broadcast storm.
- *Third step:* After the second step it is a very remote chance that a broadcast storm will occur. And even if it does which is very improbable, the last step takes care of it. As a final step of prevention, it is ascertained that the MAC address of the source (from which the router receives the message) is same as that chosen by the router to send the broadcast message. This will discard any message that has a mismatch in the MAC addresses. Thus, the third step will eliminate any chances of occurrence of broadcast storms that might remain even after implementing first and the second step.

Answer: [a] Sending the same broadcast packet more number of times than it should be

Module:4

Reference No:M4241

Question: Digital signatures should be incorporated in the presence of a certification authority in order to

- [a] Ensure the identity of the signatory and authenticate his signature
- [b] Avoid incongruity in legal policies during cross-border transactions
- [c] Give a final approval for a proposal
- [d] Identify enacted legislation for the partner and the home jurisdiction

Module 4 – Implementation issues in Digital Signatures

Introduction

Digital signatures provide a convenient means of appending signatures in digital forms. They can also be used

for legal documents, provided the implementation is foolproof and leaves no loopholes in establishing security. However for digital signatures to substitute for regular signatures, it should be authentic, easy to use and difficult to counterfeit. Prior to implementing digital signatures as a replacement for written signatures in signing documents traversing through varying jurisdictions, (like for example from one country to another), it should conform to the legal policies and specifications of the region where it is to be used. The risks involved in employing digital signatures include financial losses due to forgery, revelation of confidential information, illegitimate use of digital signatures in transactions and disruption in proper functioning of the company due to unreliable procedures to implement digital signatures.

Hence, the key issues in implementing digital signatures are contractual requisites of the trading partner, suitable scheme for implementing digital signatures, reliability in the implementation and the directives governing the implementation of digital signatures. Further, respective national laws, state and provincial laws, traders' contractual agreement on the use of digital signatures and legal viewpoint should be taken into consideration before using digital signatures in cross-border e-commerce. Each of these perspectives has been discussed in detail in this article.

- **Implication of a digital signature:** Documents are signed in order to authenticate the transactor and in turn authorise transactions or further progress in deals or business proposals. Hence, digital signatures serve the following purposes:
 - o It provides identification and authentication for the signatory. It substantiates the signatory's approval on the document, and hence it is very essential for the signatory to understand the legal consequences prior to signing the document (with e-signature).
 - o It provides a decisive statement for a negotiation. In a sense, it gives a final conclusion or formal approval for a proposal.
- **Working:** Digital signatures are implemented through cryptography. They are created using various techniques or algorithms for encrypting plain text into cipher text and vice versa. The principle and concept of implementation of digital signatures has been discussed in the previous article on digital signature.
- **Legal implications:** A fixed set of strictures that meets all the requisites of the respective jurisdiction (i.e. individual state, country or province) has to be set up so as to avoid incongruity in legal policies during cross-border transactions. In other words, each country, state or province that transacts using digital signatures must abide by standard principles that do not counter other regimes or administrations.
- **Reliability and validity:** Digital signatures should be incorporated in the presence of a certification authority (that is mutually approved) to ensure the identity of the signatory and authenticate his signature. This formalises the dealings and offers validity to the whole process of transaction. Further the encryption and decryption of messages should be carried out in a secure mode.
- **Guidelines governing implementation of digital signature:** Any set of rules and regulations set by a company for administering digital signatures in online transactions should ideally take in to consideration the following:
 - o Identifying business requirements for security, validity, due diligence, approval, clarification and finalisation of electronic documents in e-commerce environment and the application of electronic signatures
 - o Developing strategies that will meet the business requirements
 - o Identifying existing best practices relating to electronic signature implementation
 - o Identifying enacted legislation for the partner and home jurisdiction, specifically relating to electronic authentication and the use of electronic signatures
 - o Identifying new challenges with respect to electronic signature implementation, such as:
 - Basic properties of digital signatures
 - Risks associated with the use of digital signatures
 - Security and control issues

- Legality of the signature
- o Identifying technology issues
- o Transforming the current environment to using electronic signatures for document signing

Answer: [a] To ensure the identity of the signatory and authenticate his signature

Module:4

Reference No:M4243

Question: What are terminators in a bus ology used for?

- [a] To prevent messages from colliding with each other
- [b] To transfer message from one workstation to the other
- [c] To add newer branches to the main cable
- [d] To terminate a communication session between the two terminals

Module 4 – Network ologies – II The Bus ology

Physical configuration of the cables and wires, the workstations in the network including the connections with the peripheral devices are collectively known as a *ology*. In other words, a ology describes how the workstations in a network are connected to each other and the peripheral devices. A network ology refers to the physical network connections. It is different from a logical ology. Logical ology involves techniques for transferring information in a network, and it is not concerned with the manner in which computers are physically connected. Bus ology is one of the most widely used network ologies.

The bus ology

Definition: A bus ology basically refers to a type of network configuration, where all the network devices, including workstations, servers, printers and other peripheral devices are connected to a single cable commonly referred to as a bus.

In other words, all the devices in the network are connected to the central cable, i.e. the bus or the backbone of the network. A bus is a transmission path, through which every device attached to a network passes and receives signals to and from one another.

Diagrammatic representation of a bus ology network

Dataflow in a bus ology

In a bus ology, all the devices are connected to a single cable directly and all the data packets pass through each of the devices (that are connected to the cable). Every network device connected to the bus has a distinct identity. Thus, when the message transmitted through the bus holds this unique identity, it recognises the signal and immediately associates with the corresponding network device. Typically, Ethernet systems employ bus ology.

The device that wants to communicate sends a broadcast message, which is received by all the devices present in the network

The central cable that connects all the devices in a network, often referred to as the backbone of the network, uses tee connectors that are plugged into network adapter cards present in each device.

Physical configuration of a bus ology

Basically, each and every network element has a terminator at one end of the tee connector and the other end of the device has a cable going out connecting the next device. These terminators prevent the network signal from being reflected back into the cable and colliding with other transmissions. RG-58 thin net is used as a cable in a bus ology.

Typically, the speed of transmission is around 10 megabits per second. These networks are confined to only connecting a maximum of twenty network devices on one segment, and a segment cannot be longer than 185 meters. Hence, to make the network extendible, repeaters are used. *Repeaters* are devices that are used to amplify the signal so as to send it across longer cables. However the usage of repeaters is limited to only three segments.

Advantages of a Bus ology

- Very easy and simple to design and implement a bus ology, since every node is connected to one single cable. Even the main server is just another node as far as the architecture is concerned.
- Easily extendible in terms of architecture as newer nodes can be added just by introducing new branches to the main cable as long as the cable has a terminator at the end.
- Comparatively less expensive than star ology, since lesser number of cables are required in setting up a bus ology. Moreover, no hubs are required in bus ologies, thereby cutting down the implementation costs.
- Only the affected node is functioning not the entire network

Disadvantages in a Bus ology

- Difficult to troubleshoot
- Failure in the main cable of the network causes a breakdown in the whole network
- Limited in speed
- Terminators are required at both the ends of a cable, which limits the number of branches that can be added to the bus. This makes it unsuitable in implementing it in large buildings.

Answer: [a] To prevent messages from colliding with each other

Module:4

Reference No:M4244

Question: Which of the following statements is not true of a star ology?

- [a] A star ology is implemented in two variations viz. star bus and star tree
- [b] In a star ology, data is always transmitted via the central hub
- [c] Star ology allows direct data transmission among the network devices
- [d] Star ologies are extendible to cover larger geographical domains

Module 4 – Network ologies – I The Star ology

An overview of network ologies

Configuration of the cables and wires, the workstations in the network including the connections with the peripheral devices are collectively known as a ology. In other words, a ology describes how the workstations in a network are connected to each other and peripheral devices. A network ology refers to the physical network connections. It is different from a logical ology. Logical ology involves techniques for transferring information in a network and is not concerned with the manner in which computers are physically connected.

The basic types of network ologies are

- Star ology
- Bus ology
- Ring ology
- Tree ology

The star ology

Definition: A network ology that is structured in such a way that each node, be it a peripheral device, a server or a client is directly connected to a single network hub often referred to as the *central network hub*

or concentrator. Thus, in a star ology, each network element is cabled to the central network hub that provides every device connected to it with a separate network connection.

Diagrammatic representation of a star ology

Data transmission in star ology networks

Since every network element is connected to the central hub or concentrator, all the data packets first pass through the central hub before reaching the destination. In gist, all data transmissions occur via central hub and not directly between the two endpoints of communication. Thus, it can be observed that if there is a fault in the cable connecting one computer, it doesn't affect the rest of the network. This is because the central hub isolates every node from the other and hence is responsible to route all transmissions from source to destination.

Physical configuration of a star ology

Typically, a star ology is implemented using twisted pair copper cabling. Coaxial cables or fibre optic cables can also be employed in setting up a star ology. Star ology is set up in two variations viz. star bus and star tree ologies.

- **Star bus ology:** In a star bus ology, multiple network elements are connected through a bus trunk, i.e. through thin lines of network.
- **Star tree ology:** In a star tree ology, the network elements are connected through twisted pair cables or fibre optic cables. Star tree ologies, generally support communications in a much larger geographical domains.

Advantages of star ology

- Easy configuration and installation.
- Star ologies are ideal for interconnecting large physical domains.
- Further expansions in a network, (i.e. adding newer network elements in the already existing network) is simpler and easier.
- Fault detection and troubleshooting is easier, since, the central hub isolates each and every network device from the rest of the network.
- A problem with the cable in one part of the network won't disrupt the functioning of the whole network, since every transmission is directed via the central hub. Thus, as long as the central hub is not affected, the network can smoothly function disregards the problems that might be present in the individual nodes.

Disadvantages in a star ology

- Since, the central hub is the sole point of communication in the network, it amounts to a high risk in case of failure of the central concentrator.
- Cost of implementation is high, as concentrators are expensive. In addition, maintenance costs are high too.

Answer: [c] Star ology allows direct data transmission among the network devices

Module:4

Reference No:M4245

Question: What is the goal of accounting management according to ISO standards for network management?

- [a] Monitor network and system configuration
- [b] Evaluate network performance parameters and maintain acceptable network performance level
- [c] Control access to network resources
- [d] Measure network utilisation parameters

Module 4 – ISO standards for network management

Network management system is an integration of a variety of tools, application programs and devices that assist manual governance and monitoring of networks. A network management system automates the whole process of monitoring and governing all the activities in a network. It governs all the activities pertaining to interconnections that connect the workstations in a LAN or WAN, handles distributed / network databases, involves auolling of various network devices and controls network traffic and handles ology changes.

Design issues

Ideally, a network management system should conform to the following issues:

- **Security:** The primary concern of a network management system is to protect the assets of an organisation and prevent unauthorised access to the internal network.
- **Access:** It should ensure that the system data is accessible only to authenticated users, i.e. it should impose selective access to system data.
- **Optimisation:** An ideal network management system should ensure optimum utilisation of the resources (viz., workstations, bandwidth of the interconnecting cables, printers or other peripheral devices, power supply etc.) in a network. It should strive to maximise the utility value of assets in terms of cost and time.
 - Productivity and availability: A centralised management and maintenance system should be established in order to increase the uptime and system availability.

Thus, network management occurs at various levels, each level being in charge of one or more of the above design issues. ISO (International Standards Organisation) has set up a standard for network management that lays down chief conceptual areas that should be addressed by a network management system. It provides a common means for understanding the chief functions and organisation of network management systems across the globe.

The five major conceptual areas laid down by ISO standards are:

- **Performance management**

The chief objective of performance management is to evaluate various aspects of network performance and to ensure that the performance is maintained at an acceptable level. Some of the parameters taken into consideration for performance evaluation of the network include network throughput, user response times and line utilisation.

Three steps are involved in performance evaluation.

 - In the first step, data on variables of parameters (like response times, line utilisation and the like) are gathered by the network administrators.
 - In the second step, this data is analysed and normal or acceptable (baseline) levels for each of these parameters is established.
 - Finally, performance thresholds for these parameters is set up, exceeding which the system would call for attention; i.e. when a threshold is exceeded by any of the network device or interconnecting interfaces, an alert is generated and sent to the network management system.
- **Configuration management**

The primary goal of configuration management is to monitor network configuration. In other words, configuration management tracks down incompatibilities between different devices and systems and resolves them.

Every network element be it a workstation or interconnecting cable, has a specific version associated with it. Say for example, Operating system version 4.5, Serial communications controller version 1.1 and the like. Configuration management is responsible for storing this information in a database for easy access when a problem is encountered.
- **Accounting management**

The goal of accounting management is to evaluate network utilisation parameters. It is responsible for regulating the number of individuals or groups that work in the network. Since, resource capacities are limited, the number of users should not exceed the specified limit failing which the network would

encounter problems like excess network traffic and the like. Accounting management, thus, regularises resource capacities and user proportions and sets limits and thresholds on each resource.

□ **Fault management**

Fault management isolates and detects problems in the network and notifies the appropriate authority for fault-rectification. Fault management is the most widely implemented network management, since, faults comprise the primary cause for unacceptable network degradation.

□ **Security management**

Security management ensures authorised access to network resources. It protects the network from intention or unintentional damage by outsiders. It incorporates user logins to validate access by permissible users. Security management also identifies sensitive network resources and monitors various access points to such resources.

Answer: [d] Measure network utilisation parameters to maintain proportion between resource capacities and the number of users using them

Module:4

Reference No:M4246

Question: Which of the following statements is not true of a network management system?

- [a] Network management system controls network traffic and handles topology changes
- [b] It integrates various tools and application programs to automate the process of monitoring networks
- [c] It is a software module that stores the responses of network devices during a poll
- [d] It detects fault in the network by polling the network devices

Module 4 - Network Management System (NMS)

An overview

Expansion of networks led to the development of newer network technologies and topologies. Companies worldwide were struggling to ensure compatibility of the existing system with newer network devices, topologies and technologies. This called for evaluation and upgradation of the existing system. Each new technology required its own set of experts and strategic network growth planning. This led to tremendous increase in staffing requirements for large, heterogeneous networks. Thus, there was an immediate need for an *automated network management system* to assist technical experts in integrating diverse network environments.

Network management system is an integration of a variety of tools, application programs and devices that assist manual governance and monitoring of networks. A network management system automates the whole process of monitoring and governing the activities in a network. It governs all the activities pertaining to interconnections that connect the workstations in a LAN or WAN, handles distributed / network databases, involves autopoling of various network devices and controls network traffic and handles topology changes.

NMS architecture

The basic structure and set of relationships in most of the network management systems is same. Basically, a network management system sets up individual alerts for every workstation and network device in the network. On encountering and detecting a problem in the functioning of any of the network devices, these alerts are sent to the corresponding device(s) notifying the fault. The devices are automated / programmed in such a way that on receiving the alerts, they start executing a group of actions (that are pre-defined) like event logout, shutting down, automatic attempts at system repair etc. The devices also notify the operator of success or failure in rectifying the problem.

Polling: In order to detect faults in the system, the network management system adopts polling (that is either automated or user-initiated). In polling, certain variables or values are sent to individual network

device. Every device in the network responds to such polls. All the responses are stored in the management database, that finally assist the network management system in checking the system for any malfunctions. This information (residing in the management database) is provided to the network management via a *network management protocol*. Some of the examples of network management protocols are *Simple Network Management Protocol (SNMP)* and *Common Management Information Protocol (CMIP)*.

Architecture of a typical network management system

Agents and proxies: Software modules that compile the information on network devices and store the responses of each of these devices during the poll are referred to as agents. Sometimes network elements send common responses. In such cases network elements respond individually and send a collective response on behalf of the whole group through *management proxies*. E.g. when a LAN responds to a poll, a single response is sent on behalf of all the workstations connected in that LAN. The diagram above illustrates how network management system integrates all the network elements, automates the process of polling and stores the information in the database.

Answer: [c] It is a software module that stores the responses of network devices during a poll

Explanation: Software modules that compile and store the responses of network devices in the network management database are known as agents.

Module:4

Reference No:M4247

Question: Which of the following tasks is the main function of the help desk?

- [a] Better system development
- [b] Identification of the causes for problems and documenting solutions
- [c] Effective hardware configuration
- [d] Minimising operational errors

Module 4 – Automated Problem Management Processes

Introduction

The place where information pertaining to several problems is stored is referred to as a help desk, a call centre or a Customer Interaction Centre. Such data is collected based on solutions to previously solved problems. The help desk identifies causes for problems and maintains a record of solutions. Hence they facilitate organisations to solve problems and take management decisions.

Benefits of helpdesk

1. Data companies understand products and processes thoroughly.
2. The management can devote its time to finding different methods to enhance staff efficiency.
3. Improves staff productivity.
4. Training solutions can be identified through help desk outputs.
5. Software rollouts can be tested.

The above benefits can be achieved and Customer Interaction Centres can efficiently work in supplying information when the data is collected and listed according to the needs of the company. This is possible with the availability of the appropriate tools.

Need for automating the problem management process

- Requirement of a systematic process. The database must provide solutions to customer problems.
- The need to develop standards and performance measurement systems.
- Demand for data collection across the organisation.

The following are different trends that form a part of help desk services with greater emphasis on the quality of problem management: -

I. System structuring: It refers to the hardware and software of the system. Currently, several hardware and software systems can be configured in an organisation. This increases the need for addressing different problems of all those systems. Automated Help Desk (AHD) enables organisations to obtain information for different platforms. Further, workflow can be arranged in such a way that the right person solves problems on time.

II. Remote computing and telecommuting: Refers to the development of remote computing, and telecommuting for data connectivity at remote places. An AHD through the provision of system and customer related information solves the problem of remote computers.

III. Development of new software programs: Problems that arise in the course of new systems adoption can be addressed with the help of an AHD because it recognises new trends and manages them properly.

IV. Growth of the companies: It is common to experience a change in help desk requirements with the growth of an organisation. Greater number of requests can be processed by the AHD without increasing the support staff. The help desk's support to training facilities and effective communication helps avoid unnecessary investment in support functions.

Other functions

- *Customer specific:* The help desk enables data collection according to user needs. Hence customer specific products can be developed.
- *Cordial relations among groups:* By supplying information on time help desk ensures better relations among groups, which is essential for success.

Modern Help Desks

Unlike traditional help desks, a modern help desk solves issues at the route. It is proactive in nature and utilises resources efficiently. This enables the staff to be more customer centric.

Help Desk Services

The help desk provides services to several users based on the services derived from many others. The following diagram depicts the position.

The 'front-line' position of the help desk enables it to function dynamically. It serves as an effective medium to solve problems in the complex work place. Thus, it must be ensured that the help desk is integrated with the organisation properly. Its development plan, mission statement, and policy must be properly drafted. However, organisational needs have to be assessed before any of this can be undertaken.

Answer: [b] Identification of the causes for problems and documenting solutions

Question: Which of the following layers of an ISO-OSI reference model support routers?

- [a] Network layer
- [b] Application layer
- [c] Session layer
- [d] Physical layer

Module 4 – Routers

Definition

A router or a B- router is a device that works both as a bridge and as a router. In other words, a router is a bridging network that makes packet routing decisions like a router. It is a network router that integrates dynamic routing properties in order to connect different LANs. Typically, the network layer and the data link layers of the ISO-OSI reference model incorporate routers to make interconnections between LANs.

A brief overview on bridges and routers, and how they are integrated in a router

A *bridge* establishes a connection between one or more LANs that use the same protocol. When information is to be transferred from one LAN to the other, a bridge forms the intermediate network between the two LANs. A *router* refers to a router table that stores information about all the interconnected LANs as it connects many networks at the same time and then takes the packet routing decision accordingly. Thus, it can be observed that a router requires more information regarding the interconnections than a bridge does. A bridge is concerned with only one path.

A router eliminates the limitations of both the routers and bridges while transmitting data. It implements *source route bridging mechanism* to determine the routes dynamically using different routing algorithms (like a bridge) and then establishes the final communication channel through which it would send the data (like a router).

The source router bridging mechanism

As discussed above, the source bridging mechanism performs a dynamic check to discover various routes available for transmission and selects the most appropriate one among the available lot.

- First the router checks for a match between the routing information provided in the token-ring frame (or data packet) and the bridge number (the number assigned to the bridge and other rings attached to it).
- Then depending on the structure of the network and the algorithm used for selecting various routes from the source to its destination, the router settles on the best route in terms of cost and time taken to send the information.
- Finally, they establish interconnections between token rings either by implementing parallel bridging and increasing redundancy in the network or by dispersing the network traffic across various channels and cutting on hop counts between clients and the servers.

Advantages of routers

- Routers connect many token rings together and thereby allow network traffic fragmentation. This checks data concentration on a single route and reduces load on the network eventually increasing network performance.

- The source router bridging technique employed by routers is a fault-tolerant mechanism as it is capable of determining substitute paths for transmission in case of bridge failures. This is because a router is in charge of both path determination and decision-making.
- Routers allow interconnection between geographically distant LANs as it connects different token rings and thus overcomes inherent limitations present in a single-network. This expands the physical reach of data packets thereby extending the LAN capacity of sending data packets.
- Since routers segment network traffic, they are capable of localising data traffic and thus optimise the Internet capacity for data transmission.

Answer: [a] Network layer

Module:4

Reference No:M4249

Question: What is the function of Webcrawler or spider with reference to search engines?

- [a] Read through all the pages and save the contents to make information available for indexing
- [b] Build the index for every word read from the pages
- [c] Provide user interface in taking user response and displaying the relevant results
- [d] Sort out the results based on the relevancy of the web document

Module 4 – Search engines

Introduction

Search engine is a software application program that retrieves documents (or in other words web pages) relevant to the users' requests from an exhaustive database maintained by the website. Search engines basically read and catalogue large portions of web documents. Search indexes can be general, topic-specific, region-specific or site-specific. Search engine is a tool integrated in a web portal. And the web portal that has a search engine is known as a Search destination. Search destinations are websites that either have their own search tools or rely on a third party. A search engine powers the search process and provides the results for a search destination. Some examples of search engines are Google.com, Webcrawler.com and Yahoo.com.

Components of a search engine

Typically, a search engine includes:

- A spider that crawls on the web going from one page to the others to locate the relevant pages and then read those pages to index the information on them in order to make them searchable. Spiders are also referred to as *web crawlers* or *bots*. And the process of crawling is also known as *harvesting* or *robot spidering*.
- An application program that builds an index for every word read from the pages visited by the bot and stores the information in the database. This program is also known as *index building software* and is also responsible for ranking the best documents (ranked on the basis of their relevancy to the user's query).
- User interface that is responsible for receiving user requests, pass them on to the index in the back end, comparing them with the entries in the index and finally display all the relevant pages according to the ranking on the basis of relevancy.

Search engine technology

The total process of receiving the requests from the users, comparing them with the database in the back-end and then displaying the results is divided under the following categories:

- **Crawling the web:** Crawling or web-spidering is done by robots (also known as bots) that traverse web pages by retrieving the document, and recursively following the links from that document. In fact web crawlers browse the web pages just as web browsers do, with the exception that web browser traversals are user-initiated (i.e. browser traversals are controlled by users), while web crawlers are automated. The sites or pages visited by the web crawlers are indexed on a daily or hourly basis. These software applications are very fast and visit many sites in parallel. An important point to be kept in mind while implementing crawlers is that they should be restricted from visiting sites that infringe on privacy.
- **Building the Index:** A search engine index is similar to a book index that appears at the end of a book. It lists all the terms that appear on a web page. Once the web crawler reads huge volumes of pages including web documents, PDF and other file formats, all the terms are enlisted in that index. Once the indexing is done, the documents are ranked on the basis of relevance. The best document is put on a higher rank and appears first in search results. Some of the techniques employed by the search engines to rank web documents are text analysis (i.e. evaluation of web documents on the basis of matching words, font size etc.), links & link text analysis (evaluating the text on the links and on the pages directed by these links) and Page rank measure (evaluates how often a random user, while searching, would end up in a particular page).
- **Displaying search results and User Interface:** User interface of a search engine also known as the front-end, provides a search form wherein, the user types his query and clicks the search button. Once the query is sent to the database in the back-end, it is compared with all the entries in the index and the relevant web documents are displayed in order of their ranks.

Answer: [a] Read through all the pages and save the contents to make information available to form the index

Module:4

Reference No:M4251

Question: Which of the following is not a feature offered by a web browser?

- [a] A web browser allows navigation from one web page to the other
- [b] It allows to save a current web page
- [c] It connects a workstation to the internet
- [d] It makes all the web pages on the WWW accessible

Module 4 – Web Browser

Introduction

Web browser is an application program that allows users to view web documents on the World Wide Web. In other words, it makes the documents stored in a single computer or in network system, available or accessible to the browsers. A web browser allows

- ☐ Printing web pages
- ☐ Finding a particular text or phrase on a page
- ☐ Creating a bookmark

Web browser acts as an interface between the user screen and the server. It displays the pages from the web server in the user window. Internet Explorer and Netscape Navigator are the most common web browsers in use.

Web browsers run within a window. The browser window includes the title bar, menu bar, address bar, loading indicator, toolbar, page display and footer.

- ☐ **Title bar:** Title bar of the browser, displays the title of the current page.

- **Menu bar:** Menu bar is located below the title bar of the web browser window. It contains various options to open and navigate the web pages. Some of the most common options found in almost all the browsers include the following menus

- o File
- o Edit
- o View
- o Navigate
- o Bookmarks
- o Windows
- o Help

File Menu

File menu gives options to open a new web page, save a web page, close the existing web page, reload the current web page and s loading the current loading web page.

Edit Menu

Edit menu allows to find a word or phrase on the web page, copy the content of the web page, Web Browser Preferences displays a dialog box that lets you choose the page that will be displayed each time the web browser starts.

View Menu

View menu allows the user to view the text in the web page in varying font size. It also lets the browser to view the source HTML file of the current web page in the window. It allows the browser to customise the window by giving the option to select the toolbars to be viewed. It shows or hides the address and the status bar. It helps in navigating from the current page to the previous page to the next page or to the home page.

Navigate Menu

Navigate menu includes a forward button, a backward button, a history button and a shortcut to home page button. *Forward* displays the page that is viewed just before the back button is clicked. It can be used only after the back button has been clicked or if more than one page has been opened on the same window. *Back button* takes the browser to the web page preceding the current web page. Clicking on the home button takes the browser to the home page. *Home page* is the web page displayed just after the browser window has been opened. Home page preferences allow the viewer to set the home page according to his preferences.

History button opens the history dialog box that lists the titles of all the pages visited during a current session. These titles are arranged in an order, starting from the recent most page visited. The user can revisit the links appearing on the history just by clicking on them.

Help Menu

Help menu displays the help contents for help ics, an overview of the web browser, online support and descriptions of the web browser menus.

Answer: [c] It connects a workstation to the internet

Question: Which of the following is an example of LMDS (Local Multipoint Distribution Services)?

- [a] Cable television networks
- [b] Mobile networks
- [c] Wireless access networks
- [d] Customer premise configuration

Module 4 – Local Multipoint Distribution Services (LMDS)

Introduction

With the increasing dependency on networks, it has become very essential to make large amounts of bandwidth available to subscribers both for domestic and public use. This entails establishing highly directional antennas and polarisation of signals that will establish a centralised connectivity, i.e. connecting to a central hub. In this regard, LMDS serves as an economic solution by bringing high-bandwidth services to homes and offices located in locales that are unreachable by conventional cables or optic fibres. LMDS provides digital two-way voice, data, Internet and video services. Privately owned cable television networks are an example of LMDS network.

Local Multipoint Distribution Services (LMDS) is a broadband wireless point-point communication system. It is a broadband wireless local loop that integrates multiple services and accesses in a network.

Features

An LMDS service is characterised by the following:

- The propagation limit of signals in LMDS is local. This means that the potential coverage area of a single site area extends to about 5 miles and the LMDS transmitters are placed at up to this range. This is the reason why the service is termed 'local'.
- The signals in LMDS are transmitted through point-to-multipoint or broadcast method, i.e. the central hub broadcasts the message, which in turn is received by all the LMDS transmitters. However, the return path, (i.e. from the subscriber to the base station), is a point-to-point transmission. In other words the subscribers send the responses only to the transmitter, rather than broadcasting the message in the entire network.
- The distribution of signals in LMDS consists of simultaneous voice, data, Internet and video traffic.
- LMDS network is entirely dependant on the operator's choice of business. This implies that a subscriber nature of relationship exists between the operator and the customer, (i.e. LMDS operators are paid for the services they offer to the subscribers, depending on the kind of service they offer)

LMDS Architecture

Broadcast or point-to-multipoint system is the most common LMDS implementation type. Since, LMDS is a combination of voice, data and video, transmission is carried out using both asynchronous transfer mode (ATM) and Internet Protocol (IP). For a detailed discussion on ATM and IP, refer separate articles on them. Basically LMDS network comprises

- Network operations Centre (NOC)
- Fibre-based infrastructure
- Base station
- Customer premise equipment (CPE)

NOC contains the *network management system (NMS)* equipment that manages large regions of customer network. Multiple NOCs are interconnected. The fibre-based infrastructure comprises synchronous optical network (SONET) optical carriers, ATM, CO (Central-office) equipment IP switching systems, and public switched telephone networks (PSTN). Local switching allows the customers to communicate with one another without entering the fibre-infrastructure. A base station converts the fibred infrastructure to a wireless infrastructure.

Chief functions of a Base station includes modulation and demodulation of the frequency of the signals transmitted, microwave transmission channel access management, registration and authorisation of LMDS operators and subscribers. It is also responsible for local switching.

Customer premise configurations vary from vendor to vendor. Basically all the configurations include outdoor microwave equipment and indoor digital equipment providing modulation-demodulation control and customer-premise interface functionality.

Advantages

- Broadcast technology in LMDS offers a method to provide high-capacity local access with lesser cost than a wireline or cable solution. LMDS systems can be deployed without disrupting the environment much.
- It is faster to deploy LMDS network than a wireline or cable network. It also offers combinations of applications and services. Thus, the operators get paid faster too.
- Point-to-point fixed wireless networks in LMDS offer high-speed dedicated links between high-density nodes in a network.
- LMDS is a demand based architecture and is scalable as per customers requests. In other words, there is very little or no wireless network's cost till a customer requests for such a service and a customer premise equipment is installed. Thus, the operator can time the expenditure so as to match it with the requirements of the new customers. E.g. in a privately owned cable television network, till the customer subscribes to it.
- Since the deployment of LMDS networks is flexible, it delivers services directly to the end users (i.e. last-mile solution), at any point of time.
- LMDS is cost-effective and incurs less in maintenance, management and operating costs.

Answer: [a] Cable television networks

Module:4

Reference No:M4253

Question: In an Integrated Services Digital Network Basic Rate Interface, the ----channel is used to transmit data

- [a] C channel
- [b] B channel
- [c] D channel
- [d] A channel

Module 4- ISDN Part-2

ISDN is the abbreviation for Integrated Services Digital Network. It is a kind of digital telephone service that is an up gradation over the copper telephone wiring. There are many types of ISDN services. But in this article we have focused on the most appropriate type for individual users. It is called the ISDN Basic Rate Interface. Most of today's telephones are digital. Earlier, the only non-digital part was the connection from the house or office to the local exchange. With ISDN even that has been made digital.

Advantages of using ISDN services

A few advantages of ISDN services are:

1. ISDN has upgraded today's analog telephone to a digital network just as compact discs have upgraded the recorded music.
2. It can operate up to 128 kilobytes/second, which is five times more than today's analog modems.
3. It can increase the speed of transfer of information over Internet or even remote LAN connection even for information like graphics, video or audio, which are usually transferred at LAN speeds.

Limitations of using ISDN services

1. ISDN services is not yet available everywhere. As such unlike analog services, the availability becomes the main issue.
2. Since it is a digital service it is very sensitive to outside interference. The user must be within a given distance from the equipment company that serves the user.
3. There cannot be any other inconsistency near the wiring that could interfere with the transmission. As a result it may not be possible for everyone to get an ISDN service. To determine whether a particular line is suitable for the ISDN services, normally the telephone company will perform what is known as line qualification testing.

Some companies may offer something called ISDN anywhere. In this case even if the telephone company does not have the right equipment at the local central office, they might use the line extension technology to get the ISDN services wherever the user is. This might significantly increase the cost of the ISDN service.

The total cost of ISDN services has three parts- a one-time installation charge, a recurring monthly charge and the usage charge -which is based on the usage of ISDN line.

ISDN Basic Rate Interface

In this type the telephone line is divided into 3 channels. Two "B" channels and One "D" channel. Each of the channels can be used simultaneously. The B channels are used to transmit data and the D channel does the administrative work. The data transfer can be either at 64k or 56k, which again depends on the telephone company. The administrative work involved could be setting up calls or breaking the calls and communication with the telephone network. Since there are two B channels two calls can be made simultaneously.

In the next part of the article we have described the configuration and details about the various components that are utilised in this service.

Answer: [b] B channel

Module:4

Reference No:M4254

Question: In an Integrated Services Digital Network The U interface carries signals over a ----- pair of wires

- [a] Single
- [b] Two
- [c] Multiple
- [d] Two or multiple

Module 4- ISDN Part-3

Configuration of ISDN basic rate interface

There are various issues involved in the configuration of an ISDN line. Configuration is required from the telephone company as well as the user. Configuration at the telephone company end is called the

"provisioning". Various options are available and unlike an analog line all choices must be defined in order for the line to function. Among the various options, is PC connectivity and Virtual Epabx services.

Configuration at the user end

There are three components involved in the configuration of ISDN at the user end. They are

1. Switch type
2. Phone numbers
3. SPID(s) - Service Profile Identifier(s)

Switch type

ISDN hardware adapters must be made compatible to the type of switches. The switch type denotes the brand of equipment and the software level that the telephone company uses to provide the ISDN services. There are only a few types of switches available now. And in countries apart from United States there might be only one type of switch available.

Phone numbers

In some cases both the B channels will have the same number and in certain cases each B channel might carry a specific number. The telephone company usually intimates how many numbers the ISDN line will have. Separate numbers can be chosen if the user plans to take the incoming calls on the ISDN line.

SPID(s) - Service Profile Identifier(s)

This helps the switch understand the type and kind of equipment attached to the line. And if there are multiple devices attached, this identifier helps in routing the call to the appropriate device on the line. This is applicable only to users in United States and Canada.

ISDN adapters

Two types of hardware adapters are available -internal and external. Internal adapters are put inside the PC. The external adapters are connected to the PC by a port.

□ Internal adapters

To install an internal adapter, a free slot is required in the PC to support the same type of Bus. The performances of the internal adapters are generally higher than internal adapters

□ External adapters

These can be easily connected to the PC. These do not require any special software. These can be plugged into both serial and parallel ports. But there are certain limitations imposed by these ports. Most of the serial ports cannot transmit information faster than 115 kilobytes per second, which is lower than maximum speed of 128 KB.

ISDN interfaces

There are two types of ISDN interfaces- the U and S/T interfaces.

□ U-Interface

This carries signals over single pair of wires between the location and central office. This interface can carry signals over long distance.

□ S/T Interface

This is the abbreviation for subscriber/Termination interface. This uses two pairs of wires to deliver the signal from the wall jack to other equipment.

Answer: [b] Two

Question: Which among the below is a security threat to a Wi-Fi wireless LAN?

- [a] War driving
- [b] DMZ (Demilitarised Zones)
- [c] CSMA (carrier sense multiple access)
- [d] Complementary Code keying (CCK)

Module 4- Security issues of Wi-Fi

What is Wi-Fi?

A high frequency WLAN (Wireless LAN) is termed as Wi-Fi or wireless fidelity. It comes as an IEEE (Institute of Electrical and Electronics Engineers) 802.11b specification standard. It finds wide applications as an alternative to wired LANs and in home networks. Wi-Fi uses the Ethernet protocol and deploys the CSMA/CA (carrier sense multiple access with collision avoidance) technology.

Working Range

Wi-Fi works on the 2.4 GHz range and employs Complementary Code Keying (CCK) modulation. This modulation is a development over the conventional phase-shift keying (a digital signal transmission and reception technique in which the phase of the transmitting signal is varied to carry information) PSK, used in 802.11. CCK modulation offers the inherent advantages like higher speeds upto 11 megabits per second and is more immune to multipath-propagation interference.

Security issues

Wi-Fi wireless LAN is vulnerable to security breaches as unauthorised users could access it. This occurs from outside the network in order to use it as a free Internet connection. Since, many of the wireless LANs have ranges beyond an office building, an intruder can easily get into the network and obtain a free Internet connection. Access to company records and other confidential data is also possible in such an intrusion.

There are two different activities that form a potential threat to a Wi-Fi wireless LAN. They are commonly termed as:

1. War driving
2. War dialing

War driving: The process of locating and establishing connections with wireless local area networks while driving around a fixed geographical area or a city is termed as war driving. All that is necessary for war driving is a vehicle, a laptop, a wireless Ethernet card (in promiscuous mode) and an antenna that could be surmounted on the vehicle. With the use of an omni-directional antenna and a Geographical Positioning System (GPS), the war driver can map the locations of Wireless LAN access points.

War dialing: The usage of a computer program to identify the phone numbers that can connect with a computer modem is termed as war dialing and the program is called as war dialer. The war dialer dials a defined range of phone numbers. Then it logs on into a database and records the numbers that could successfully connect to the computer's modem. In some cases, the war dialer attempts a predefined list of usernames and passwords in order to gain access to the systems. These programs are capable of identifying the specific operating system running on the host computer and can conduct penetration testing (the act of checking with some permutations & combinations of names and passwords). Commercial war dialers are also known as modem scanners. In some cases, even system administrators, for the purpose of identifying

unauthorised modems on an enterprise network use modem scanners.

Security measures: Wired Equivalent Privacy (WEP) encryption standard, usage of a virtual private network, IP Sec (Internet Protocol Security), firewalls or DMZ (Demilitarised Zones) are some of the possible ways of countering the threats to Wi-Fi.

Answer: [b] War driving

Explanation: War driving, since the other techniques make up the building block of a Wi-Fi wireless LAN and also cater to security

Module:4

Reference No:M4256

Question: Which of the following makes WEP vulnerable?

- [a] RSA Security Algorithm
- [b] Network Interface Card (NIC)
- [c] Static keys
- [d] Shared secret keys

Module 4 – WEP (Wired Equivalent Privacy)

What is WEP?

Wired Equivalent Privacy (WEP) is a security protocol that was developed for securing the IEEE 802.11b Wireless Fidelity (Wi-Fi) standard. Framed as an equivalent to the level of security and privacy provided by the wired LAN, it comes as an optional encryption standard. It is accommodated in the media access control (MAC) layer or the physical address layer found in almost all radio network interface card (NIC) and access point vendors support. MAC is the layer that manages, maintains and coordinates different access points in a wireless network to enhance communications over a wireless medium. Hence, MAC is often known as the brain of the network.

Mechanism

Physical security mechanisms that have controlled access to a building are most appropriate to a wired local area network. They provide protection and security. In the case of a WLAN such methods become ineffective since the walls containing the network do not bind radio waves. WEP is aimed at establishing a similar protection like a wired network's physical security layer. This is achieved by encrypting data transmitted over the WLAN. First the encryption is done to protect the vulnerable wireless link between clients and access points. Other inherent LAN security mechanisms like authentication, password protection, end-to-end encryption, and virtual private networks can then be deployed to ensure privacy and security.

How does it work?

When a user enables WEP, the Network interface card (NIC) encrypts the data of each 802.11 frame before being transmitted by using RSA Security (An algorithm based on the use of a random permutation). At the receiving end station, which could be an access point or another radio NIC, the algorithm is decrypted on arrival of the frame. So WEP only encrypts data between 802.11 stations. WEP doesn't come into the picture as a frame enters the wired side of the network (For eg. between access points). WEP employs a shared secret key of 40 or 64-bit length to encrypt and decrypt the data. In certain cases, vendors use 128 bit keys, called WEP2. The receiving station must use the same key for decryption. This requires that each radio NIC and access point is manually configured with the same key.

Security Goals

The WEP protocol was framed to address three main security goals, namely confidentiality, access control and data integrity. Checking casual eavesdropping ensures confidentiality. An optional feature that discards all data packets that are not encrypted properly ensures access control. To preserve data integrity a checksum field that prevents tampering of transmitted messages is introduced.

Security lapses

Relatively short Initialisation vectors (IVs-Numerical sets used in encryption) and static nature keys makes WEP vulnerable to hackers. 24 bits are used so the same IV is deployed for different data packets. 802.11 has no provision for any functions that allow the exchange of keys among stations. Therefore, system administrators and users use the same keys for weeks, or months and in some cases even years. Intruders thus get ample time to monitor and hack into WEP networks.

Answer: [c] Static keys

Explanation: Short Initialisation vectors (IVs-Numerical sets used in encryption) and static nature of the keys makes WEP vulnerable to hackers

Module:4

Reference No:M4257

Question: Which of the following is the application core of an Unified Communications?

- [a] Directory profile
- [b] Personal Assistant
- [c] PSTN
- [d] IP

Module 4 - Unified Communications

What is Unified Communications (UC)?

Unified communications (UC) is a development over unified messaging (UM). . The service it provides is a combination of voice (voicemail & faxes) and email (IP-data environment). Unified communications is a modification over unified messaging. Integration of UM with advances in wireless connectivity and converged networks capable of handling data, voice, and multimedia communications resulted in UC.

Concept

Unified communications is about networking people, not just devices. Anyone with access to a network (through a laptop, desktop computer, cell phone, land-line phone, pocket PC and the like) can have a personalised Web content. With this they can access telephone calls, online chat, email, voicemail, and faxes.

Functions

In a unified communications network integration of voice, data, and fax functions with advanced IP features take place. Hence, it requires a uniform platform to manage the flow of data to all communications forms . Necessary functions include management of incoming and outgoing calls from multiple mediums from any terminal type, sending and receiving data of any medium from any terminal type, performing media conversions from one form to another when required and allowing user addresses.

Network Structure

The two structures that make a UC network are

- *Directory profile:* This forms the core or centre of a UC network. It serves as bridge between the Public Switched Telephone Network and IP networks. These UC applications provide the medium for incoming and outgoing calls and data transmissions. They also control the flow and format of the data so as to allow users to access all UC functions with the help of the personal assistant.
- *Personal Assistant:* It is the application core, in the form of an inbox and can store any type of message. A personal agent that manages all incoming calls, other data for the user, and notifications wraps this inbox. With their personal devices that access network services, content and their personal profile users can log into the next generation networks.

Developments

Legacy systems, proprietary technologies and the want of intelligence in the network and access devices have come as a cropper for the acceptance of unified communications. With advanced technologies enterprises have understood the need for consistent standards and limitations are dwindling . The devices enable them to interact with new high-speed 3G wireless networks. Also manufacturers are creating newer innovations and techniques to advance the capabilities of access devices. Next generation switches designed with the intelligence features are bludgeoning the market with enhanced capabilities of converged networks.

Unified communications have a great potential to become a standard that will save time, increase productivity, and allow seamless exchange of information from any location across the world. This is quite possible as messaging technologies are merging with the tools used in business and daily lives, along with new technologies like SOAP (Simple Object Access Protocol) and WAP (Wireless Access Protocol) that provide new levels of interactive content.

Answer: [b] Personal Assistant

Module:4

Reference No:M4258

Question: Which of the following features of Authenticated Virtual Local Area Network simplifies network administration?

- [a] Authentication server
- [b] Authentication agent
- [c] Segmentation
- [d] Network usage card

Module 4 – Authenticated VLANs (Virtual Local Area Network)

Introduction

The increase in network traffic and participation of customers, remote users and vendors has made it mandatory to address the issues of security in a business environment. Security has to be ensured in all network layers and its components. An internal mechanism aimed at enhancing the security of a network is Authenticated VLAN.

What are VLANs and Authenticated VLANs?

A switched network that comes as a logical collection of components grouped together in a common broadcast structure is a Virtual LAN (VLAN). In a VLAN setup, a network administrator can divide the network into different entities that perform optimally and are easily manageable.

In order to achieve network authentication a VLAN based on user's identity called Authenticated VLANs was developed. Here the end users have to identify themselves in advance to gain access to the network. After

authentication, a switch-based packet filtering of data is enabled to take control of the users access to other subnets and services. This gives an authorised access to the network as the services reside in layer 4 and subnets in layer 3 of the network protocol layer.

Administration

Event logging records are maintained in A-VLANs, which furnishes details like what, when and where a user has performed any operation in the network. Such information is used to tune a network for optimal performance, monitor-billing applications and to identify potential bottlenecks. Logging further aids the administrators in ascertaining the problem as specific to a user, VLAN or some other network entity and ensures proper tracking of the users in the network. A-VLAN has segmentation capabilities that simplify network administration. Networks can be designed so that mobile users can access resources from anywhere without any lapses in security.

Operations

In an authentication state, a user has no network privileges until the three-step process takes place as below:

Initiation: The identification of the end user

Authentication: The validation of the user's identity

Authorisation: The assigning of user's privileges

The three components that make this process possible are:

1. **Authentication server:** This server provides user authentication, communicates and delivers the users authorisation to the switch, and ensures usage accounting of the authentication and authorisation activity.
2. **Authentication agent:** The part of the software that is found on the switch's management module is the agent. Its main function is to communicate with client and the server to ensure authentication. As and when the authentication is successful, the agent gets the authorisation for a particular user or the network
3. **Authentication client:** The client allows the users to present their identification credentials. Then access to the network is possible. A variety of interfaces for the user like telnet, web-based and windows applications are also applicable in some VLAN solutions.

Benefits

VLANs enhance wireless LAN security through segmentation and authentication. So, they can be deployed for mobile users applications. In telecommunications, carrier-provisioning services can be defined for different customer classifications. Others benefits are:

- Provision for network usage card
- Enhance network security without any trade off with performance
- Differentiation into manageable entities
- Proper network administration

Answer: [c] Segmentation

Question: Which of the following does not come under privacy of the user?

- [a] User location
- [b] User information
- [c] Conversations of user on mobile
- [d] The mobile handset used by the user

Module 4 – Privacy in Mobile Communication Systems

The Mobile communication systems enable easy access to telecommunication services from any part of the world. This demands high protection of network and subscriber assets against unauthorised usage. The security in a wireless network is vital than in a wired network. This is because a wireless communication is more vulnerable to eavesdropping and tapping. Again, because of its wireless nature, it is difficult to such happenings.

General architecture of mobile communication system: The user is connected to the network through air-interface. Such a connection is established through the radio port. The communication between the mobile station and the fixed network also takes through this port. The user is registered with the service provider who has the billing information and the location information. The service provider is connected with roaming service provider, which facilitates the user to communicate when he is out of his home network.

Privacy issue

Before designing a concrete system to secure the mobile network, the issues related to privacy are first defined. Privacy of the mobile communication users can be set at any of the four levels.

1. *None:* This indicates no privacy at all. Anybody equipped with a scanner can easily monitor the call or data. Such systems must be equipped at least with a privacy indicator, which alerts the user of insecure call . The indicator could be a simple beep tone, which lasts for 15-20 seconds or a message tone warning of the insecure line.
2. *Wired equivalent privacy:* This states that the level of privacy in a wireless communications network should be equivalent to that of wired network. This category covers general conversations of people especially those of personal nature. A cryptographic system is used for this purpose.
3. *Commercially secure:* This level covers the more important aspects of conversation, which could be transactions, or exchange of proprietary information such as contact negotiations, mergers, acquisitions, stock transaction and the like.
4. *Military/government secure:* The military or government departments would use this level.

Requirements for end-user privacy

The subscriber requires privacy or security in the following areas:

1. *Security for call setup information:* During the call setup process, the mobile instrument communicates a lot of information to the service provider. These could be calling party number, calling card number, service requested for etc. Information such as these should be protected and secured against eavesdropping.
2. *Security for speech:* The conversations should be properly encrypted against being intercepted by any eavesdropper.

3. *Privacy of data:* Wireless networks with a high bandwidth data communication services should be encrypted and should be more secure than the voice security.
4. *Privacy of user location:* The user can be easily located when there is a signal leak in his network and therefore any threat to his privacy.
5. *Privacy of calling patterns:* Information generated about the calling habits of user such as the caller number, frequency of calls made to a particular number etc. should not be made available to the eavesdropper.
6. *Privacy of User-ID:* The user in a mobile network is identified with an ID. This information should be protected from hackers and should therefore never be transmitted over the air-interface.

Answer: [d] The mobile handset used by the user

Module:4

Reference No:M4260

Question: In a PKI audit, the auditor needs to gain an understanding of

- [a] The PKI architecture
- [b] The trust model
- [c] The uses of the certificates
- [d] All of the above

Module 4 - PKI Certification part 2

PKI certification/audit can be understood in two phases. The first phase being the pre-audit phase has been dealt in one of our articles. The second phase regarding the actual audit has been dealt in this article.

PKI Standards

Standards play an important role in the PKI audit/certification. They provide a basis for the auditors to determine the effectiveness and the quality of the PKI standards. Currently one of the most widely used standards for PKI operations is the American National standard (ANS) X9.79: 2000 PKI practiced and policy framework. This was adopted by the AICPA/CICA Electronic Assurance Task force, for its web trust program for CA. This web trusts program provides specific audit guidelines for CAs and is now most widely used by professional accounting organisations worldwide. And also ISO is developing an international standard for PKI based on the input by X9.79. But X9.79 is rapidly gaining international recognition, for instance it is adopted by Microsoft and referenced by host of other professional bodies like American Bar Association, European Telecommunications standards Institute and the like.

The audit process

The entire audit process has been described in three stages

Stage 1 pre-audit stage

This stage consists of planning phase. At the end of this stage the auditor should have a well-defined audit plan to proceed with the audit. This stage requires gaining an understanding of:

1. The CA's operations
2. The PKI architecture

3. The trust model
4. The existing users of the certificates
5. The uses of the certificates
6. Volume of certificates handled
7. Certificate validity periods

This stage also consists of reviewing the following documentation

1. CP and CPS documentation
2. PKI strategy documentation

The last and final activity consists of confirming the scope and objectives and the appropriate standards and the reporting format to be utilised for the conduction of the audit.

After all this, the auditor will now be in a position to draw up an audit plan for the commencement of the audit.

Stage 2 Actual audit stage

This stage consists of the actual test procedures. A sample checklist and test procedures has been dealt in part 3 of this article. The extent and the focus of the testing procedures will depend on the scope of the audit. If the audit is focused on the sufficiency of the procedures for a point of time then audit will be focused on existence of controls for that time. Otherwise the audit will be focused for a period of time.

Reporting

The reporting format depends on the objective of the audit. If it for internal purpose it may take the form of risk assessment. For external purposes it might be prepared like a webtrust for CAs or any other special format if certain local or national standards prescribe the same. One of the most commonly utilised report formats is the webtrust for CAs format wherein the procedures are conducted by auditor to determine if the webtrust guidelines have been complied with. PKI certification based on X9.79 standards or webtrust regulation may provide additional legal status for the CAs to issue qualified digital certificates.

Answer: [d] All of the above

Module:4

Reference No:M4264

Question: Which of the following is not a Peer-to-Peer networking?

- [a] Gnutella
- [b] Freenet
- [c] Linux
- [d] Napster

Module 4 - Types of Peer-To-Peer Networking

A Peer-To-Peer network is the one in which each workstation has the same capabilities and responsibilities, unlike the client to server architecture where some computers are dedicated to serve other computers. That means each system functions both as server and a client. Although it existed from the time when networking of computer started it gained momentum only recently. On the Internet, P2P is a type of transient Internet network, which allows a group of computer users having the similar networking program to connect to each

other and directly access files from one another's hard drives. This facilitates users to search network file database, share files directly from another system without requiring any server. There are different types of peer-to-peer networks owing to the difference in the protocol. are .

Gnutella

Each computer acts as both client as well as a server and therefore does not have any centralised server. Lets presume there are three machines A, B, C, which have formed a network wherein A is connected to B and B is connected to C. A searches for a file and sends a query to B. If B doesn't have the matching file then it sends the query to C. If A has the file then A connects to C and shares the file.

It is essential to know the location of the servers to provide a link to Gnutella network although it's not a part of Gnutella Protocol. This type of P2P networking model decreases reliability, speed, and search capabilities, and increases network traffic.

Napster

Unlike Gnutella, the Napster P2P networking model requires a centralised directory server. The client, say A first communicates with a directory server. The Directory server responds with a message and registers availability of A along with the other clients connected to it. When a client B sends a query for a certain file to the server, the server responds with a list of all the clients having that file. When client sends a request for file in client A, the server sends information about client A such as the IP address and listening port. Then client B connects to client A sends the file request and responds with the file.

Freenet

This is similar to Gnutella. The users in this network do not have absolute command over the content in their shared space (datastore) but only the amount of space. The client inserts a file, which is encrypted and broadcasted over the network with a unique key identifying the file. Suppose the client A requests a file from servant B, it in turn checks for the clients that have the closet key. Let us suppose it finds client C with the closet key requested by client A. Client C again searches for closet matching key. On finding client D with exactly matching keys it requests for the file. Client D responds to client C with the file, which in turn responds to client B, which again responds to client A.

The main advantage of P2P computing is that it reduces the dependence on centrally managed server. This helps reducing the cost of maintaining the infrastructure. Since the P2P requires a distribution of network and computational resources, it results in fewer bottlenecks and shorter distances for messages and data to travel.

Despite all its advantages it has its share of drawbacks too. If a person accessing important information from a workstation and the workstation is suddenly shutdown, it results in loss of data.

Another critical problem is that of virus, which could again easily infect a computer when an infected file is downloaded by mistake.

Answer: [c] Linux

Module:4

Reference No:M4265

Question: Which of the following is a feature of Second Generation architecture?

- [a] Data is transmitted in an encrypted form over the networks
- [b] Communication is flexible and can be upgraded
- [c] Data integrity is absent
- [d] The base transceiver station is strong and cannot be easily controlled

Module 4 – Third Generation Architecture

The Third Generation has evolved due to the demand for a 3rd Generation Mobile System based on GSM core networks and the supported radio access technologies.

3G Architecture

All the network components are listed into three units.

1. User equipment (UE): It has two parts viz.,
 - a. Mobile station (MS): It is the radio terminal used for radio communication over User Interface.
 - b. User services identity module (USIM): It is a smart card which has information such as subscribers identity, authentication algorithms and is used to store authentication and encryption key and subscriber related information.
2. Radio access network (UTRAN): This manages all the radio-related functionality. It has two distinct logical elements
 - a. Node-B: It basically converts data flow between interfaces and partly handles some of the radio resource management.
 - b. Radio Network Controller (RNC): It owns and controls the radio resources in its domain.
3. CORE Network (CN): This is responsible for switching, routing calls and data connections to external networks. The main elements of CN are:
 - a. Home Location Register (HLR): It's a database that stores the user related information such as services the user is authorised to avail, permitted roaming areas, and other call related services such as call-forwarding .
 - b. The Mobile Switching Centre (MSC)/Visitor Location Register (VLR): The switch (MSC) is used to switch the circuit switched (CS) services and the VLR is used to store the information about the user's service profile and the precise location of the UE in the serving network.
 - c. Gateway Mobile Switching Centre (GMSC): It is the switch where the UMTS PLMN is connected to external CS networks. All the incoming and outgoing CS connections must pass through GMSC.
 - d. The Serving GPRS (General Packet Radio Service) Support Node (SGSN) is similar to MSC/VLR but is used for Packet Switched (PS) Services.

3G security principles

The 3G architecture was designed based on three fundamental considerations:

1. The security features of second-generation system would provide the foundation for the security architecture of 3G.
2. The security of the 3G systems will be an enhancement over 2G systems.
3. 3G security will have new features and will secure new services on the basis of 3G.

Weaknesses of 2G security systems

1. The base transceiver Station (BTS), which provides connectivity between the network and mobile station, could be easily controlled. This is because the mobile does not check the authenticity of BTS before establishing connection.

2. The cipher keys and authentication data are transmitted without being encrypted between and within networks.
3. Data integrity is absent.
4. 2Gs are not flexible for upgradation.
5. The home network is not aware of the parameters through which the serving network authenticates the mobile station for roaming subscribers.

Answer: [c] Data integrity is absent

Module:4

Reference No:M4266

Question: When Mobile users travel from their home network to other network

- [a] They cannot access any mobile services
- [b] They have to take permission from the new network for mobile
- [c] Users are to be permitted by their home network
- [d] Users have to take a new connection

Module 4 - Privacy And Authentication Techniques For Mobile Communications Users

Authentication and security are two very important aspects of mobile communications. Authentication is essential to defend the network assets from intruders and Privacy is essential to protect the subscriber assets.

Privacy and authentication are taken care of in two different stages.

1. *Authentication and key agreement (AKA):* In this process, the network checks the identity of the mobile user and a session key is generated for encryption. This is the most important stage because the session key once established can be used directly to develop an encrypted connection.
2. *Encryption for privacy:* In this process, the session key generated from the previous stage is used to encrypt the user traffic for absolute privacy.

Authentication and key agreement (AKA)

This process takes places in three stages:

1. Provisioning:- During this stage, the subscriber with a personal handset is recognised as a legitimate user of services.
Provisioning is done through
 - i. GSM (Global system for mobile communication) by using "smart cards" also called SIM (Subscribers Identifier Module) cards. The SIM card is issued when the user purchases the service from the service provider and contains information about the services purchased and a 128-bit number called Ki. Ki is unique for each SIM, enabling the network to authenticate the user.
 - ii. Provisioning can also be done using A-Key, which is a 64-bit value issued to the subscriber in a confidential manner. The user enters this security parameter in the handset using keypad while the security software in the handset checks for its veracity. The service provider in home network also stores this number. A security variable, Shared Secret Data (SSD) is also derived from A-Key. This is shared between the network to which the user belongs and the network which the user visits.

2. Support for roaming: This comes into play when the user has to authenticate his identity to a local network, which may not be his home network. When in home network, the user's data is shared by the servers of the service providers. But when the user moves out of home network and still has to access the services, the serving network should be in a position to authorise and serve him.
Now, the user information is only available at home network and not in the serving network. For this purpose, the Home Location Register (HLR) and Visitor Location Register (VLR) are used. The HLR, at the home network is billing database and stores information related to billing. The VLR, at the serving network is location database and stores the information about the users who roam into the serving network.
3. The final part is the implementation protocol, to permit network access and establish a key for protection of user-traffic. This means the serving network is assured of the services the user is permitted. This is done by sending a random number to the user's handset. The software in the mobile responds by generating a number and a key called session key using an algorithm and the secret Ki number. This is then sent back to the fixed network, which verifies the validity.

Encryption for Privacy

The session-key obtained in the above process is then used to encrypt the user's data traffic so as to provide utmost privacy.

Answer: [c] Users are to be permitted by their home network

Module:4

Reference No:M4267

Question: Which of the following limitations of using Gigabit Ethernet has been addressed by a better bus architecture?

- [a] Processing power
- [b] Peripheral Component Interconnect (PCI)
- [c] Cost
- [d] Storage

Module 4 – Gigabit Ethernet: To the Desk

Introduction

With increased applications in a networked environment, users felt the absolute need for value-added features and high speed from their computers. Local area networks (LANs) came as a blessing for individual users to hook up with each other so they could do more and share information. Despite this, as applications and data files grew in size, the demand for increased network speed also grew sharply. This saw networks increasing from a meager speed of 4 Mbps of token ring to 10 Mbps, then to 100 Mbps, and now Gigabit levels through Gigabit Ethernet (GigE).

As speed and the size of applications increase, there is a need for much faster networks. To serve this need, faster speeds have been developed and used for network backbones. Core-networking equipment is capable of 40-Gigabit range speed, though but the typical desk's access capability is only about 100 Mbps. Gigabit Ethernet NICs (network interface cards) for desk computers -- which have been available for years-- are mostly deployed in server class computers.

Limitations on desk applications

The average desk computer is not designed to handle the full bandwidth. This poses a problem on the following design limitations:

- Interface that exists between the Gigabit Ethernet card and the 32-bit peripheral component interconnect (PCI) bus of a computer does not have the speed to pass all the data from a gigabit link.
- Data packets that form an overhead utilise a disproportionate processing power, thereby slowing down the performance of a desk computer drastically.
- Storage media like hard disk drive and memory do not match the process data in speed
- The c involved is very high and an average user never fully uses a gigabit of bandwidth.

Solutions

- The communication between the Gigabit Ethernet expansion card and the PCI bus was a problem since the 32-bit 33 MHz PCI bus could only handle 133 Mbps of bandwidth. Recent advances in bus architecture can upgrade the 32-bit PCI bus to a 64-bit architecture operating at 66 Mhz. Intel has introduced a 64-bit bus operating at 133 Mhz. A faster PCI bus with a bandwidth of 64 bits can accommodate the current bus architecture to support speeds up to 1,000 Mbps.
- The slow rate of data transfer between the CPU, the memory and the hard disk drive are two more problems. As a Gigabit Ethernet card operates at one gigabit, the desk computer could only process 200 to 400 Mbps, wasting potential bandwidth and money for speed that could not be accessed. Advances in microprocessor technologies have enabled Pentium and Xeon processors by Intel to come up with high speeds that can run on Double data rates (DDR) to counter this.
- Newer invention, standardization and specifications of copper Gigabit Ethernet adapters have reduced the cost of a desk adapter considerably. The price per port of a gigabit in core and edge switches continue to reduce as GigE becomes a more feasible option, even for small and medium enterprise businesses.

Answer: [b] Peripheral Component Interconnect (PCI)

Module:4

Reference No:M4269

Question: ----- standard defines a way of using XML to describe other XML documents

- [a] XML Schema Instance namespace
- [b] XML Schema for Data types
- [c] Web Services Meta Language
- [d] XML Schema

Module 4 - Web Services Standards

Web Services are based on a number of XML standards, some of which are not easy to understand. It is especially more challenging if you haven't had a taste of XML before. However, all these standards are simple representations of information necessary for the discovery, invocation, and description of Web Services.

The following are some of such standards and its uses

XML Schema

This is a standard that defines a way of using XML to describe other XML documents. It puts in force a check on type and constraints on allowable elements and attributes of a document. XML schemas are not required for all Simple Object Access Protocol (SOAP) implementations. Most of them, however, use them to perform checks while making method calls on Web Services.

XML Schema Instance (XSI) namespace

This namespace declares the type attribute that SOAP messages often use to define the scope of data types, parameters and their return values.

XML Schema for Data types (XSD)

It is the namespace that most implementations use to refer to the main XML Schema definition that contains all data type definitions used by the standard.

Web Services Meta Language (WSML)

This is another XML-based document format used by some Web Service tools. Microsoft SOAP Toolkit is one such tool. It provides mappings between Web Service methods and their parameters. It also relates them to underlying code objects such as COM components.

Web Services Discovery (Disco) tool

Disco is an XML document format that contains entries that point to WSDL resources describing available Web Services. Disco simply provides a way to centralise the listing of multiple Web Service providers into a single document. Tools use this to select the desired Web Service and obtain a reference to it.

The above Web services standards act as a foundation. They allow companies to describe services, register them in a directory to be located, and then use these services through a range of platforms. The second phase is expected to focus on security.

However, the evolution of standards has been quite consistent. Further, they are being blamed for a number of failures. Another issue of contention is SOAP interoperability. The protocol cannot be used for sending transmissions concurrently to multiple recipients. SOAP also cannot support complex transactions; instead it is more suited for the request and reply types.

Phase Three is where Web services will be used for workflow and systems management. However, there's a lot to be done before that happens.

Due to shortcomings in the existing standards, Web services aren't expected to make it to the enterprise just as yet. The standards need to become more cost effective, in terms of implementation and maintenance if they are to improve. Companies are looking at bringing in new standards that incorporate issues such as authentication, reliable messaging and security.

Answer: [d] **XML Schema**

Module:4

Reference No:M4270

Question: Which of the following is a feature of Hybrid systems?

- [a] Centralised server, example Napster
- [b] Centralised server, example Gnutella
- [c] Centralised server and peer to other servers
- [d] Centralised server and no downloading capability

Module 4 – Super Peer Networks

A super peer can be defined as a node, which acts as a server to a group of clients and as a peer in a network of super-peers. A super peer network serves the purpose of a centralised search, load balancing, robustness and the like in a peer-to-peer network. It also helps in making use of the available bandwidth, processing power across the peer network.

In general, there are three types of peer-to peer networks. **Pure system**, in which all peers have identical roles and responsibilities such as query, download and the like. Gnutella, Freenet are examples of pure

systems. **Hybrid systems** perform search over a centralised directory, but downloading of files occur in a fashion similar to pure system; therefore, peers are identical only in download feature. Napster is a Hybrid System. **Super-peer system** is a combination of pure system and Hybrid system. It functions as a centralised server to a set of clients. When a client submits a query to a super-peer, it receives results from it like in any other hybrid system. Nevertheless, just like pure systems, super-peers are also interconnected, route messages over network, submit and answer queries for clients and themselves. A super peer is therefore equivalent to other super peers with respect to search and all peers are equal in terms of download. A super peer network is therefore a network of super peer and its clients.

Why Super peer network?

In spite of all their strengths both pure systems and Hybrid systems have their disadvantages. The pure p2p systems become inefficient when the network is flooded with query messages and when bottleneck arises due to limited capabilities of some peers. This was generally caused due to users with dial-up modems, who were inundated by increased load, disappearing and disintegrating the network while leaving the system. One reason was the equal roles and responsibilities allotted to every peer.

Hybrid system, incurred huge costs for housing a single node for centralised index. It also gives rise to performance and scalability bottleneck due to the heavy load it has to bear. They are also susceptible to hacking and attacks, as bringing down of one system would bring down the entire network.

So a network is required, which apart from having all the advantages of pure systems and hybrid systems, should be equipped with features so as to tackle the weaknesses of the above systems too. Here, super peer comes into play. The super peer has centralised search and can therefore act as a centralised server for its clients, reply queries with more efficiency. Since there are a lot of super peers in a network the load is distributed to other super peers also, thereby reducing the potential bottleneck. Also, since there isn't a single system, which act as centralized server, the chances of bringing down the entire network is also decreased.

Answer: [a] Centralised server, example Napster

Module:4

Reference No:M4271

Question: Which of the following statements is true with regard to web services?

- [a] Web services are based on XML standard
- [b] Web services requires a visual interface to the user
- [c] They are standalone tools
- [d] None of the above

Module 4 – Web Services

Web Services, a breakthrough technology, is going to revolutionise the way the software applications are built. The main idea behind these services is the integration of the processing power of computers with the omnipresence of the Internet.

A Web Service is a business function that is made available online to customers or partners via an XML-based interface. Web Services make integration part of software's basic architecture. They have the potential to alter IT spending of many industries. They would also significantly enhance the value of existing software investments.

All major software companies are taking to Web Services in a big way. Microsoft is providing tools and infrastructure to create, deploy, and manage Web Services through Microsoft .NET. Rival, Sun Microsystems has also entered the arena. The Open Net Environment (Sun ONE) is being sold as the company's platform

for Web Services on Demand.

Importance of Web services

- Web services are based on an open XML standard. Thus, if an application can access one Web service, it can access any one of them.
- Web services are basically composed of functions. So, they do not have to present a visual interface to the user
- They are available throughout the Web and so we have applications that can access different functions and diverse information across the globe
- They break down geographical barriers because using the Internet as a carrier makes the actual location of a service immaterial. Also, Simple Object Access Protocol (SOAP) provides a single mechanism for accessing data

Web Services allows to create applications that accomplish more complex tasks than software packages can achieve. Distributed systems can be accessed through standard Web Service interfaces. They provide new ways of building applications without being at the mercy of the overworked IT department.

With Web services, software application code becomes much more reusable. Once a particular service is written, connected device or software can use it. Also, it is easier and more economical to integrate applications with existing solutions than to rewrite them. The standards that surround Web services allow companies to use the 'power of reuse' like never before.

The ability to use standardised components for software development will be a pioneering methodology. Just like the transition from hand-built products to assembly line ones did in manufacturing. It will be faster, cheaper, easier, and far more efficient. Secure and free flow of data can make it possible to reach or service more customers and establish many new partnerships. Also, Web Services not only reduce IT costs, but also business and transaction costs as well.

Problems

Unfortunately, despite all the benefits of Web Services, a number of problems act as a deterrent to its widespread adoption. The most prominent among these is reliability; the Web still is infamously unreliable. Applications relying on several Web Services are thus vulnerable to the failure of any one service. Web Services are provided by external businesses. Thus, the customer has no control over server load or any other unreliability.

There is another problem. Since Web services are not standalone business tools, they are incomplete without applications that use them. On the other hand, applications that rely on specific services will not be created until an abundance of such services exist. A final and more prolific challenge being faced by Web Services is the lack of standardisation of subscription and authentication. Customers need to specially implement each Web service call to support different service providers' methods of authentication.

Answer: [a] Web services are based on XML standard

Question: Where do traffic shaping parameters feature in a voice network?

- [a] Software Stability
- [b] Redundancy
- [c] Protocol Resilience
- [d] Distributed Intelligence

Module 4 – Voice Networks – Availability Issues

Introduction

Voice networks have emerged as a major source for conducting businesses in an enterprise. Small delays in voice communications usually leave a severe impact on one's business. Besides, network downtime results in a variety of losses in terms of monetary, business critical communications, corporate image and customer confidence. There is an absolute need for a network that can deliver uninterrupted service.

What does availability mean?

A measure of the ability of network devices to provide resources on demand across the whole network at all times is called availability. With respect to voice communications, availability is termed as a highly available system that gives a dial tone whenever a handset is picked up, without any kind of disruption. In order to ensure availability, a lot of requirements have to be fulfilled. They include careful selection of protocols, equipment, configuration, software systems and management, put together as the "five nines" of availability.

How can one achieve high availability?

A look at some of the building blocks that help to guard against a system failure is the surest means of achieving high availability. They include physical reliability, redundancy, distributed intelligence, protocol resilience, software stability and management.

1. **Physical reliability:** The importance of physical reliability can best be understood with the help of this example: If an engine unit gets overheated after a few hours of usage, it is said not to be reliable. Moreover, if the unit lacks the physical capability to bring redundancy or a power backup, the chances for failure of the engine are greater. Some specific physical characteristics like high Mean Time Between Failure (MTBF), wide range of operating temperatures, modular design, hot swappable components and backup power capability are essential for devices used in highly available systems.
2. **Redundancy:** The most important aspect of availability is redundancy. Stand-by management, line cards and power supply make failure in one component transparent to users.
3. **Distributed intelligence:** Intelligence on traffic-shaping parameters like such as quality of service (QoS), routing services, queuing and other bandwidth management functions are necessary to contribute to high availability. This, in turn, emphasises the need for distributed intelligence. In a nutshell, the distribution of intelligence and call routing capabilities to all nodes in a voice network will pave the way for the system to maintain a minimum level of dial tone service even in case of system failure.
4. **Protocol resilience:** Standardised protocols like TCP/IP, XML, SIP and the like that come under the purview of organisations such as the Internet Engineering Task Force (IETF), the International Telecommunications Union (ITU) and the International Organisation for Standardisation (ISO) must be deployed. These standardised protocols increase the reliability of the system and ensure maximum availability. Proprietary protocol, on the other hand -- if not properly tested and refined -- ruins the integrity of a voice network and causes disruptions in service, thereby putting the business at stake.
5. **Software stability:** The software in a voice system is the primary source of intelligence features to the system. This makes it essential for each software package to be put to rigorous testing by credible sources like third-party companies under real world conditions. The result gives a true understanding of

the stability of the product. It is important to look for accreditation from reputable organisations that have performed testing on the voice system.

6. Management: High availability in a voice network for a management system means the ability to reproduce the changes from a single system or node to all other nodes in the network. Therefore, a change made by a system administrator will ensure that the entire network is configured in the same line.

Answer: [d] Distributed Intelligence

Module:4

Reference No:M4275

Question: Which one of the following is used by Simple Object Access Protocol (SOAP) to send and receive data over the Internet: -

- [a] HTTP and UML
- [b] FTP and XML
- [c] HTTP and XML
- [d] FTP and UML

Module 4 – Simple Object Access Protocol (SOAP)

Introduction

Large Internet based applications are distributed over various locations and communication between these distributed applications is a major problem. Traditionally Remote Procedural Calls (RPC) was used to communicate among these distributed objects, which does not support Hyper Text Transfer Protocol (HTTP). Hence HTTP was not able to adapt itself to the Internet. This gave rise to many security related issues. For instance, data traffic was blocked by firewalls and proxy servers installed in the network.

SOAP was developed to overcome this problem.

SOAP

Normally a client requests the server for some specific service and server responds to that service in a specific manner. There are various ways by which this activity is conducted, but SOAP provides a simple way to do that.

SOAP is an Extensible Markup Language (XML) based technology, which supports web services. It is a messaging protocol, which identifies a set of rules and regulations to transmit messages in a distributed and decentralized environment. It communicates the messages between applications formatted by XML via HTTP. SOAP plays a very important role in distributed computing. It is due to the following reasons: -

- SOAP is not associated with any other transfer protocol except HTTP.
- SOAP is not linked to any operating system
- It is language independent.

Since SOAP messages are in XML format it brings with it a number of advantages vis-à-vis messaging protocols. One of the major advantages is that the developer can read the XML message with the help of text editor. This simplifies the debugging process.

Web services under the blanket of XML and HTTP are not enough to provide interoperability among diverse systems. The two major challenges in the way of these web services are: -

- Defining a simple and easy way to deploy these web services.
- Storing the web services and defining methods for the end-user to search for the particular service

In order to overcome these challenges Web Service Description Language (WSDL) and Universal description, Discovery and Integration (UDDI) were developed. WSDL identifies a standard mechanism, which defines a web service in an XML format. WSDL has the ability to convert the message (in any format) using any network protocol into XML document. On the other hand UDDI facilitates identification of other web services operating in the cyber world.

Characteristics of SOAP

- SOAP is a lightweight communication protocol i.e. it does not use transmission Control Protocol (TCP) mechanism for setting up the connection.
- It is designed to communicate through HTTP.
- SOAP is free from any component technology.
- SOAP is appreciated by World Wide Web Consortium (W3C) and is expected to soon become a standard for W3C.
- SOAP is very simple and extensible.

Pros and cons of SOAP

Pros

- SOAP can be made user friendly through natural language bindings. Implementation of language binding makes it easy to use and widely accessible.
- Implementing SOAP is very easy because it can be used on any platform.
- It is firewall friendly protocol. It is one of the biggest advantages of SOAP because it works successfully over HTTP.

Cons

- It is more expensive to encode as compared to RMI/IIOP. SOAP is an ASCII protocol, so all the data should be converted to strings before transmission.
- SOAP needs more memory because most of the memory is wasted in structuring XML strings. In addition to memory wastage it also results in garbage accumulation.
- A programmer needs to write more codes to bridge the gap between SOAP and the objects used.

Answer: [c] HTTP and XML

Module:4

Reference No:M4276

Question: In Web Based Application Development, the term 'shared host' is used for the company when the website is owned and administrated by: -

- [a] Third party service provider
- [b] Associated service provider
- [c] Company itself
- [d] None of the above

Module 4 - Web Based Application Development

Introduction

Applications that depend on the Internet to perform their desired function are known as web-based applications. For example, online stores, universities, or software companies using web based applications either to advertise or to interact with users.

Prerequisites for Web Based Application Development (WBAD)

The following aspects must be considered before one goes in for web based application development: -

- **Technology support:** Since WBAD is Net-based, suitable hardware and software components are required to enhance its performance. Some of them are database software, encryption hardware, network switches, network hubs, multimedia support and many more. Some of the components supporting WBAD are: -
 - o **Switching network:** The Internet makes use of the packet switching technique to transmit messages between the sender and the receiver. The messages are grouped into small packets on which the source and destination path are electronically signed. The router chooses the path of least traffic and accordingly routes messages to the destination.

- o **Protocol:** protocols are a set of rules and regulations used to send data via the Internet. Some of the most important protocols used are TCP/IP (transmission control protocol an Internet protocol), HTTP (hypertext transfer protocol), SMTP (simple mail transfer protocol), POP (post office protocol), and IMAP (interactive mail access protocol).
- o **Domain name and IP address:** In WBAD, address and identification have to be specified. The address is represented in the form of 124.255.192.255., which is a 32 bit number. On the other hand, conventional domain names like www.themanagementor.com. are easy to remember.
- o **Internet connection:** One can connect to the ISP (Internet Service Providers) through such mediums as the dial-up connection, ISDN (Integrated Service Digital Network), etc. Bandwidth is the measure of speed. Larger firms use higher bandwidths and vice versa.
- **Selection of platform:** The hardware requirements of a web server depend on the type of server software one wants to use. It could be: -
 - o **Shared host:** This refers to corporate websites owned and administrated by third party service providers.
 - o **Dedicated host:** In this type of web hosting, the corporate website runs on an individual dedicated server and is administered by a local service provider.
 - o **Self-host:** The website is both, owned and controlled by the online business firm itself.
- **Web server software and tools:** The primary function of server software is to preserve information such as the date, time and URL of each and every request made to the server. The web server software controls the operations from the time it receives client requests to the time the response from the database server is directed to the client. The tools used are as follows: -
 - o Apache HTTP server
 - o Microsoft Internet Information Server
 - o Netscape Enterprise Server
- **Constructing application:** Development tools for a website include HTML, visual web page editor, front page, cold fusion, Dream weaver and many more. Static pages are developed with the help of HTML or front page and dynamic pages with ASP while java applets are used for interfacing with clients. Once the website is complete, it is hosted on the Internet. The final step is site maintenance and management, which includes script-checking, validation, checking links etc.
- **Security:** It is the most important aspect that should be considered for web based application development. It involves securing the website and protecting valuable data from unauthorised access. Other threats in web based application development include virus attacks, insecure communication channels, risk at the server level and so on. Some protective measures such as anti-virus programs, sending the message by digitally signing it, installing firewalls in the network, encryption and decryption standards etc, are necessary to safeguard the system.

Answer: [a] Third party service provider

Module:4

Reference No:M4277

Question: With regard to monitoring intranet performance it is ideal to collect data during

- [a] Peak period
- [b] Non peak period
- [c] Both peak and non peak period
- [d] Either peak or non peak period

Module 4 – Monitoring Intranet Performance

Monitoring the intranet performance has always been a daunting issue for the network administrators. Each of the network assets can be easily monitored through various means but when it comes to reviewing the

performance of the intranet as whole, not much information is available. The difficulty arises with lack of precise definition of what constitutes an intranet.

Steps to monitor the intranet

There are four steps involved in monitoring an intranet. They are

1. Understanding of the environment
2. Determining the business growth that will effect the intranet performance
3. Defining the data collection process
4. Defining the data analysis techniques

Understanding the environment

This involves understanding the entire environment of the intranet, the components and assets it comprises of etc. Intranets may be a simple one, which use only IP software and standards consisting of IP tools like firewalls, Virtual Private networks, load balancers etc. The intranet may also cover different locations connected through WAN.

Users can be interviewed and network diagrams can be studied in order to obtain an understanding of the environment. User interviews may throw light on work patterns, data flows, application information indicating which application is critical to the business etc.

Determining the business growth that will effect the intranet performance

In order to determine the possible growth in the intranet, it is important to determine the growth in business that will have significant effect on the technological aspects in the business. For instances, mergers and acquisitions may have a significant effect. This will not increase the load on the network, but also may bring in new technologies, which are incompatible with the technology used by the organisation. There are many network products available in the market today. The only way to select is to choose those that best serve the purpose of the organisation.

Defining the data collection process

This involves finding answers to three basic questions of when to collect the data, where to collect the data and what data should be collected.

- **When:** It is ideal if data at both peak and non-peak periods are collected. This will give a more complete picture
- **Where:** It is now possible to place the monitoring agents at certain high profile places, which will give a more complete picture of the network usage. In this LAN switches are of great use. In case of server farms, outfitting the server farms will provide all the server information
- **What:** It is practically infeasible to collect all the information for measurement. Only certain relevant ones like application response time to measure the web server transaction processing times. If primary metrics are not available then the company should focus on the secondary data like network response time. Then there are tertiary indicators like number of users on system, network throughput. Metrics beyond tertiary data may just confuse the performance analysis

Defining the data analysis techniques

The last step involved in the entire process is the data analysis techniques. The data analysis should encompass the entire primary, secondary and if applicable, tertiary data. If the indicator is web traffic then the analyst should look at web traffic pattern to identify the peak bottleneck time. Then he should look at the performance time to look at the effect of web traffic on the network. Based on the observations, decision should be taken to improve the infrastructure if necessary.

Answer: [c] Both peak and non peak period

Question: ----- is one of the scopes of the PKI audit/certification

- [a] CA functional disclosures and documentation policies
- [b] Key life cycle management
- [c] Certificate cycle management
- [d] All of the above

Module 4 – PKI Certification/audit

PKI certification/audit can be understood in two phases. The first viz. The pre-audit phase is being dealt in this article. The second phase regarding the actual audit has been dealt in the subsequent article.

Almost all large and medium corporations, which deal with transmission of sensitive information through the public and open network mediums, are utilising the PKI mechanism to secure their data. Users and third party rely on the digital certificates for identification purpose. These parties need an assurance that the public key infrastructure comply with certain quality standards and are effective.

Major audit issues

Some of the major audit issues that needs to be considered during a PKI certification are as follows

1. Proper implementation of PKI and key generation process.
2. Trustworthiness of the systems and procedures.
3. Compliance with requirements of certificate policy and certificate practice statement.

Audit areas

For a thorough insight on the audit scope and methodology, all components of the infrastructure will have to be understood. Separate series of articles are devoted to the concepts and PKI and its services. Given below are the audit areas involved in the certification/audit of PKI.

Abbreviations used

CA - Certification Authority
RA - Registration Authority
Certificates - Digital certificates
User - End users of the PKI

Scope of the certification/audit

Corresponding to the above components the scope of the audit could be in any of the following areas:

1. General IT management regarding CA: This includes ensuring the adequacy of the functional environment of CA that is technical, procedural and policy related controls.
2. Key life cycle management: This includes ensuring the adequacy of technology related controls throughout the life of the keys for security and integrity of keys.
3. Certificate cycle management: This includes ensuring the adequacy of technology related controls throughout the life of the digital certificate.
4. CA functional disclosures and documentation policies: This includes the compliance with the policies and procedures with regard to different types and classes of certificates to be issued, operational

procedures for CA and the communication of the CA policies and procedures to the end users and third parties. Normally the communication is made through a document to the public via documents called Certification practice statement or CPS. And certificate policy or CP. These contain the details regarding the certificates issued and the checks and control measures adopted by the CA to ensure reliability.

With regard to defining the scope of the audit the audit needs to take into consideration the following issues

- a. Whether the CA itself or any external RA agency is carrying RA functions? If so, does the scope of audit include or exclude the services of external RA?
- b. Is the organisation itself issuing the certificate but has outsourced the CA management to a service provider. If yes, has a third party audit been completed for the CA service provider?
- c. Does the scope of the audit include compliance with industry specific standards, regulatory requirements or community requirements?

Audit Objectives

The objectives of the audit could be either to provide

- a. Assurance to the management regarding the effectiveness of the PKI operations and quality of the design.
- b. Assurance to the external parties likes customers, regulators to meet their needs.

Answer: [d] All of the above

Module:4

Reference No:M4279

Question: Access manager in an environment of web portals is primarily responsible for _____

- [a] Speeding up internet access
- [b] Security and authentication
- [c] Data integrity
- [d] Searching information

Module 4 - Web portals and security

Web portals are simply websites from which a user can access information, application and services in any field. Web portals make use of standard technology i.e. browser to access information. During design of first portal (Netscape Navigator), security aspect was not given much consideration. Security features were added later. Security for web portals falls in two categories: -

1. Web single sign-on: For verifying and identifying the user, web portals prompts user for authentication information like user name and password.
2. Authorisation: It will determine what resources a user can access even after authentication.

Access Manager: It is an enterprise level security product that provides a single point of user authentication and authorisation. It is a secure tool for e-business and distributed applications. It minimises the cost for e-business security, addressing growing complexity, implementing security across platforms. Access manager provides authentication and access control services for web resources.

Access manager and web environment: Access manager helps in application integration. There are three level of integration that developers should take into consideration. Each level has its base in the previous level.

1. **Web single sign-on:** It is the first level of integration and it involves configuring of WebSEAL (an access manager component) for any HTTP Web server or application server accomplished with WebSEAL. By junctioning these servers, WebSEAL can provide Web single sign-on access control, high availability of data.
2. **URL access control:** It is second level of integration and involves access control for individual objects on web server or application server. It needs a Common Gateway Interface (CGI) script on web server called Query_contents. This will manage web space and application space for web and application server respectively.
3. **Web application server aznAPI integration:** This is level three integration and involves implementation of aznAPI by access manager that allows an application to call an authorisation service for authorisation decisions. Access manager recognises the information given to application server by HTTP header. This information assists aznAPI to make more specific access control decisions. Level three requires installation of aznAPI on application server. By use of aznAPI integration can be improved by making use of dynamic roles, which are facilitated by privacy manager.

Integrating Access Manager with Websphere Portal Server: -

Websphere Portal Server (WPS) is an application running on Websphere application server and can use security services offered by application server. The joint implementation of Websphere server and access manager, offers choice for doing authorisation and authentication. Access manager can be integrated in the following ways:

- **Single sign-on to WPS:** WPS trust of WebSEAL is maintained by establishing physical connection between WebSEAL and Webserver. It also allows WebSEAL to protect its own resources and the sources on the junction server.
- **URL access control:** The next aspect of integration involves access control for individual objects on WPS, which requires small CGI script called query_contents on WPS.
- **Authentication and authorisation integration:** WebSEAL provides robust authentication, authorisation, availability and single sign-on service for the web environment. So, as soon as the browser attempts to access web resources, WebSEAL filters all the HTTP traffic, before encountering Internet. In this way it can isolate and save web servers from internal attack.
- **Common Security Model:** Access manager supports the java 2 security model and Java Authentication and Authorization Service (JAAS)-it identifies the user who is managing the code. Support for the standards provides great flexibility for java developer to use security and authorisation as an integral component of java application and platform software.

Answer: [b] Security and authentication

Module:4**Reference No:M4280**

Question: Time Division Multiple Access (TDMA)- a technology used for wireless communication allow multiple user to share:

- [a] One channel
- [b] Two channel
- [c] Multiple channel
- [d] None of the above

Module 4 - TDMA**Introduction**

One of the major problems in the conventional spread spectrum techniques for wireless communication was the intervention of one or more users. Basically, this was due to the fact that the users would transmit the data at the same time on the same frequency.

TDMA

Time Division Multiple Access (TDMA) is a technology used for digital transmission of voice and data in mobile communication. It permits multiple users on a single channel without any cross intervention. This is possible by dividing a radio frequency into time slots (also called epoch) and then assigning the unique time slots to each user in a particular channel.

Working of TDMA

Basically in TDMA, audio signals are converted into digital signals; i.e. the signals are divided into several multi-second long packets. A particular frequency channel is allocated for a short duration of time and then the packet is automatically moved to another channel. For example, let us take a case in which six different conversations occurs simultaneously. In such situation a single channel can hold all six conversations by dividing these into small fragments and assigning a time slot to each of them. TDMA boosts the cellular frequency capacity by about three times by dividing a 30 kHz channel into three different time slots. Initially one of the weaknesses of TDMA was misuse of bandwidth. The time slot would be allocated even if the two parties do not hold a conversation. In order to overcome this problem, extended time division multiple access(ETDMA) was introduced. With the use of ETDMA, instead of waiting for a subscriber to transmit the data, ETDMA transmits it in pauses that takes place in normal conversation. If the user needs to transmit the data, the required bandwidth is allocated accordingly; otherwise it is switched over to next subscriber.

Pros and cons of TDMA**Pros**

- Multiple signals can be transferred through a single channel.
- TDMA improves the efficiency of transmission by transmitting both voice as well as data.
- It can hold data rate transmission from 64 kbps (kilo bites per second) to 120 mbps (mega bites per second).
- It offers the user with extended life of battery as well as talk time because the cell will only transmit a portion of time while the users are busy in conversation.
- It is cost effective.
- Signals in digital form are easy to decode.

Cons

- Each user is given a predefined time slot. If the time slot at the other end is not free, it may result in the call getting disconnected.

- TDMA involves risk of path distortion in the sense that there may be hindrances (e.g. buildings) along the path while the signal moves from tower to handset. This may cause some interference.
- Request for a particular service is turned down if all the channels in a cell are currently engaged.
- Requires planning for frequency synchronization.

Future outlook

The competing technology for TDMA was introduced in 1989 called CDMA (Code Division Multiple Access). Both these technologies have their own pros and cons and it is hard to say that which technology is better.

Answer: [a] One channel

Module:4

Reference No:M4281

Question: 802.11b is an IEEE standard for wireless LANs. Which one of the following protocol supports the secure wireless communication in respect of 802.11b: -

- [a] Wired Equivalent Privacy (WEP) protocol
- [b] Hyper Text Transfer Protocol (HTTP)
- [c] Simple object Access Protocol (SOAP)
- [d] All of the above.

Module 4 – 802.11b

Introduction

Wireless network are more vulnerable to attack than that of wired network. Attack from intruders or other interventions in wireless communication has profound effect on day-to-day business.

Hence security has become a challenge for telecommunication industry. In this respect number of standards and regulations are functioning. One of the most important standard for secure wireless communication is 802.11b.

What is 802.11b?

802.11b is a standard used in wireless LAN technology, which has improved the quality of data as well as increased the data transfer rate from 2Mbps to 11 Mbps in the 2.4 GHz band. It usually works using the Direct Sequence Spread Spectrum (DSSS). 802.11b was developed by Institute of Electrical and Electronics Engineers (IEEE) in 1999 and provides encryption and authentication of data and user respectively. It provides means for secure wireless communication as wired communication with the help of Wired Equivalent Privacy (WEP) protocol.

802.11b has evolved from 802.11 standard developed by IEEE in 1997 for wireless LAN. It was the first WLAN standard that was sanctioned at international level. These standards enable administrators to form the network by connecting multiple LAN, which better meets their business and user needs.

802.11b is nowadays widely known as more friendly name called Wi-Fi or Wireless Fidelity.

Wireless Ethernet Compatibility Alliance (WECA) is -a regulatory body which controls and certifies cross vendor interoperability and ensures compatibility of 802.11b wireless products.

802.11b architecture

802.11 standard basically emphasizes on the two bottom layers of Open System Interconnection (OSI) model i.e. physical layer and data link layer. The performance level of WLAN 802.11 standards is comparable to Ethernet. So, all the LAN applications, OS, Protocols etc. work on 802.11 platform in the same way as if they are working on Ethernet connection.

On the other hand 802.11b standard operates only at physical layer of OSI model that provides faster data transfer rate and more robust connectivity.

Working of 802.11b

The original 802.11 IEEE standard operates on an 11-bit chipping known as Barker sequence. This Barker sequence was used to encode the data traffic to send through air medium. Each 11-bit chip is transformed to a waveform (called symbols) and represented in the form of 0s and 1s. These symbols make use of a technique called Binary Phase Shift Keying (BPSK), which transmits the data at the rate of 1Mps (1 million symbols per second). On the other hand when we consider the case of 2 Mbps, we need more complicated implementation technique called Quadrature Phase Shift Keying (QPSK), which almost doubles the efficiency as it was used in BPSK. This is basically done by use of radio bandwidth.

As far as the mechanism of 802.11b standards are concerned, it employs sophisticated coding techniques like Complementary Code Keying (CCK). It incorporates in itself a set of 64 code words each of eight bytes. These code words have unique properties that do not allow them to mingle among themselves when the receiver gets the message. These code words are not even susceptible to noise or interference in the communication channel (air).

The transfer rate of 5.5 Mbps uses CCK to encode 4 bits per carrier but to achieve transfer rate of 11 Mbps, CCK needs to encode 8 bits/carrier. In both the cases QPSK is used as a modulation technique. In this way higher data rates are achieved.

Let us assume the case of very noisy and chaotic environments. In such case 802.11b WLANs make use of *dynamic rate shifting*. It permits the data transfer rates to be adjusted automatically according to the changed environment. It takes place at the physical layer and speeds up the transmission rate.

Answer: [a] Wired Equivalent Privacy (WEP) protocol

Module:4

Reference No:M4282

Question: Which of the following services is a special feature provided by SIP?

- [a] User mobility
- [b] Call set-up
- [c] User location
- [d] Call splitting

Module 4 – SIP (Session Initiation Protocol)

What is SIP?

A signaling protocol that is used to establish the Internet Protocol addresses and port numbers for end systems, which send and receive data is known as Session Initiation Protocol. Since, SIP doesn't carry data it is not a transport protocol. SIP is an end-to-end, client/server session signaling protocol that facilitates two or more entities to communicate.

Principle

The SIP is involved only in signaling and the actual data is not communicated. The main principle of SIP is to provide interoperability between different Internet entities. This is done in the form of communication that is separate and simple with some additional services. SIP is dependent on the Session Description Protocol (SDP).

Features

Some important features provided by SIP are:

User mobility: It uses the URL Internet address format like `firstname.surname@icai.com`

A session is established without the necessity of an IP or MAC (Media Access Address). Thus, user mobility is achieved by the user himself, programming the physical location at a time. Manual / automatic call control on top of the protocol: By using simple and dynamic programming SIP users can redirect calls from unknown callers to any other attendant, reply with a web page, send a JPEG image and the like. In short, SIP is Internet telephony and not a Voice Over Internet Protocol (VoIP).

Services

The different services provided by SIP include:

User availability: In order to determine the willingness or availability of the party that had called to engage in communication.

User location: To ascertain the end system to be used for communications.

Call set-up: The process of ringing and establishing caller and calling functions for both the parties.

User capabilities: To determine the media and the different media parameters to be used.

Special deliverables

Splitting a call: SIP has a special provision for splitting an incoming call. So, many extensions can ring at the same time with a single originating call. The first extension to answer gets the call. The usage is realised if the called party is identified by in one of several locations.

Replying with alternative media: As soon as the SIP server receives a connection request it is possible to return a web page to the client who had called. In times of vacation or absence due to illness this web page can be a source of alternate information.

End users and / or third parties may program SIP: This gives very high levels of flexibility in personalising SIP communication services. It also allows the users to dynamically change the response to calls. They can block all calls from a particular person / number, get distinctive rings (ring selected based on who is the calling person), redirect known friends to a mobile phone and everyone else to 'my assistant'.

Answer: [d] Call splitting

Module:4

Reference No:M4283

Question: Which of the following about SNA cluster controllers is true?

- [a] They come with the D model
- [b] They are Link-attached cluster controllers
- [c] They are called as physical unit devices
- [d] They come with model number c

Module 4 – Cluster Controllers

Introduction

Communication controllers are deployed to manage input and output of data to nodes in a computer network. These units range from the complex front-end mainframe interfaces to simpler devices such as bridges, routers and multiplexors. They are responsible for the conversion of computer data from parallel form to serial data for transmission. In addition they also perform control functions, error checking, and synchronisation. The communication controllers are mostly referred to as front-end processors since they are separate devices that are different from the host system that handles all communication with external devices such as terminals. The host computer is thus being freed from being continuously engaged by

external devices thus allowing it to function more efficiently.

What is a cluster controller?

A Cluster Controller is a communication controller that provides hosting service thus allowing the system administrators to maintain a fault tolerant group of nodes. In addition to that they also provide contract-based access to third parties. The Cluster Controller controls the member nodes with the help of Node administration section of the Application Programming Interface (API). Each node runs a special netlet (a special program) through which the nodes administrative API can be accessed and establish connection with the Node Management API. The Cluster Controller has a provision for an administrative interface with the basic Hosting API, which is used for cluster administration. Some of the administrative functions are contract management, node shutdown, and resource allocation.

IBM

International Business machines have been a dominant player in the evolution of cluster controllers to the extent of their name being synonymous with them. This makes it necessary to have a look on IBM cluster controllers.

An IBM-manufactured or compatible device that can channel-attach 3270 terminals to a host system is termed as a Cluster controller by IBM. It can also communicate with a host through an SDLC (Synchronous Data Link Control) link or a bisynchronous link to a host-attached with a communication controller. Two widely used cluster controllers are channel-attached cluster controllers and link-attached cluster controllers:

- **Channel-attached cluster controller:** The controllers that are directly attached to the multiplexor channel of the host system come under this category. Some of the cluster controllers in channel-attached type are "A SNA [Systems Network Architecture] controller" and "D (non-SNA controller)".
- **Link-attached cluster controller:** They come connected with communication controllers. The communication controller is in turn attached to one of the channels of the mainframe. A modem in an analog circuit and CSUs / DSUs (channel service units/data service units) in digital circuits form a link between the cluster controller and the communication controller. Model numbers for this type of controller end in C.

The SNA cluster controllers are called as PU (physical unit) devices and terminals that are attached to it are called LU (logical unit) devices. The new models of cluster controllers have advanced features like IBM Token Ring attachment interfaces, management and monitoring.

Answer: [c] They are called as physical unit devices

Module:4

Reference No:M4284

Question: In remote connection security for GPRS (Global Packet Radio Service), which of the following method encryption of message is done at client VPN (Virtual Private Network):-

- [a] End-to-end VPN
- [b] Network level VPN
- [c] Dedicated connection from GGSN
- [d] None of the above

Module 4 – GPRS (Global Packet Radio Service) Security

What is GPRS?

A standard for wireless communication with an enhancement over GSM (Global System for Mobile Communications) with speed up to 115 kilobits per second is GPRS (Global Packet Radio Service). This standard provides all time dedicated mobile access in the form of email, Internet and the like. Packet-mode of transmission is used to transfer both high speeds and low speeds over GSM networks. GPRS supports a wide range of bandwidths and makes efficient use of limited bandwidth.

GPRS Security

Since GPRS is implemented on IP (Internet protocol) networks, routing and all other security considerations must hence be taken care of. The major drawback in IP is that the data packets are accessible to anyone having access to router. In order to overcome this problem IPsec has been developed. Although this process results cost overrun, but still IPsec(Internet Protocol Security) provides integrity and privacy of IP packets.

How to save GPRS network?

It can be done by eight methods:

Encryption, Authentication, Firewalls, Routing, IP-Addressing, Secure Protocols and Frequent Backup.

Methodology

- **Border gateway:** This firewall guards the GPRE backbone against IP-spoofing as border gateway holds the information regarding network address of other operators.
- **GGSN (Gateway GPRS Support Node):** This type of firewall allows user's data to pass transparently and prevents MS (mobile station) from outside attacks
- **SGSN (Serving GPRS Support Node):** The subscriber is recognised at this point and it is used for ciphering and authentication of mobile stations.
- **LIG (Lawful Interception Gateway):** This is a functionality by which one can gather information from the data intercepted by the user and enables the authorised person to access that data. At this point of time the role of GPRS is to hand over the user data to LIG where it is stored.

How to secure remote connections over GPRS?

There are basically three ways to implement secure remote connection:

1. End-to-end VPN (Virtual Private Network)
2. Network level VPN
3. Dedicated connection from GGSN.

End to end VPN: This is the best security from customer viewpoint as encryption is done at VPN client and decryption at corporate VPN server. But this will create problems when NAT (Network address translation) is used, as GGSN's NAT will change the address fields of IP packets, which will reject the IP checksum at the decryption point. Hence these packets will be discarded and treated as "corrupt packets". The solution for this is to encapsulate the IPSec packets in UDP (User Datagram Protocol) before sending.

Network level VPN: Here VPN is set up between the corporate intranet and the GGSN, which provides access to Internet. The traffic is encrypted at the VPN server so that data can be encrypted over the public Internet, which is used to access the corporate intranet. The data is decrypted at the similar VPN server residing at the corporate intranet gateway. The user is authenticated on the basis of his permission to access the points that are defined in the HLR (Home Location Register).

Dedicated connection from GGSN: A dedicated connection from GGSN to the corporate intranet is established. This provides constant bandwidth and security as it bypasses the public Internet completely. The cost of such type of connection is very high and hence only large organisations can afford it.

Answer: [a] End-to-end VPN

Module:4

Reference No:M4285

Question: Which of the following is/are the essential elements of VoDSL architecture?

- [a] IAD (Integrated Access Device)
- [b] DSLAM (Digital Subscriber Line Multiplexer)
- [c] Voice gateways
- [d] All of the above

Module 4 - VoDSL (Voice over Digital Subscriber Line)

DSL (Digital Subscriber Line)

It is an interconnection between Internet service provider network and the customer (user). In DSL the user need not dial the number or establish the connection for communication because it makes use of "always ON" service. The speed of DSL is about 35 times more than that of conventional dial-up connection. DSL transfers voice and data enabled by copper wires.

VoDSL

It is a technology that transmits high quality voice signals over the Digital Subscriber Line using the same copper wire network. This service is basically used by small and medium enterprises. The prerequisites for providing VoDSL service are:

- **Customer equipments:** Customer will require site equipments like PBX (Private Branch Exchange), modem, telephone and the like.
- **Integrated Access Device (IAD):** It resides on the customer site and works as an interface between customer's voice equipments and DSL network. The voice is integrated into packets at this point by using technologies like Asynchronous Mode (ATM).
- **DSL line:** It serves as a channel for carrying the voice using twisted pair copper loop.
- **DSLAM (Digital Subscriber Line Multiplexer):** It acts as a hub where a multiple DSL lines from various locations assemble. As a result voice and data traffic is collected from DSL lines.
- **Data Switches:** DSLAM hands over the voice and data traffic to data switches. Data switch segregates voice from data. Data packets and voice packets are transferred to data network and voice gateways respectively.

- **Voice gateways:** De-packetization of voice packets takes place at voice gateway and converted into standard format. These are then sent to class-5 voice switch.
 - **Class 5 voice switch:** It is the local telephone exchange which finally provides dial-tone, routes the call and service to a particular customer and generates records for billing purpose.
- Eventually Public Switched Telephone Network (PSTN) is required which is nothing but public telephone network.

Layers in VoDSL

There are basically four layers through which the whole process of voice transfer takes place on VoDSL. They are:

1. **Physical layer:** It represents the physical connection in the network that connects the customer and service provider at the two ends respectively. This is enabled through a twisted pair of copper wire.
2. **Transport layer:** It deals with the transmission of voice & data and is carried by: -
 - Internet Protocol (IP)
 - ATM
 - Frame relay
3. **Voice coding layer**
4. **Signalling layer**
5. **Service layer:** It provides a support to the network, assists in services like dial tone and call waiting. Voice capable switches help in all these processes.

Benefits of VoDSL

VoDSL provides many additional benefits over traditionally used telephone system. Some of them are:

- One network for voice and data transmission.
- Customer can use their existing devices
- More flexibility in using additional services due to simple network
- Multiple voice channels can exist over a single copper line.
- Low cost.
- Improves efficiency

The only disadvantage of VoDSL is that it is accessible only up to a limited distance from the local exchange.

Answer: [d] All of the above.

Module:4

Reference No:M4286

Question: Label Switched Paths (LSPs) that are established before the transmission of data in Multi protocol label switching (MPLS) are: -

- [a] Data driven
- [b] Control driven
- [c] Network driven
- [d] None of the above

Module 4 – Multi Protocol Label Switching (MPLS)

Introduction

Even as the Internet is growing by leaps and bounds, the speed, scalability, bandwidth and traffic management are some major issues to be tackled. MPLS addresses all the problems in the networks.

MPLS

It is a framework developed by Internet engineering task force (IETF) and offers an efficient routing (action taken by the network to move the data packets from source to destination), forwarding and switching of voice and data over the network. MPLS helps in detecting the path followed by traffic over the network and also supports virtual private networks. Some of the functions performed by MPLS are:

- Manage the flow of traffic shuffling between different networks, hardware, machines and in different applications.
- It provides interface to the routing protocols like Open Shortest Path First (OSPF) and Resource Reservation Protocol (RSVP).

Working of MPLS

In Multi protocol label switching (MPLS) transmission of data takes place on label switched paths (LSP). LSPs can be defined as series of labels (a path identifier that assists in data forwarding process) placed at every node in the channel while the data moves from one place to another. The establishment of LSPs can be:

- **Control driven:** LSPs are placed before the actual transmission of data.
- **Data driven:** LSPs are placed after certain data traffic is detected over the network.

The devices that contribute in MPLS protocol mechanism can be categorized into: -

1. **Label Edge Router (LER):** It works at the border of MPLS network and access network. LER establishes LSPs and assembles the data traffic from dissimilar networks. This traffic is then transferred to MPLS network. LER also plays a crucial role in adding and removing the labels from the communication channel as the traffic enters or leaves the network respectively.
2. **Label switching router (LSR):** It is a router device in a MPLS network that takes part in establishing LSPs. LSR makes use of label signalling protocols for this purpose.

Advantages of MPLS

The most important benefit of MPLS is that it is a standard framework based on label switching technology that allows interoperability among different vendors. Some of the advantages of MPLS are: -

1. **Explicit routing:** It is the ability of specifying a path over the network and then choosing the data packets to follow the specific path. It is much more efficient technique than that of traditionally used source route option in Internet protocol (IP).
2. **Virtual Private Networks (VPNs):** Now-a-days most of the organisations use VPNs, which makes use of public network like Internet to connect and communicate to their multiple sites. MPLS plays a very important role in constructing such networks. The labels of MPLS are used to isolate the VPN traffic from normal traffic.
3. **Inter domain routing:** MPLS provides a clear distinction between inter as well as intra domain routing. In this process less routing knowledge is needed within a particular domain.
4. **Supports different types of traffic:** Generally this advantage of MPLS is not visible to user. MPLS allow unicast as well as multicast data packets to be transmitted over the network.

Answer: [b] Control driven

Module:4**Reference No:M4287**

Question: Personal communication services (PCS) requires_____ antenna(s) for receiving and forwarding the data and voice traffic.

- [a] One
- [b] Two
- [c] Several
- [d] None of the above

Module 4 – Personal communication services (PCS)**Introduction**

PCS is a wireless technology introduced by Personal Communication Industry Association (PCIA) in 1996. It offers a wide range of mobile services (voice mail, stock quotes, caller ID, etc.) to users and allows communication irrespective of the location . PCS does not make use of public switched telephone network (PSTN), thus enabling the user to communicate from anywhere.

The major difference between a cellular services and PCS is that PCS is based on digital technology i.e. all the transmissions of human voice are in the form of 0's and 1's and then again converted into analog signals at the receiving end. On the other hand most cellular operators uses analog networks.

PCS bring in the following major advantages to the customer:

- PCS can transmit voice as well as data simultaneously.
- A single number is allocated to the user without any location constraint.
- Transmission is much faster in PCS.
- PCS systems are equipped with advance voice mail and caller ID facility.
- PCS can also transmit voice and data traffic to laptops and fax machines
- PCS handsets are much lighter than that of cellular operators.
- These are cheaper for long-term use and offers extended battery life.
- It allows Short Message Service (SMS) to transmit along PCS and cellular phones.
- It supports wireless e-mails, and Internet access.
- Message waiting indicator (MWI) feature alerts the user for voice mail messages.

Advantages of PCS and how it differs from cellular operators

- Although cell phones, modems and faxes all operate on the same principle the difference lies in the user interface. A tower receives a radio frequency signal sent by transmitting devices. This signal is authenticated to ensure that legitimate person is receiving the bill. It also ensures that the call is directed towards its destination. In such cases the transmitter does not fall in this range, the call is transmitted to a nearby tower, which comes in the range of the transmitting device.
- PCS requires a number of antennas (Very Small Aperture Terminal (VSAT) dishes) to cover a particular area. This results in wider coverage as also reducing the frequency of dropped and disconnected calls. When the user makes a call from any location the phone signal is accepted by the nearest antenna, which is then passed on to the base station. It is then connected to the wired network.
- PCS technology uses much higher frequency as compared to cellular system operators and falls in the range of 1850-1990 MHz . Higher frequency does not permit signals to travel as long as cellular signals. This is the reason that PCS requires number of small antennas to transmit the traffic.

Future outlook

The only problem faced by PCS technology in the present scenario is the lack of proper infrastructure to support the full fledged use of PCS. This is basically due to the fact that PCS infrastructure requires high cost and it is a time intensive work. The biggest players in the industry are Teledesic (a joint venture between Microsoft and McCaw) and Motorola's Iridium.

Answer: [c] Several

Module:4

Reference No:M4061

Question: Rapid Application Development is not appropriate when the development cycle involves

- [a] Reusability
- [b] Short time cycle
- [c] High technical risks
- [d] Small-integrated teams

Module 4- Rapid Application Development

The Rapid Application Development (RAD) is a software development model that emphasises on a short development cycle. It is a methodology that condenses analysis, building design, and tests a series of short, iterative development cycles. RAD is generally adopted when the project has a very short time limit (generally 60 -90 days), and has been clearly outlined.

Traditionally, a project would require planning, analysis, designing, testing and finally deployment. A RAD project is split into modules, and after completion of their task, individuals can move out. The RAD team is generally small and integrated, consisting of IT personnel managers, developers and end users. Members have to communicate with each other effectively, to complete projects successfully, without delays and costs over runs.

Such a process adopts a different iterative approach in executing projects. Unlike the traditional process, where projects have to undergo a series of steps; this process condenses all the steps of planning, analysis, design and the like, into small repetitive steps. It makes the process accurate, auto-corrective and thereby effective. RAD promotes the use of object-oriented methods to reduce repetitive jobs and supports reusability.

The RAD process can be carried out in the following phases:

1. Initial analysis: First, the requirements are identified then the product is designed, and possible threats are assessed. This stage also considers methodologies that have to be used, and gives an idea of the end product
2. Data analysis: Based on the requirements and the methodology, data is grouped into objects. Each attribute of the data object is identified, and relationships between them are also established.
3. Process modelling: Data objects change to allow information flow, necessary to implement a business function. The data object processing includes adding, deleting and modifying.
4. Development of modules: RAD generally uses fourth generation techniques. It makes use of existing components or creates new reusable components.
5. Testing and fielding: By the end of the final phase, individual components are tested a number of times. New components however are tested again, before the final product is ready for the market.

In spite of all its cost and time saving features, RAD may not always be effective.

1. **Team spirit:** If the team does not work in cohesion, and there is a communication gap, it may lead to overruns in time and cost
2. **Technological expertise:** The team should be acquainted with the technology being used. Lack of experience not only delays the project, but may also result in errors.
3. **Understanding the requirements:** This is one of the biggest reasons for the failure of a project. Requirements should be carefully identified and clearly understood, and should not be changed frequently.

Answer: [c] High technical risks

Module:4

Reference No:M4192

Question: In which phase of the primary operating system is software tested?

- [a] Project
- [b] Pre-alpha
- [c] Alpha
- [d] Golden master

Module 4 – Essentials of Software Testing

Introduction

Software testing is the crucial function of software developers. They have to guide organisations in testing software. Guideline steps for testing the software have already been established and in usage for a long time. The audit objective of software testing is to ensure the adequacy of testing methodology and evaluating the testing criteria. Auditors should ensure that the risks are identified and remedial actions are taken.

Phases in Software testing

1. **Project:** In this first phase of the testing process, the procedure to examine the software's ability to meet the requirements is defined.
2. **Pre-alpha:** In this phase the quality assurance team, internal users and sometimes-external customers (on special request) conduct the test.
3. **Alpha:** All urgent and high priority bugs are removed before taking up Alpha testing. The product in this phase is tested on the primary operating system platform. Any verification from customers must be addressed in this phase. The first cut of the documentation must also be passed here.
4. **Beta:** In this phase the product is ready to be used in the production environment and its ability to meet the requirements can be tested. Before moving the product to Beta testing, all customer identified bugs are addressed and more than 50% feedback received from Alpha testing customers is positive.
5. **Golden master:** This stage must ensure that all the bugs have been addressed and documentation should be arranged for final printing. Documentation must be approved and negative responses evaluated.
6. **First Customer Ship:** It is the last phase and the product is ready for purchase.

Verification of software

The developed system is compared with the requirements specified in the early stages. This process is known as software verification. Under a formal verification process, software is executed repetitively until the correctness of the software is ensured.

Alternatively, a mathematical process could be followed for testing. Here, a function generated or computed by the programme is matched with the specified function. If it matches, the end result will be "true". This method is very difficult.

These two methods attempt to evaluate only the correctness of the output for the given input. Under software testability analysis, the possibility of software code failure in case of any error in the code is tested.

Audit role

Audit should concentrate on the External Beta testing process as it ensures the efficiency of the process. Since the product is moved to external customers, organisations need to be careful. Defects that are identified in the earlier stages must be eliminated, because when the same are moved to outsiders and they identify the defects, it results in duplication of processing.

Common Beta problems

When the external beta testers are not available, beta fatigue can be set in. The installation and de-installation processes ought to be correct lest problems should arise. These could be in the form of test cycles being lost, crucial things being leftover or beta cycles failing to identify problems. The user is crucial in designing a product; hence, a programme must follow the user's task.

Effective internal reviews

Internal QA staff is more efficient than the external beta testers because the:

- Interaction with developers enables QA staff to know the product
- QA team can do better if the management supports and an effective test plan is developed
- QA team can be more disciplined than an external tester and they can ensure clarity and consistency.
- QA staff receives compensation for their services, which motivates them unlike external testers.

Beginners can depend on outside testers but should exercise complete control over the quality and quantity of the reports generated by them. Testers must be trained on tools, understand testing goals and probable inspection areas.

An incentive to the testers will motivate them to work efficiently. Hence, incentives must be provided for developing clear reports. Finally, when the product is ready for testing and testers are trained, the auditor must ensure that the quality of the product can be enhanced.

Answer: [c] Alpha

Module:4

Reference No:M4272

Question: TQM in software development needs to be more

- [a] Problem based
- [b] Process based
- [c] Both problem and process based
- [d] Problem or process based

Module 4 - Software Development - Total Quality Management (TQM)

TQM is a blanket term that brings within its fold a wide range of concepts and ideas. The focus of this article however is its application in the realm of software development.

Very indicative of software development is its thrust on problem solving. Continuous improvement also covers probing techniques to reveal improvement opportunities. The methodology involved is very similar to what software professionals do on a day-to-day basis. The one banal mistake that TQM implementation results in often is to make continuous improvement a formal, time consuming, people intensive project. Most organisations overlook the basic idea that part of the effort to make continuous improvement continuous is to make it an employee friendly task, which can be done as and when deemed necessary.

If the continuous improvement methodology needs to be effective and successful, it should comprise of the following steps:

- a. Addressing the problem areas/ issues
- b. Detecting the reasons
- c. Resolution
- d. Follow-up

Addressing The Problem Areas/ Issues

Identifying areas that demand improvement is relatively easy. This is because aids exist in the form of trouble reports, customer complaints, and employee ideas. Another means to detect opportunity areas is to make use of the knowledge database piling up throughout the software life cycle.

Once these areas have been identified the focus must be on describing the problem/issue thoroughly. Again quantifying the consequences of making these recommended changes is equally necessary. This can either be the cost incurred in letting the problem go unattended to, or the savings accrued to by bringing about the improvement.

Detecting The Reasons

Dealing with the root of the problem is key to improvement. Only then we can ensure total quality improvement through permanent problem resolution. Often the symptoms are attended leaving the causes to lie where they are. Hence improvements so brought about do not last long.

Resolution

Arriving at this stage may involve exhaustive brainstorming and research sessions. Lot of analysis is needed here. It is pertinent to know what kind of individual authority and responsibility is necessary put down the requirement levels of involvement from others. Equally important is to review the impact of all these recommended actions on time, cost, customers, suppliers, and schedules. The resolution stage usually involves exhaustive decision making on activities, responsibilities, and time frames.

Follow-up

This stage completes the cycle of process change. Here organisations understand how successful the TQM implementation has been. Results are studied alongside the reduced costs and improved productivity. Follow up also ensures that future improvement areas are addressed.

If TQM is to benefit software development, then it needs to be applied to processes and not problems. Again, it needs to be addressed on a periodic basis. Further process improvement must be a part of the daily task list.

Answer: [b] Process based

Question: Viruses that can change their appearance and use encryption are known as:

- [a] Boot sector virus
- [b] Polymorphic virus
- [c] Stealth virus
- [d] Mutipartite virus.

Module 5- Viruses

Biological viruses are organisms capable of causing harm to the human system by replicating itself. Similarly, computer resources are also vulnerable to virus attacks. Just as biological viruses can spread from one /person to another, computer viruses are also capable of infecting system resources.

What are viruses?

Malicious program codes that can replicate and spread across computer systems, causing damage to systems and their components are termed as viruses. On execution these programs infect other files and documents in a system, extensively damaging data stored and other programs.

Transmission modes

Modes of transmission include e-mails, downloads and hardware components like diskettes or compact disks. They often get transmitted without the knowledge of the enduser. Some viruses become active on execution, while others are inactive, till some users perform specific operations with their codes. These operations that activate a virus is referred to as a trigger. Payload is the attribute of the virus that is injected to infect a system at a particular point of time. Many virus attacks result in loss of data and reformatting of the system.

Types of viruses

- File infecting virus

Viruses that infect files and are present in the memory are termed file-infecting viruses. These viruses infect executable files such as those with an extension .com, .exe. Some file infecting viruses attack operating system files only (such as command.com). MS-DOS (Microsoft Disk Operating System) executes the .com file, before the .exe file, so the .com file is executed first, loading the virus.

- Boot sector virus

Viruses that infect the boot sector (master boot record) on a computer system fall under this category. They first replace the original boot code, with the infected boot code. They then move the original boot sector information to another sector on the disk. Detection of such viruses is difficult, as the boot sector is the first thing loaded when a computer starts. The most common way a system gets infected with a boot sector virus is by using an infected floppy disk.

- Polymorphic virus

Viruses that change their appearance with each infection are termed polymorphic viruses. These viruses use encryption, and alter the encryption algorithm with each new infection.

- Stealth virus

These viruses remain hidden from the operating system and anti-virus software. The virus can hide changes it makes to file sizes, directory structures, other operating system aspects and the like. Part of such a virus is memory resident. This results in less memory availability for users.

- Multi-partite virus

Viruses that infect both boot sectors and executable files are termed multi-partite viruses. These viruses can cause extensive damage since they combine stealth techniques, along with polymorphism to prevent detection.

Macro viruses

This forms a separate classification among viruses, since they affect application programs in a system. A virus that damages a Microsoft Word or similar application, and causes a sequence of actions is known as a macro virus. These actions are performed automatically, when the application is started or is triggered by something else. 'Melissa' is the best example of macro virus.

Answer: [b] Polymorphic Virus.

Module:5

Reference No:M5002

Question: Logical access controls are built into_____.

- [a] Software and operating system
- [b] Operating system, hardware and communication devices
- [c] Software, hardware, operating system and communication devices
- [d] Communication devices and operating systems.

Module 5- Logical Access control

Introduction

Storing and processing information is the main function of any information system.

The main objective of information systems is to facilitate information sharing . Systems now support multi-users, and require a mechanism to keep track of e users accessing the system, and preserve integrity and security.

What is meant by access control?

Access means the ability to use, change or view any information in a computer environment.

Set of policies and mechanisms that restrict access to computer resources + is termed as access control. When information stored in a system can be accessed by a number of users, several issues of information sharing have to be dealt with.

What is logical access control?

Information may be accessible to users, but not all of them will be entitled to make modifications. Protection techniques that limit access to information, as well as, restrict forms of access to only the appropriate user is logical access control. Computer-based access controls are termed logical access controls.

Where is logical access control used ?

Operating systems, application programs, communication network components and data base management systems incorporate logical access control techniques.

Concept of logical access control

Logical access control is based on access modes. They enable systems to support different kinds of user accesses , and determine the kind of data, service, programs and hardware that can be accessed by the user. These include:

1. Read only: Such a privilege enables the user to view, copy and print data/files, but not alter its contents.This is the read only access mode.
2. Read and write: Here, apart from being able to view information, the privilege to alter it is also provided.

3. Execute: This privilege allows users to run programs and files.
4. Create: This privilege gives users access to create new records.
5. Search: This privilege empowers users access to search any kind of files in a information repository.

Administration

For effective functioning of systems , logical access control has to be administered in an effective manner.

Administration includes implementing, monitoring, modifying, testing, terminating user access to systems and resources. There are three forms of administration -centralized, decentralised and hybrid.

In centralised administration, the overall control for configuring access rests with a single group/team. Decisions regarding access privileges and disputes are dealt with, by this centralised authority.

In decentralised administration, the access to information in different files and directories is open to creators or users of the information system.

Hybrid administration is a combination of both whereby, some information is controlled by the centralised authority, and the rest is left to the discretion of the user.

Answer: [c] Software, hardware, OS and communication devices. Logical access control can be implemented in application programs, utilities, operating system, backend tools and even in communication devices.

Module:5

Reference No:M5003

Question: Physical access control does not depend upon which of these factors?

- [a] Working environment
- [b] Hiring procedure
- [c] Public key infrastructure
- [d] Access privileges.

Module 5- Physical Access Control

Information systems in any enterprise have to ensure that security and integrity of data are maintained. The workplace becomes vulnerable to theft or tampering if due consideration is not given to securing the work area. An important component of a company's information security strategy is Physical Access Control (PAC).

What is physical access control?

Employees in an organisation are given time specific physical access privileges, for use of computers and other resources. This is known as physical access control, where access is restricted to authorised persons only.

Considerations

Access to restricted zones (places where confidential information is processed) in an enterprise must be controlled, especially when mission critical applications are underway. . An integrated physical access control system has to be developed to make it cost-efficient. . Efficiency in the administrative level is achieved through the deployment of authentication databases for all the individuals associated with the organisation. An important consideration would be the decentralisation of the access authorisation so that privileges are granted with more flexibility. This will in turn enhance the post implementation of access control by making audit and monitoring systems simple. Physical access control implementation involves more of a systems integration effort. This is due to the reason that most of the tools required to achieve this are standard hardware and software. The primary issue is customising these components to meet the needs of the organisation function in a distributed environment.

Tools for physical access

Badges, keys to restricted areas, card control systems like smart cards and biometric systems are some of the most commonly used tools for physical access control. Biometric systems play an important role in PKI (Public Key Infrastructure), in e-commerce, which forms the basis for physical access control techniques.

Personnel practices

Professional work environment, hiring and termination procedures are related to information systems security. Since, these issues have specific impact on its integrity, it is essential to be effectively considered for physical access control.

- Professional work environment: An enterprise information system demands confidentiality, security, and personal ethics. Misuse of the extremely sensitive information by former employees and security professionals mounts to a severe loss to the enterprise. Newly hired professionals' ethical outlook and attitudes play a major role in defining the company's work environment.
- Hiring policies: Selection of the individuals must be done after a careful scrutiny and after ascertaining the candidate's personal and professional integrity.

Answer: [c] Public Key Infrastructure. PKI forms the basis for e-commerce transactions and is not an essential factor for physical access control.

Module:5

Reference No:M5004

Question: Components of an ACL include_____

- [a] Roles
- [b] Roles and rights
- [c] Roles, rights and resources
- [d] Roles, rights, resources and filters

Module 5- Access control Lists (ACL)

In case of a small network, a simple system with basic access control is sufficient. As system requirements increase, user access has to be regulated to ensure security and integrity. ACL refers to a repository of information, which contains details of individuals/groups who have access to information (in the form of files, directories, programs and the like). In addition to storing permissions assigned for different users of a system, it also has the access modes assigned to these groups/individuals.

Definition

Access Control List is a mechanism that defines rights associated with each individual's access, and assigns Definite roles/groups for information processing. ACLs provide security and control to the information system.

Components

ACLs consist of three basic components:

1. Roles: Rights are assigned to individuals to access information, based on certain parameters referred to as groups. These parameters could include position/ function/responsibility of the individual within a group. . Within work groups, the level of permission can vary, some members may have access to certain directories/files, but not the subdirectories. For example, if A is a salesperson, he belongs to the Sales group. Rights will be assigned to

him for all information that he requires to do his job. His supervisor will have access not only to information pertaining to A, but also to all sales persons working under him. When an individual is assigned one or many roles, he becomes a part of a group/ class of users.

2. Rights: After defining the class, users have to be assigned access types, rights or permissions. Different types of access are Read, Write-Append, Write-Create, Execute, Delete. Access can also have advanced rights classification. For instance, deleted files could have an archive for recovery, or sometimes have a delete-remove to track files deleted.
3. Resources: Any role defined for an individual/group differs from another, based on the level of access allotted. Each /role within a group is assigned access to a resource (information/file/drive/directory), and there arises a need to define a hierarchy of rights, which is the basic rule for ACL. One such hierarchy rule specifies that if a user has a low level of access, then he cannot have a high level of access. This means, if a user doesn't have rights to read a file, it is impossible for him to write/append it.

Application

ACLs are extensively used in routing traffic, through routers, and are a major security control in a network. Access lists are configured to route network protocols like IP (Internet Protocol) that filter packets of data through the router.

Working

ACLs work with filters and routers in a network. They have a criteria list that gives details of packets that can be allowed into the network, and others that can be removed. Access list criteria contain the source address, the destination address of the traffic and other information. Thus, they work in tandem with firewalls in a network to regulate traffic.

Answer: [c] Roles, rights and resources

Module:5

Reference No:M5005

Question: Which of these biometric tools use thermal sensors along with infrared rays for identification?

- [a] Key stroke dynamics
- [b] Iris/retinal scan.
- [c] Speech recognition
- [d] Finger print scanning.

Module 5- Biometrics

One of the techniques gaining widespread prominence for physical access control is Biometrics. It has emerged as an effective solution to ensure security and integrity of the work environment.

Biometrics has evolved over the years as a field of development of statistical and mathematical methods for data analysis in biological sciences.

Definition

The field of study that deals with recognition and identification of a person based on his/her psychological or behavioural characteristic is called as biometrics. A pattern recognition system for accomplishing this personal identification is termed as a biometric system.

Principle

The primary focus of a biometric system is either verification or identification. Verification is to confirm or deny a person's claimed identity whereas identification refers to establishing a person's identity. A person's unique traits are stored in a database and are matched at the time of verification. These traits include the physiological or behavioural characteristics. Physical indicators are iris, fingerprint, facial or hand geometry. Behavioural aspects encompass voice print (Speech recognition), keystroke dynamics and handwritten signatures. Biometric tools that are employed to measure human traits fall under Static and Dynamic categories.

Static is the measurement of a trait that requires no action to be performed during verification. Dynamic refers to measurement of a trait when the action takes place. Written signatures can be verified both statically and dynamically.

Biometric tools

Most commonly used biometric tools are:

Hand geometry: The distinct features of the hand like external contour, length of fingers, palm, fingerprints, geometry of hand and the like form the basis for this biometric tool. The user's identification is done and hand is made to be placed on an automated system for processing. Image samples that are already stored in the database are compared with the hand characteristics with the help of a camera. The analysis is based on the principle that there are correlations between different measurements. This finds extensive application in physical access control.

Fingerprint verification: This has been traditionally followed in forensic sciences with conventional methods. First a high-resolution digital camera generates a fingerprint image. The basic pattern of the print (arch, whorl, loop, etc.) and finer details like curves, patterns, the friction ridges of a fingerprint, points of bifurcation and convergence are taken into consideration. The relative location of these points and their interrelations form a unique profile for identification.

Iris/Retinal Scan: The unique pattern of blood vessels on the back wall of the retina is used here. The user is made to position their head against a support, and a low power infrared light is directed against the back of the retina. The image of the pattern of veins is reflected back to a camera. The image is analysed, based on the sizes of veins, location of vein bifurcations, and capillary endings. Using thermal sensors, further secure systems can be devised.

Keystroke dynamics: The way a person applies/types a keyboard is the unique identifier, which is also called as typing biometrics. The time delay between keystrokes, frequency of typing errors, duration of contact and the like are differentiated for individuals for identification.

Speech recognition: The inherent characteristics of sound like vocals, phonetics and vocal features like nasal cavities, vocal tract serve as distinct identifiers for speech recognition in individuals.

Apart from this other biometric identifiers include body odour, DNA information, Gait, and signature dynamics.

Answer: [b] Iris/Retinal scan.

Question: Which of this is not an internal access control mechanism?

- [a] Passwords
- [b] Host-based authentication
- [c] Roles
- [d] Permission bits.

Module 5- Internal Access Control

Organisations implement different forms of access control based on security, operational requirements and user-friendliness. Logical access control that specifies the type of access permitted to each individual/group in an enterprise has to be the most appropriate and cost effective one. The generally adapted principle is to grant least privilege to the employees so as to perform their official functions.

What are internal access controls?

The act of segregating the defined users or groups logically with privileges to system resources is called as internal access control. Some of the commonly used internal access controls include passwords, roles, permission bits, encryption, access control lists, constraint user interfaces, labels and the like.

Passwords

The main purpose of using passwords is user identification and authentication. Passwords are also employed in systems to protect data and programs. For example, payroll applications are password protected so that access to specific data is restricted to HR department.

Roles

Access to information is allowed based on the functions. For example, what role an accounting officer, a purchase officer and the like shall have depends on the information necessary to perform their function. Roles are deployed both in the system level and application level. Business process oriented roles are assigned to work groups so that application level activities can be streamlined.

Permission bits

In a multi-user environment systems access rights to files are based on the concepts of owner, group, and world, which have a set of access modes (read, write, and execute). The owner of a file who is usually, its creator specifies the allowed modes of access to the object. Users who are members of the group associated with a file are granted modes of access distinct from non-members, who belong to the rest of the "world" that includes all of the IT system's users. User groups are arranged according to department, project, or other teaming functional relationships.

Encryption

Encryption uses cryptographic keys to ensure access control and is most suitable for applications where physical access controls are unable to be implemented. This is used along with key management techniques to ensure effective implementation. Examples are using encryption in handheld devices, laptops and floppy diskettes.

Access control lists

The registry that contains information about the users (groups, machines and processes) and the types of access mode that they are entitled to have is referred to as access control lists. They are more flexible and dynamic than permission bits for complex applications. They also contain advanced ACLs for finer precision

control.

Constraint user interface

Constrained user interfaces work on the principle that a user should be able to access system functions for which he/she is specifically authorized. Customised menu driven systems are common examples for constrained user interfaces. The immediate direct application of this concept Automated Teller Machine (ATM). The user is prevented from using other system interface and is prevented from bypassing the logical access controls.

Labels

In order to meet stringent security requirements, labels are frequently used as the basis for logical access control. An unchangeable label is given to each file that indicates its sensitivity. In addition user sessions are assigned to labels. This will determine the degree to which access to information at different sensitivities is granted.

Answer: [b] Host-based authentication.

Explanation: This is an external access control mechanism.

Module:5

Reference No:M5007

Question: Which of this is not an external access control mechanism?

- [a] Port protection devices
- [b] Secure gateways
- [c] Security Labels
- [d] Host-based authentication.

Module 5- External Access Control

The mechanism adopted to control interaction between the system and the outside world (people, systems and services) is termed 'external access control'. A dedicated physical device like a computer is installed between the system being protected and the network, for external access control. Such control makes use of host-based authentication, port protection devices and server gateways.

Host-Based Authentication

In conventional methods, the identity of the user making a request is established. In host-based authentication, the host source from where the request arises is identified instead of the user. This mechanism can be used when the legitimate host is located physically close to the host that is impersonating. Host-based authentication systems use RPC (Remote Procedure Call) and DES (Digital Encryption Standard) to provide secure identification of the client host.

A remote procedure call consists of the request/reply exchange, which functions as follows: The client places the operation code and other parameters in the request buffer (a temporary data

storage device), and on receiving a reply, it reformats the data in its sent form (since data sent is in encoded format). The server checks the capability, extracts the operation code and other parameters from the request. After this, it calls the appropriate procedure. The result of the procedure is placed in the reply buffer. However, it is easy to use/emulate host-based authentication, especially when the impersonating host is situated close to the impersonated host.

Port Protection Devices

A Port Protection Device (PPD) is one that is fitted to a communications port of a host computer, and authorises access to the port. This is done before the data packets arrive at the computer, and is independent of the computer's own access control functions. PPDs employ a separate authenticator with passwords to access the communication port. A dial-back modem is the best example for a port protection device. Here, legitimate users make a call to the system they want to connect with, types in the user ID and password, disconnects and waits for the system to call back at a prespecified number.

Secure Gateways / Firewalls

The primary security function of the secure gateway is to provide authentication of users. A program or a hardware device that enhances the security of the network by filtering data packets that enter or leave a network is a firewall. They also check for restrictions and perform 'accept' or 'reject' operations. Firewall technology can be used to give virtual access by using proxies. A proxy server (sometimes referred to as an application gateway or forwarder) is an application that mediates traffic between a protected network and the Internet. Proxies are often used instead of router-based traffic controls, to prevent traffic from passing directly between networks. Many proxies contain extra logging or support for user authentication. Firewalls use IP (Internet Protocol) filtering to permit access to only certain types of resources. Secure gateways may provide additional auditing and session monitoring. Gateways can also perform an intrusion detection function. For example, the secure gateway can monitor a session for keystrokes, which may indicate someone trying to exceed access.

Answer: [c] Security labels. These labels are deployed for internal access control under logical access control.

Module:5

Reference No:M5008

Question: Which of these components of NFS uses authentication?

- [a] Cache file system
- [b] Virtual file system
- [c] Mount protocol
- [d] Remote procedure call.

Module 5- Network File System

Host-based authentication is a method to implement external logical access control. Here, access rights are awarded to users based on the identity of the hosts, from whom the request originated. The best example of host-based authentication is the Network File System (NFS). It was developed by Sun Microsystems as a file server standard. NFS provides remote access to shared file systems across networks. NFS protocol uses the Remote Procedure Call (RPC) method for communication between computers.

What is NFS?

A distributed client /server system that allows users to access, store and update files/directories from a remote computer, and work on them as if it were their own, is termed as a Network File System. NFS is devised as a mechanism to create a file system on diskless clients (dummy systems). The NFS protocol is designed to be portable across different machines, operating systems, network architectures and transport protocols.

Concept

NFS incorporates the client-server architecture. The nodes/systems that make their files or directories available on request for remote access are termed as servers. This action of making essential files available is called as exporting. Terminals that use the server resources for access and processing are referred to as clients. The server does not store any information about the logons made from the remote clients, and adopts the stateless mode of transaction processing. This helps in recovering from network failures.

Remote Procedure Calls (RPC)

RPC is a library of procedures, which provides procedure-oriented interface to remote services. The procedure body has a code number that identifies remote procedure and parameters that are to be transferred to the remote procedure. The combination of host address, program number, and procedure number specifies each remote procedure. RPC employs authentication to identify the process from which the request originated. Digital Encryption Standards (DES) are used for encoded key based authentication to identify the issuing host. All these procedures are blocked, and do not return until they have been processed, which means that they are synchronous.

Mount protocol

Mounting is the action of designating a file accessible. Using NFS, the user or a system administrator can mount the whole or a portion of a file system. The portion of the file system that is mounted can be accessed depending on the privileges for access to each file (read-only or read-write). NFS clients attach remote directories to a mount point in the local file system. An empty directory created to attach a remote file system is a mount point. Mount protocol enables the server to grant remote access privileges in order to restrict the number of clients.

Cache file system

A cache is a place to store data temporarily. Computers include caches at several levels of operation, including cache memory and a disk cache. Caching can be implemented for Internet content by distributing it to multiple servers that are periodically refreshed. A file caching mechanism that enhances NFS performance by reducing server and network load is CacheFS. It increases the client-per-server ratio, and increases the speed of data transfer for slow running clients that use Point-to-Point Protocol (PPP).

Answer: [d] Remote Procedure Call. RPC employs Digital Encryption Standard (DES).

Module:5

Reference No:M5009

Question: Dial back modem uses which of the following feature for external access control?

- [a] SLIP protocol
- [b] Port protections
- [c] Point-to-Point Protocols

[d] Blue boxes.

Module 5- Dial back modem

Port Protection Devices (PPD) are deployed to act as means of external access control in the port itself before the data enters the access area. A port protection device (PPD) is an external device fitted to the communication port of a host computer. It authorises access to the port, prior to and independent of the computer's own access control functions. A PPD can be a separate device in the communications stream. Dial back modem is one such PPD.

Basic concept

Dial back operation starts with the legitimate user making a call to log on to a remote system. The user after entering the user ID and password disconnects, and is put on waiting mode. The remote system calls back at a prearranged number.

Working

A list of valid user logins and phone numbers are stored by the dial back modem. After the user dials and disconnects, the modem cross checks these details with its stored data and then calls back. Hackers cannot gain access because the listed details will show a mismatch. These modems are suitable for immobile applications and in SLIP (Serial Line Input Protocol) and PPP (Point to Point) protocols usage.

Vulnerabilities

- It is possible for a hacker to use special equipments and connect to the modem (after it has cross checked). Giving the answerback tone in tandem with the legitimate callers tone can get through the tone detecting circuitry in a modem without verification.
- Test connections are established through the telephone switches called as "blue boxes" for testing and checking. Even one of the dial out tones from this test line could be picked by intruders to access test ports and trunks.
- Outdated caller control switches use the same line for dial in and dial out, making it most insecure for dial up operations.

Security

Security can be enhanced in a dial back modem by the following measures:

- i. There should be separate lines for incoming connection requests and dial-back. This measure effectively curtails a hacker from getting into the network.
- ii. Random time delays between dial in and dial back periods.
- iii. Enable the modem to answer during the wait period. This would reduce the vulnerability to a great extent.
- iv. Special techniques to check if the modem is in original state or answer mode can be introduced to recognise the original legitimate call.
- v. Dedicate a separate one-way line and modem for dial back operation increases the security, in particular when the dial out line is not easily traceable by an intruder. Employ dial out only lines, which comes with a trade-off between security and costs.
- vi. Call forwarding is done whereby the incoming calls are forwarded on the dial out line to the security office. But, this could be cancelled randomly by the central office software reboots.
- vii. Reprogramming the microchip in the modem to monitor line state provides secure connection for the dial back line. Dial back facility through dedicated dial-out lines provides good security.

Answer: [b] Port protection.

Question: Which of these access control mechanisms is not based on multi-level security?

- [a] Mandatory Access Control (MAC)
- [b] Discretionary Access Control (DAC)
- [c] Role Based Access Control (RBAC)
- [d] Internal Access Control.

Module 5- Role Based Access Control (RBAC)

Security is a critical area of access control administration. To ensure security, various mechanisms like Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role-Based Access Control (RBAC) are adopted. RBAC complies with the natural structure of an organisation, where functions are grouped into roles, and users often have to fulfil one or more roles. It is appropriate for systems that process unclassified, but not for sensitive information and classified information.

Evolution

Access control security standards and guidelines specify DAC, MAC and RBAC as the primary means of access control.

- DAC permits individual users to grant and revoke access privileges, without the intervention of the system administrator.
- MAC restricts access to data based on varying degrees of security requirements, for information contained in the objects. Information is associated on the basis of multi-level security requirements with labels like 'Confidential', 'Top Secret', and 'Secret'.
- RBAC evolved from MAC, and access control decisions are based on the roles of individual users in an organisation.

What is RBAC?

The access control mechanism whereby access rights are based on the roles of individual users within an organisation is termed RBAC. Users are assigned roles according to their functional responsibilities or designation. The role defining process is done after an intricate analysis of the organisation and its functioning.

Framework

Individual users are granted roles on the basis of their competencies and responsibilities within an organisation. Operations that a user is permitted to perform are based on his role. Role associations simplify the administration and management of privileges. Roles are updated, without changing the privileges for every user on an individual basis.

Role hierarchy

Sometimes, employees who perform similar operations may be assigned different roles. In such situations, role hierarchies are established that reflect the natural structure of an organisation. Role hierarchy defines a roles with unique attributes, yet includes operations that are associated with another role.

Integrity

Ensuring integrity of data is an important consideration in RBAC. Authorised roles are allowed to modify and process data. Integrity is ensured, despite the complexity of transactions within an

organisation. Certified and trusted transactions provide absolute integrity. For example, a bank teller and accounting supervisor perform similar functions, but of different processes/output. A teller in a bank takes care of savings deposit transactions. This requires read and write access to specific fields, within savings and transaction log files. An accounting supervisor executes correction transactions, requiring exactly the same read and write access to the same files, as the teller.

Advantages

- Greater flexibility and range of applications: Definition of roles, role hierarchies, relationships and constraints, gives wide scope for authorised access control in an organisation.
- Integration with OOT: adapting the concept of 'methods' in RBAC can incorporate Object Oriented Technology. This finds optimum usage in operating systems and other applications.
- Distributed systems: Administration responsibilities are divided among central and local protection domains through RBAC. This feature is more appropriate for distributed computing systems.

Answer: [c] Role Based Access Control (RBAC).

Module:5

Reference No:M5011

Question: Which feature of RBAC specifies event-triggered conditions?

- [a] Role perspective
- [b] Role activation
- [c] Role hierarchy
- [d] Role based management.

Module 5- Role Based Access Control-Features

A group of security mechanisms that restrict access to resources in an organisational information system, through identities/ roles is termed as Role Based Access Control (RBAC). Features of RBAC include role perspectives, role activation, role hierarchy and role based management.

Role perspectives

The basis on which roles are assigned to different users in an organisation depends on relationships, convenience and the like.

- Group by relative relationship: The mode of interaction between members of an organisation, and the relationship they share for discharging their duty is the basis of this classification. It establishes sub-roles also. As in the case of managerial roles that differ depending on projects, people or technology.
- Group by organisation: This is the conventional view of an organisation, as consisting of various segregated roles that make up the composite whole.
- Group by convenience: Here, the ease of reference through which authorisations can be manipulated and assigned in a flexible manner, is taken as the criterion for classification.
- Group by selection: Grouping by capability is similar to access control used in a workflow process.

Role hierarchy

Each role possesses unique attributes that differentiate it from another. However, some attributes/properties are common to different roles. This means that one role may contain operational characteristics possessed by another. Operations and roles are dependent on organisational policies and constraints. For example, in a hospital, an individual may don the role of both doctor and intern. There are distinct operations that could be carried out in a hospital by doctors and interns. A person assigned a role of intern can do operations related only to an intern, and not that of doctors. Further, a doctor can do the role of a cardiologist, a neurologist and the like. Authority and responsibilities of individuals in an organisation is realised through role hierarchies. Roles can have overlapping responsibilities and privileges. Thus, when operations overlap, hierarchies of roles can be established. Role hierarchies take cardinalities and other integrity constraints into account, while resolving overlapping of various roles.

Role activation

Typically, RBAC framework and policy constraints of where, when and what are not sufficient to activate a role that has been conceptualised. These conditions are enabled dynamically and some of them include the following:

- Qualification: A dynamic attribute that suggests a user may have a different role depending on circumstances is qualification.
- Event-triggered: For a role to be activated, a composite condition involving other events has to occur. Based on this condition, activation takes place as soon as, pre-set events get triggered/enabled.
- Delegation or transfer: This is in keeping with the normal transfer of authority in an organisation. It specifies whether or not the granter of access retains the authority, as it is passed on within a hierarchy. For example, a manager delegates authority to a subordinate, as empowerment; while the manager transfers authority to a replacement, if he/she leaves the organisation.

Role based management

RBAC is used as a tool to simplify and improve administration of access rights, within an organisation. Based on organisational roles, duties and authorities, the concept of Role Based Management has evolved. It identifies the concepts of obligation policies and object orientation.

- i. Each role has responsibilities to fulfil. In addition, authorisations are explained through obligation policies. Security administrators are obligated to ensure proper configurations with regard to vulnerability analysis, and to maintain surveillance with intruder detection software.
- ii. Defining a role in terms of obligation and authority, through a set of management policies will allow for organisational restructuring, and does not require policy manipulation. This is conveyed through the object orientation principle.

Answer: [b] Role Activation.

Question: Which transmission impairment is dependent on propagation velocity as a function of frequency?

- [a] Attenuation
- [b] Noise
- [c] Delay distortion
- [d] Cross talk.

Module 5- Transmission impairments

Data transmitted through communication networks are subjected to a number of disturbances and distortions. Thus only part of the signal from the source reaches the destination, resulting in loss of data. Such elements that are responsible for losses and hinder the proper transmission and reception of signals are termed as transmission impairments. The commonly encountered transmission impairments are attenuation, noise and delay distortion.

Attenuation

The loss in the strength of a signal as it is transmitted over a distance is called as attenuation. Attenuation can occur in case of both digital and analog signals. The unit of measurement of attenuation is decibels (dBs).

Attenuation power is given by the formula:

$$A_p = 10 \log_{10} (P_s/P_d) \text{ dBs}$$

Where P_s is the signal power at the transmitting end (source) of a communications circuit and P_d is the signal power at the receiving end (destination) and $P_s > P_d$.

The efficiency of the cables used to transmit signals is inversely proportional to attenuation. For long distance signal transmission, a communication hardware device called as repeater is inserted. Other devices like amplifiers and equalisers are also used to enhance the signal carrying capacity of the cables. Signal to noise ratio (SNR) is the measure of signal strength relative to background noise. This ratio has to be kept as high as possible to minimise attenuation.

Noise

Any form of unwanted electrical or electromagnetic signal/disturbance that degrades the quality of signals and data in a communication channel is termed as noise. Noise is inherent of digital and analog systems and hinders communications of all types. Even files including text, programs, images, audio, and telemetry are affected by noise.

In telephone network circuits external noise is generated from appliances in the vicinity, electrical transformers, the atmosphere, and from outer space. Noise originating from outside the system is inversely proportional to the frequency, and directly proportional to the wavelength. The internal noise generated from wireless devices is less dependent on frequency.

The following categories of noises interfere with communication channels:

- Thermal noise: The noise generated by thermal agitation/movement of electrons in a conductor. All communication devices exhibit thermal noise.
- Intermodulation noise: When different signals with different frequencies and their multiples interfere with the original signal due to non-linear effects, intermodulation noise is produced.
- Crosstalk: When signals from different media intermingle with one another, it leads to a coupled signal. Coupling of signals with the nearby media/adjacent cable results in undesirable noise and disturbance called crosstalk.

- Impulse noise: Random noises that are of large amplitude emanating from sources like lightning and elevators fall under this.

Delay distortion

Signals are transmitted as sine waveforms for modulation and demodulation in a communication system. In a waveform consisting of two or more wave components at different frequencies, distortion caused by the difference in arrival times of the frequency components at the output of a transmission system is called as delay distortion. This distortion arises due to the fact that propagation velocity (the speed at which the signal travels over the communication medium) is a function of frequency.

Answer: [c] Delay distortion.

Module:5

Reference No:M5013

Question: Which access control mechanism does security label fit into?

- [a] Logical access control
- [b] Discretionary access control
- [c] Physical access control
- [d] Mandatory access control.

Module 5- Security Labels

Discretionary Access Control(DAC) systems grants or revokes access based on the discretion of the individual user . It has its limitations. This is true to every application of DAC. For example, in the case of SQL (Structured Query Language), users can grant or control access to data. Though access to a relation is strictly controlled with 'SELECT' it automatically permits the creation of a copy. Moreover, programs infected with Trojan horses can cause havoc .

What are security labels?

To overcome these limitations of DAC, another control mechanism termed as Mandatory Access Control (MAC) has been evolved. MACs are based on security labels associated with each data item and each user. Security labels are associated with databases that impose multi-level security such as TOP SECRET, SECRET and CONFIDENTIAL to the data. The security label on a data item is called a security classification. The label on a user is termed security clearance.

Structure

Security labels have a lattice structure , and consists of two labels, S for Secret and U for Unclassified. S information is not allowed to cross into U data items. This condition is met by applying three mandatory access controls rules:

- Simple security property whereby a U-user cannot read S-data.
- Star property wherein a S-user cannot write U-data. This would prevent any secret data being accidentally written into 'U'. The (weak) star property allows a U-user to write S-data. This results in overwriting and destruction of S-data by U-users.
- Strong star property where a S-user cannot write U-data, and a U-user cannot write S-data. In order to ensure integrity, the strong star property limits users to writing at their own level.

Database integration

Granularity is the relative size, scale, level of detail, or depth of penetration that characterises an object or activity. It can refer to the level of hierarchy of objects or actions, to the fineness of detail in a photograph. In an RDBMS, security labels are assigned to data at different levels of granularity. Assigning labels to entire relations or columns of a relation is useful, but inconvenient. For example, if some salaries are secret but others are not, these salaries must be placed in different relations.

However, when each row (tuple) at the user level is labelled, it is said to have achieved the finest granularity. This offers considerable flexibility, and is labelled at the level of a tuple. This approach is definitely more convenient than using relation- or column-level labels.

Labels in distributed systems

Users and data with different security labels coexist in a multilevel system. Security labels are incorporated in three viable architectures, which include:

- Integrated data architecture (Trusted subject architecture).
- Fragmented data architecture (Kernelised architecture).
- Replicated data architecture (Distributed architecture).

Answer: [d] Mandatory access control.

Module:5

Reference No:M5014

Question: Object control is widely used in:

- [a] Single user systems
- [b] Multi-user systems only
- [c] Multi-user and distributed systems
- [d] Distributed systems only.

Module 5- Object Control

Object control is of great significance in distributed computing systems. It is essential to control access to individual objects and methods. In large distributed systems, lots of data/control information get accumulated, and becomes difficult to handle. A scalable access control mechanism has to be implemented in a distributed object oriented system. Moreover, most system implementations are multi-user. This leads to several users trying to update/modify the same objects/data at the same time.

What is object control?

An object control provides access to specific rows in specific database tables. An Enterprise Service Object control provides access to an enterprise service and its members. For example, one row in the Enterprise Service table and related rows in the Enterprise Service Member table are controlled by an enterprise service object.

What is object concurrency control?

It is the control strategy through which updates and modifications made to the same object by multiple users are resolved, and reflected.

Concept

The fundamental idea behind control is to preserve the integrity of data and transactions in tandem with

changes in technology. To support multiple users working on the same object, the system develops clones/copies of the object for each user. Thus, concurrency control synchronises updates to an object.

Figure: Concept of Object Concurrency control

The figure above shows a source object, which may be a C++ object, a row of data in a relational database and the like. The object clones/copies may be in the form of entity beans in an Enterprise JavaBean (EJB) application server or java objects of an HTML page.

Control strategies

The three basic object concurrency control strategies are pessimistic, optimistic and truly optimistic.

Pessimistic: Sources are locked for the entire time, till a clone is created. Other clones are not allowed to exist, till the clone that has been locked has finished its transaction. The appropriate source is locked by the clone that seeks to make changes. Simultaneous access to common objects is blocked by pessimistic control, and is most suitable for small-scale systems.

Optimistic: The source is marked each time it is accessed by any of the clones. Access implies a refreshed clone or another copy. The clone is then modified in accordance with the requirements of the user. After changes are made, the clone locks the source, and ensures that another clone does not update the mark placed on the source. This mechanism is widely used in large systems and for systems with regular concurrent access.

Truly Optimistic: Changes to the source are updated by software, without the usage of locks and marks. Single user systems and static web sites can make best use of the truly optimistic control strategy.

Collision

In optimistic concurrency control, the 'mark' on the source when updated indicates that another clone of the source has accessed it. The instance at which the clone discovers this action is termed as collision. False collision is when two users delete the same object or make the same update. Software makes it easy to handle such collisions.

Answer: [c] Multi-user and distributed systems.

Module:5

Reference No:M5015

Question: Which application of Biometrics employs speech recognition systems?

- [a] Employee records
- [b] Telecommunications
- [c] Banking
- [d] Forensics.

Module 5- Biometrics-Applications

Biometric applications are used in various areas, ranging from physical access control to restricted areas/data to law enforcement, banking and finance. Biometric technologies like fingerprint scanning, hand geometry, iris/retinal scan, voice/pattern recognition and the like find specific usage in allied industrial and commercial applications. Some of these applications are used to enable computer access, electronic benefit transfer, and in national identity, immigration, physical access, forensic, and time and

attendance systems.

Computer access

Computer systems and networks like the Internet are exposed to fraudulent access and usage. This leads to under utilisation of network capability. Biometric technologies like finger print scanning, hand geometry and the like find extensive use in securing banking data, business intelligence, credit card numbers, medical information and other personal data.

Physical access

Securing the physical movement of people in places such as schools, nuclear power stations, military facilities, theme parks, hospitals, offices and supermarkets is essential to minimise security threats. Applications use biometric tools to ensure access restrictions in home and car security systems also.

Telecommunications

The rapid growth of telecommunication infrastructure and networks has increased vulnerabilities to fraud and misuse. This demands more stringent security measures, particularly in the case of cellular, mobile and wireless systems and Dial Inward System Access (DISA) services.

Stolen code numbers are fed into new phones, and users feign to be legitimate subscribers. This is known as cloning. Telephone hackers are targeting DISA that allows authorised users to contact a central exchange, and make free calls. To tackle the problem, voice recognition and speech identification techniques like speaker ID that uses biometrics are employed.

Employee records

Manual systems for maintaining employee details like time they arrive at work, take breaks, and leave for the day can be rendered ineffective, by impersonation /punching in for someone else. This is commonly termed "buddy punching". It reduces productivity and increases overhead costs for companies. Biometrics prevents misuse of the system, and is integrated with time management software, to produce management accounting and personnel reports.

Banking

Banks require enhanced security systems for services like ATM transactions, credit cards, online banking, telebanking, mobile banking and the like. Any breach of security results in considerable loss to the bank and the consumer. Automated Teller Machines (ATMs) and transactions at the point of sale terminals are vulnerable to fraud, and can be secured by biometric technologies like finger print scanning, hand geometry and face recognition. In Electronic Benefits Transfer (EBT), funds are loaded electronically onto a plastic card. The card can then be used for purchasing, where point-of-sale smart card readers are installed.

Forensics

Criminal identification and prison security are important applications of biometrics in forensics. Law enforcement agencies use biometrics to identify, track and locate criminals. Prisons use biometrics to securely detain prisoners. Wide ranges of biometric devices are employed in police detention centres to enforce home confinement orders, and regulate the movement of probationers and parolees.

Immigration

Terrorist activities, drug trafficking, illegal immigration and an increasing number of travellers forces immigration authorities to follow procedure with utmost care and security. Governments use biometrics to automate the flow of legitimate travellers and deter illegal immigrants, by as well as, to record population growth, identify citizens, and prevent frauds from occurring during elections.

Answer: [b] Telecommunications.

Question: A data unit 01000101 sent from the source was received as 01111101. What is the type of error?

- [a] Single-bit error
- [b] Byte error
- [c] Burst error
- [d] Spike error

Module 5- Error concepts

Data must be transferred accurately, without affecting integrity. The network must guarantee accuracy while transmitting data. However, due to defects in the transmission media and electrical power surges, errors tend to creep in, but they have to be detected and corrected.

In the OSI model, error detection and correction can be handled either in the Data Link layer or in the Transport Layer.

If the voltage fluctuates, the bits may change, affecting message integrity.

There are two types of errors:

1. Single-bit errors

In this type of error, only one bit in the entire message is changed, either from 0 to 1 or from 1 to 0. Information exchange over a network takes place by binary representation. In this representation, data is converted to a sequence of 1's and 0's. For example, the letter 'A' in the American Standard Code for Information Interchange (ASCII) has the value 65, which in binary form, is 1000001.

This binary value is transmitted over the network, in the form of electrical pulses. Disturbances from unwanted electrical sources corrupt the binary data and change the entire message. For example, a change from 0 to 1 in the second last bit changes the ASCII value to 67, which represents the character 'C'.

The probability of single-bit errors occurring is very small, since a noise for mere 1 microsecond is required to cause a single-bit error. If the noise persists for more time, more bits get corrupted and the message becomes garbled. However, such errors are common if we send data in parallel mode, in which many wires are used to simultaneously to send data, with each wire carrying one bit at a time.

2. Burst errors

When noise voltages occur for a long duration, then more than one bit may get corrupted. Such errors are termed 'burst errors'.

In a burst error, consecutive bits may not be damaged, only some bits in the entire message may change.

The distance between the first error bit and the last error bit is termed as the "length" of the

burst. This type of error is common when transmitting data in serial mode, i.e. data is transmitted bit by bit. The speed of transmission, referred to as the 'data rate' and the duration of the noise voltage influences the number of bits that are changed or corrupted. A data rate of, say 56 Kbps (normal speed of a dial-up modem) and a noise of 0.01 second can corrupt 560 bits. The number of bits corrupted is given by

No. of bits corrupted = 56000 bits per second $\times$ 0.01 second.

If the speed of transmission is increased by a factor of 1000 to 56 Mbps, then the number of bits corrupted increases to 560000 bits, i.e., the corrupted number of bits is proportional to the speed of transmission.

To detect error, a number of methods can be adopted. But the most commonly used concept is 'redundancy', in which the computer adds information to the original message. The receiving station then uses this additional information to check for errors. After checking whether the entire data has been received, the receiving station discards the redundant information.

Answer: [c] Burst error. Explanation: When noise voltages occur for a long duration, then more than one bit may get corrupted and this type of error is called burst error.

Question: Which of the following methods can detect burst errors only if the number of errors is in each data unit is odd?

- [a] Vertical Redundancy check (VRC) - even parity
- [b] Vertical Redundancy Check (VRC) - odd parity
- [c] Longitudinal Redundancy Check (LRC)
- [d] Checksum

Module 5- Error- Detection I

For reliable transmission, it is necessary to ensure that messages are transmitted without any errors from source to destination. A method that can detect errors must be simple to implement in either hardware or software, and fast enough for real time data transmission.

One such technique is to send the data twice, so that the receiving station can compare these two messages, and find out if there is any error in transmission. However, this takes up a lot of time and uses up valuable bandwidth, since every set of data has to be transmitted twice. A better way is to add some information in addition to the data, which then can be used by the receiving computer to detect errors. This concept is termed 'redundancy'.

This is implemented as follows:

1. The data to be transmitted is passed through an algorithm that inspects the data, and generates appropriate redundant information that can be added to the original data.
2. This data and redundant information is packaged into one single unit and transmitted.
3. When the receiving station gets the information, it removes the redundant part from the message. Then it applies the same algorithm to the original message and computes its own redundant set of data.
4. The receiving station compares the redundant data received from the sending station with that generated by it. If there is any discrepancy, then an error has occurred during data transmission.
5. If there is no error, then the redundant information sent by the sending station is simply discarded.

There are four types of error-detection methods that use redundancy. They are VRC, LRC, CRC and checksum. VRC and LRC are discussed here.

- **Vertical Redundancy Check (VRC)**

This method is most often used for error detection, and does not consume much resource. This method is also referred to as a 'parity check'. A redundant bit is added to the end of every data unit, such that the total number of 1's (or 0's) is even for even parity check.

For example, assume that the binary data unit 1000101 is to be transmitted. There are three 1's in the data unit. A parity generator is used to convert this odd number into an even number by appending 1 to the data unit, making it 10001011. When the receiving computer receives this data unit, an even-parity checking algorithm is used, which evaluates the number of 1's in the received data unit. If the number of 1's is even, then it is accepted as accurate. If there is a bit error, then the data unit becomes 10001111, which has an odd number of 1's. This means that an error has occurred in transmission.

This type of parity checking is termed 'even-parity'. Parity checking can also be done using an 'odd-parity'

algorithm, where the number of 1's is kept odd.

This means that VRC can detect all single-bit errors. A drawback in the VRC is that burst errors can be detected only if the number of errors is such that the data unit has violated the parity checking principle. For example, if the transmitted bit is 1000101 and uses even parity, then the data unit becomes 10001011. If two errors occur and the data unit becomes 10011001, then the even-parity checker at the receiving end finds an even number of 1s, and hence the erroneous data unit passes the test though there are errors.

- **Longitudinal Redundancy Check (LRC)**

In this method, a data unit of 32 bits is divided into a table with 4 rows and 8 columns. Parity information is computed for each column, and then appended as a new row. The algorithm works such that the first bit for parity in one column is computed on the basis of the first bits in all the columns. The second parity bit is computed by taking the second bits in all the columns, and so on. For example,

11000011 00110011 00011110 11001100 is made as

11000011
00110011
00011110
11001100

LRC 00100010

The data is sent like 11000011 00110011 00011110 11001100 00100010

The advantage of the LRC over the VRC is that this method can detect all single-bit errors and all burst errors of a size equal to the number of columns in the LRC table.

A LRC may also detect errors more than this number, but no guarantees can be given as to its success. However, one type of error escapes this method. If two bits in one column are changed and two bits in another column in the same position of the table are also changed, then the LRC cannot detect the errors. E.g., If the data is 11100010 and 11000011 and if the first and last bits in each of them change to make the data unit read as 01100011 and 01000010, this error cannot be detected with LRC.

Answer: [a] Vertical Redundancy check (VRC) - even parity.

Explanation: If even parity is used, then the received data unit is checked for even number of 1's . If the number of errors is odd (number of 1's is odd), then an error has occurred, which is detected.

Question: Which of the following method uses binary division to check for errors during transmission?

- [a] Checksum
- [b] Cyclic Redundancy Check (CRC)
- [c] Vertical Redundancy Check (VRC)
- [d] Longitudinal Redundancy Check (LRC)

Module 5- Error- Detection II

Communication systems must accurately deliver information sent by one computer to another. To achieve this, there must be way to detect errors when they occur and inform the communicating entities of the error.

There are many methods to achieve this, but all of them use the common concept of redundancy. Additional information, generated from the message itself, is appended to the original message and sent by the sending station. The receiving station generates its own version of the redundant information and compares it with the one sent by the source. If there is no discrepancy, then the message has been transmitted without any errors. Else, an error has occurred and then it is up to the higher layers to recover from the error.

Cyclic Redundancy Check (CRC)

CRC is the most powerful of the algorithms that uses redundancy to check for transmission errors.

Unlike the VRC and LRC which use addition, the CRC uses modulo-2 binary division. A sequence of redundant bits called CRC remainder is appended to the data in such a way that the data now is divisible by another binary number, which is also predetermined. At the receiving end, the entire data with the CRC is divided by the same predetermined number. If the results shows a remainder, it is taken as "data corrupted." The CRC is determined using an algorithmic polynomial. This polynomial is determined before the CRC process begins. The remainder of this division is called the CRC or the CRC remainder.

There are two conditions for the CRC:

- It must be one bit less than the Generator polynomial (the divisor)
- After appending the CRC to the original data block, the resultant message must not leave any remainder, i.e., it should be exactly divisible.

The following steps demonstrate how the CRC algorithm is used for error detection:

1. A generator polynomial is determined and the original data block is converted into a binary sequence.
2. A string of 0's is appended to the data block. The number of 0's to be appended is one less than the number of bits in the binary data block.
3. The resulting sequence is divided by the Generator, with the remainder being the CRC.
4. This CRC is now appended to the original data, after removing the previously appended 0's. When the remainder is appended, the original message is now perfectly divisible by the Generator

- polynomial, i.e., the remainder is now zero. This message is transmitted to the receiving station.
5. At the receiving station, the message is again divided by the generator polynomial. If the remainder is zero, then the data block has been transmitted correctly, but if it is not, then an error has occurred. The CRC Checker does the error checking process at the receiving end.

CRC can detect the following errors:

- All single bit errors
- All burst errors that affect an odd number of bits
- All burst errors whose length is equal to or less than the highest power of the generator polynomial
- All burst errors greater than the degree of the polynomial can be detected with more guarantee of success than other methods

The commonly used CRC algorithms are CRC-16 and CRC-32.

Checksum

Lower layers in the OSI model and the TCP/IP Protocol Suite, like the Data Link Layer mostly use the error detection methods discussed so far. Higher layers like the Transport Layer use another method called 'Checksum.' This method is most used in the TCP protocol.

In this method, the Checksum generator breaks up the data block into equal units, usually 16 bits each. These units are then added using an arithmetic method called "one's complement". The resulting bit sequence is then corrected, if necessary, to be equal to the number of units.

This sum is again complemented, i.e., each 1 is inverted to 0 and each 0 is made 1. For example, if the sum is 11000111, then the complement is 00111000.

After complementing the sum, it is appended to the original data block and sent to the receiver. At the receiver, a Checksum checker again divides the data (along with the checksum) into the same number of units and adds all the units. The sum is again complemented and if the sum is zero, it means that there is no error in transmission. If the complement is not zero, then an error has occurred in transmission.

If the error has odd number of bits, Checksum algorithm can detect it. The algorithm also can identify errors with changes in even number of bits, but the probability is slightly less than those with odd number of bits.

However, if an error occurs such that a bit in one unit and the corresponding bit or its complement in another segment gets corrupted, then the Checksum algorithm fails to detect it.

Answer: [b] Cyclic Redundancy check (CRC).

Explanation: The cyclic redundancy check method uses binary division for error detection.

Question: The auditor before commencing audit of access controls should obtain the following information by interviewing the organisation's staff

- [a] IT organisation structure
- [b] Key business activities
- [c] Significant changes to network
- [d] Method of authorising access

Module 5- AUDIT OF ACCESS CONTROLS

Information system consists of hardware, software, communication facility, online transaction facilities, database etc. The information systems are valuable resources of the organisation. These assets must be protected from unauthorised use, damage, loss or modification. The management must control the access to such resources. This assures that there is control over deliberate or accidental errors caused by improper use or manipulation of data files, unauthorised or incorrect use of computer programs and improper use of computer resources. The auditor during the course of audit of access controls must ensure that there is an effective access control mechanism.

Pre-audit

- Before commencing the audit, auditor should have knowledge of the information assets, location of these assets, the persons in charge (custodian), and the persons responsible for authorising "who will access what assets/resources and for what purpose". The auditor should also note the person responsible for implementing such authorisation and maintenance of the same.
- The auditor should interview
 1. Documentation librarian
 2. Programming manager - Systems and applications
 3. Data Base Administrator
 4. Director of Data Processing
 5. Users of application
- While interviewing the auditor should try to find out
 - (i) The method of authorising access to assets
 - (ii) The method of accessing the assets (programs, data files, database etc.)
 - (iii) The actual process of access (through logs)
 - (iv) Process of handling access breach
- He should get the knowledge of what are the types of hardware and software access control mechanisms are implemented. Each type of IT asset needs different types of access control either controlled at the system level or application level or operating system level.

Audit

Following are some of the items that the auditor shall specifically look into

- Policies for access security:
 1. The access control policy should be obtained. The auditor should ensure that the policy is complete.
 2. He should interview security administrator and the other users in the organisation to make sure that the policy is being implemented and have been understood by them.
 3. The logs should be scrutinised to determine if there has been any unauthorised access.
 4. The procedure for reporting and investigating the violations should be understood.
- Access to system software:

The auditor should determine if the access to systems software is restricted to authorised

persons. He should interview the authorised person and review the logs to see that only authorised persons are able to gain access. He should also ensure that access to systems software is limited by terminal address.

- Access to production programs:

The programs should be protected through passwords and other utilities. The auditor should review the effectiveness of controls by interviewing the person responsible for controlling the access to programs source and object code and that the access is on "need to know" basis.

- Access to data files:

The review of access to data files should be by examining the controls over processing of programs in the library against data files and the access to such data files.

- Access to online systems: It should be reviewed that

1. The users of the data have authorisation from the owner of the data.
2. Terminal address and hours of operation is used to limit the access to applications, data and updating of transactions.
3. Information that is not to be disclosed is adequately protected.

- Access to program documentation:

The auditor should ensure that the documents are adequately secured. The access to the information that is in printed form or online should be observed. The logs should be scrutinised to determine that only authorised persons are gaining access to documents.

- Password administration:

1. Determine the frequency at which the passwords are changed.
2. Verify whether the passwords of the employees who have left the organisation are deleted.
3. Verify access to password tables and it is on "need to know" basis.
4. Verify the limit on the number of unsuccessful attempts to login.

The auditor should ascertain that the weaknesses in the above controls are properly compensated by some other controls. If they are not then the same should be reported to the management.

Answer: [d] Method of authorising access.

Module:5

Reference No:M5020

Question: Host 1 wants to prove its identity to Host 2. Host 2 is also authenticating Host 3, but by mistake uses Host 1's credentials. This is possible in which type of authentication?

- [a] Zero Knowledge Proofs
- [b] Message Digests.
- [c] Kerberos
- [d] Token Authentication

Module 5- Authentication

Authentication, in the context of computing, refers to the verification of the identity of a user before access is given to resources.

To perform an operation on a computer, a user must first have to prove his identity to the authenticating entity and then prove that he has permission to perform that operation. For example, if a user wants to open a file on a computer, he must first login to the computer using a user id and password. The privileges assigned to that user

by the authority then determine whether he can open the file or not.

Authentication of a user does not mean that he has permission to do whatever he requires. However, authentication is the most important aspect, since checking for permission is accomplished simply by looking up the privileges assigned to the user.

There are numerous methods of user authentication, each having its own advantages and disadvantages. They are enumerated below:

Hash functions and Message Digests

A hash function is the mathematical computation applied to a message in order to generate a digest (small string) that will represent the whole file or message (large strings). This resulting data is called the message digest. A Message digest can be defined as the digital fingerprint of a message. The length of the message digest does not vary irrespective of the length of the original message and is fixed around 128 to 160 bits depending on the algorithm used. It is not possible for any person to guess the original message by looking at the message digest. If there is even a difference in one alphabet, the message digest is entirely different. Also, it is not possible to get an identical message digest from two different messages. Hence, a message digest is also known as a "one-way hash function". Since generating a public key for a big message is very slow, message digests are used for creating digital signatures.

Zero-Knowledge Proofs

This little-known method involves host-to-host authentication, so that there is no necessity to transmit confidential information like passwords. In this method, many steps are needed for authentication. The host, which is to be authenticated, devises a complex problem and then solves it. It then transmits the solution along with the problem to the authenticating host after committing it using a special scheme. The user must then prove the committed solution is the solution to the problem. It is like solving a problem in an exam to demonstrate knowledge of the solution. Many such communications may take place before full authentication takes place.

The zero-knowledge proof authentication method also has some drawbacks. The easiest and most often used attack is as follows:

Host1 gets an authentication request from Host2. Host2, in turn, passes on to Host3 all Host1's messages, pretending as if it is Host1. This is similar to the man-in-the-middle attack in encryption.

Token Based Authentication

It is possible for a user to be authenticated by using a physical object which has a special characteristic built into it. Such authentication mechanism is called Token Based authentication. For example, smart cards and biometrics are examples of such tokens.

The physical features of a token, such as shape, nature and materials from which it is made are termed as the 'form factor' of that token. The form factor is response for the usability and durability of the token. Tokens can be classified into two major categories:

Memory Tokens

In this type of token, the information required for authentication is stored in the token itself in of electronic or magnetic form. Duplicating such tokens is impossible since it is difficult for a person to know how the token is read or written to by devices. Tokens with memory cells using Integrated Circuits and magnetic cores are the most widely used. An additional security layer is achieved by encrypting the information stored on the card. Typically, the user has to enter an Identification number which is then used to decrypt the data on the card, so

that mere reproduction of even the encrypted data cannot is not very useful.

Microprocessor Tokens or Smart Tokens

Microprocessors are now being increasingly used in token based authentication systems. These tokens consist of a microprocessor that is able to make intelligent decisions in real time, i.e., it can make calculations during operation of the token. This is the reason such tokens are termed as smart tokens. Smart tokens also require some sort of Identification Number to be entered before data is read or written by devices. This prevents an attacker from manufacturing a device (called a host system), which can read data from the token. Some Smart tokens also contain memory along with the microprocessor in which some programs can be stored. The microprocessor can execute these programs to perform certain operations depending on the application for which the token is used. Such programs embedded into the token are called firmware.

Kerberos

The Kerberos authentication protocol uses a Key Distribution Centre (KDC) to provide authentication to users wanting to access confidential data. The protocol uses encrypted 'tickets' provided by the KDC to verify the authenticity of the users. The steps in the Kerberos protocol are given below:

1. The user sends a request to a workstation for accessing a particular service. The workstation then sends a request to the KDC to send a ticket for that user.
2. The KDC, which stores the secret keys for the user and the service, generates a ticket which is valid only for a certain amount of time. This ticket is then encrypted using the client's secret key.
3. The KDC then sends this encrypted ticket to the user.
4. After receiving the ticket from the KDC, the workstation asks the user to enter his password which is then encrypted. The encrypted password is nothing but the secret key of the user with the KDC. This key is used to decrypt the ticket sent by the KDC and verify that it is valid. Then the user creates another ticket containing its identity and encrypts it using the secret key. This is sent to the KDC.
5. The KDC decrypts it, verifies that the user indeed has sent the ticket and provides the service asked for by the user.

Answer: [a] Zero Knowledge Proofs.Explanation: The easiest and most often used attack in Zero Knowledge Proofs is as follows: Host1 gets an authentication request from Host2. Host2, in turn, passes on to Host3 all Host1's messages, pretending as if it is Host1.

Module:5

Reference No:M5021

Question: Direct Manipulation Interfaces (DMI) cannot help reduce?

- [a] Error-rates
- [b] Learning time
- [c] Easy remembering of operations
- [d] System resources

Module 5- Direct Manipulation Interfaces

For computer systems to be usable by average users, they must satisfy five main criteria:

- Learnability: It should be easy for the user to learn and operate the system within a reasonable amount of time
- Efficiency: Once the user has learned to operate the system, he must be able to use at a fast pace,

increasing his productivity and efficiency

- **Memorability:** If a user stops using the system for some time and then starts using it again, he must not have any substantial problems, i.e., it should be easy for the user to remember the basic operation of the system
- **Low error rate:** The system must prevent the user from making errors by proper validation. If possible, the system must be intelligent enough to correct errors in case the user makes them. Errors made by the user should not affect data integrity and must not cause the system to crash
- **Satisfaction:** The user must find the system to be comfortable to work with. Complex manipulations by the user to achieve results must be avoided

Direct Manipulation is the visual representation of the activities we perform. In this we use real world objects and concepts to do tasks. The best example is that of using a Graphical User Interface (GUI) to perform tasks using point and click tools rather than wading through textual menus. Thus, a properly designed DMI can satisfy all the usability features specified above.

The benefits of DMI are:

- Actions can be reversed if they are found to be wrong
- Any operation is visible immediately
- Since there is no syntax or commands to be remembered, there is less chance of error
- It is easier to predict and prevent errors
- It is easier to learn and can be remembered for a long time, since most of it is visual in nature

As with any concept, DMI also suffers from certain drawbacks. However, these drawbacks are most often technical in nature, which can be solved by further research.

- To design and implement a DMI, more system resources may be required, which are often expensive
- Because of the visual representation, objects may take up more screen space and can cause more relevant information to be scrolled down. Also, visually impaired users may find it difficult to navigate through the system
- For some systems, it is necessary for the user to accurately control the input mechanism, which can be difficult for new users. For example, Computer Aided Design requires high precision drawing with the mouse for proper representation

The basic approach to Direct Manipulation is by understanding the flow of the operations required to complete a task. Then a sequence of flow charts is prepared to visually represent these operations. Based on these flowcharts, the user interface may be designed.

Some common examples of DMI are:

- Word Processing Programs
- Screen editors
- Geographic and other three dimensional representation software
- Computer-based games
- Form-based data entry screens

A good understanding of the Direct Manipulation Interfaces can give one a good idea on how to design effective User interfaces, which ultimately leads to better Human Computer Interactions (HCI).

Answer: [d] System resources. Explanation: To design and implement a DMI, more system resources may be required, which are often expensive because of the visual representation.

Question: Which of the following techniques are used in anti virus detection and is based on some specific signature in a program?

- [a] Scanning
- [b] Integrity checking
- [c] Heuristic detection
- [d] Interception

Module 5- Working of anti virus software

what are viruses?

Viruses are malicious codes that make their way into the computer systems and networks intended for destructive purposes. They make their way to the system via e-mails, corrupted floppies, CDs and the like.

Such a situation results in huge losses to the company. Hence it is necessary to deploy anti virus software to manage this problem.

Anti virus software

These software programs check the hard disk, floppy disk and e-mails for viruses and try to eradicate them from their respective locations. Anti virus software nowadays come with an auto update feature, which allow the systems to remain alert against any new virus attack. The most popular anti virus packages in the market are Norton anti virus and virus scan.

Working of anti virus software

Anti virus software detects the infected file and tries to repair the file. If unable to do so, it will at least not allow the malicious code to run on the machine thus preventing any harm. There are basically 4 methods to detect the virus: -

1. Scanning
2. Integrity checking
3. Heuristic detection.
4. Interception

Scanning

This method of virus detection is the simplest and is implemented in most of the anti-virus packages. A scanner will search for all the files in a boot sector and on the disk. It will look for specific signature that is present only in viruses and not in normal programs. In order to prevent false detection most of the scanners ensure checksum (a technique used for determining the changed data) of the file. There are basically two types of scanners: -

- On-access scanners: It scans for files at the time when they are loaded into the memory before the execution takes place.
- On demand scanners: It scans for files in the main memory, boot sector and disk memory. It is usually triggered by the user.

Integrity checking

An integrity checker stores all the integrity information about a particular file on the disk. It is

usually done by checksum techniques. The integrity information for virus-infected file will no longer match the integrity information, which was stored previously. The user is intimated, so that he/she can restore the files to pre-infected conditions.

Heuristic checking

It is the most common method of detecting the viruses. Anti virus software are incorporated with a set of rules and regulations, which differentiate virus from non-viruses. For example F-Secure virus software uses this method. The biggest advantage of heuristic virus checking is that the user need not update and download the anti-virus package frequently.

Interception

It detects the behavior of the virus and alerts the user about the same. This method works in close integration with heuristic checking method. Interception identifies the skeptical behavior (installing itself as a resident program, relocating itself again and again in the memory, etc.) of the program and alerts the user.

Shortcomings in anti virus software

The major problem with anti virus software is that, they are unable to detect some of the viruses. This is because the users generally do not update the anti virus software. . Anti virus software cannot protect the system from new type of virus because the configuration of new virus remains undetected by the existing anti virus software.

Answer: [a] Scanning

Module:5

Reference No:M5022

Question: After an action has been performed successfully in a database, the changes are permanent, and must be present, even after a subsequent failure. This is a principle of: ?

- [a] Durability
- [b] Atomicity
- [c] Consistency
- [d] Isolation

Module 5- Database Concepts

A database is defined as a systematic collection and storage of data for easy and efficient querying and retrieval. A Database Management System (DBMS) is used to control the operation of associated databases. A database and a DBMS together are referred to as a Database System (DBS). The DBMS is the heart of the DBS, since it manages access and use of the database.

With huge amounts of data to be stored, databases have become indispensable for organisations today. Databases differ in the way they store data. Some of the different database models are:

Hierarchical model

This is the first model developed for databases, and uses a flat structure. Data is accessed linearly i.e. records can be accessed one by one. Also, referred to as the tree structure, it is very slow and cumbersome, when a large

amount of data has to be stored. Every record contains information about the next record only, and it is very difficult to move backwards through records.

Relational model

The relational model is based on real world data. For instance, information about an employee is often a relationship between entities. In this model, all data related to an entity is stored in the form of rows in tables. Each row is termed a record, whereas data in a column represents a characteristic of all entities stored in the table. This model is the most widely used, since there are stringent rules on creating, storing, accessing and retrieving data. It is also possible to restrict access to data in a granular way. As with real world entities, relationships are clearly established and stored.

Object-oriented model

The object-oriented paradigm that is revolutionising programming has also been applied to the database model. In this model, entities with similar characteristics are grouped into "classes". Further, similar classes can be grouped into "class hierarchies."

Accessing or modifying characteristics of objects is only through well-defined functions, which must be specified beforehand. It may be required to extend common data types such as integers to represent more complex and real world entities. Every database, regardless of the model has to satisfy four principles:

- **Atomicity**
This is the most important property of a database. Any operation on the database, referred to as a transaction, must happen in its entirety or not happen at all. For example, assume that a user has requested the bank to transfer \$100 from his account to another user. The bank debits \$100 dollars from his account, but before money is credited to the other account, a problem occurs, and the operation is not completed. This can lead to a loss of data integrity.
- **Consistency**
This principle follows from the principle of atomicity. At any point of time, data integrity must be maintained. This is achieved by synchronising database operations so that a record of all operations is kept. If an operation has not been performed completely, then the record is looked into, and the entire operation is 'rolled-back'. This brings the database into the state it was before the operation, and helps it to maintain stability
- **Isolation**
There must be no relationship between two operations on the database. This prevents the outcome of one operation, from affecting other operations. All related changes to the database is categorised as one unit, and executed as one operation.
- **Durability**
After an operation has been performed successfully, the changes are permanent, and must be present even after a subsequent failure.

Answer: [d] Durability

Explanation: After an operation has been performed successfully, the changes are permanent, and must be present even after a subsequent failure.

Question: A malicious user can change an application to get the full database. This is a pitfall in which type of database security measure ?

- [a] Passwords
- [b] User Accounts
- [c] Isolation
- [d] Backup

Module 5- Database Security I

Most often, security violations occur not because of poor technology, but due to poor implementation of procedural mechanisms. For example, a colleague asking for a password to confidential data is most often obliged, even though he may not need to access the data. Data has to be protected from external sources, but more importantly from attacks occurring within the company. The following measures may help:

- **Passwords**

Well-constructed passwords can help in preventing unauthorised access to databases. Employees must also be made aware of the need to change passwords once in a while, and a security policy must be implemented to enforce it. Passwords must be programmed to expire after a specified period. This is suitable for small projects where access to the database is for a few days only. Also, it will prompt users to change their passwords.

- **Backup of Data**

Much has been said and written about the need to regularly back up data. However, few people realise that backup data is the most vulnerable and common point of attack. The entire corporate data is present on the back up media, and mechanisms used to protect data are not applied to this important source, making it an easy target.

Back up data must be controlled using the same measures as the original data. Measures like logging of persons requesting the back up copy, and details of the way in which the copy is used, can prove to be very effective. In short, the person responsible for maintaining the backup must know where each copy is present, at any time.

Another vulnerable aspect is the use of original data for testing database-related applications. For example, if a company is developing application software that access the database, developers and testing personnel typically test the application on confidential data. It is better to use sample data generated from the company's database, but not containing any confidential information for such purposes.

- **Isolation**

Isolation of a database means that confidential data must not be accessible to people, who do not need to access it to discharge their duties. Most often, developers and testing personnel use the data for product development. The following measures could be useful:

1. Do not give operating-system privileges to developers to the system that holds the main database.

2. Reveal the name of the server and its location only to personnel who need access to the information
3. Disallow the use of confidential data for development or testing.
4. Include database access controls in the security policy

- **Manipulation of user accounts**

Accounts may be created with various privileges for different access levels. For example, read, write or modify privileges can be given for three separate accounts, so that employees can access the data based on their requirements. If a person merely needs to read a block of data, there is no use in allowing him to modify the data.

A common pitfall is the poor monitoring of application accounts. These accounts are created for applications that need to access the database to function. Typically, they have full permissions, and hence a malicious user can modify an application to access the full database.

Further, applications by third-party vendors have built-in passwords to access the database. This can be exploited by hackers, and hence the database must be configured to overcome the drawback.

Answer: [b] User Accounts Explanation: Application accounts are created for applications that need to access the database to function. Typically, they have full permissions, and hence a malicious user can modify an application to access the full database.

Question: Which of the following allows the most granular access control mechanism for database security ?

- [a] System and Object Privileges
- [b] Database Integrity mechanisms
- [c] Data Encryption
- [d] Row-Level Security

Module 5- Database Security II

Appropriate security measures as detailed below can ensure that the database is secure.

System and Object Privileges

Users are given permissions to access certain objects in the databases. These permissions authorise the user to perform operations on the database and are called "privileges." Privileges are of two types:

System Privileges - These privileges allow the user to operate on the database in such a way that the operation affects the entire database. Such privileges are very powerful and are given only to the administrators of the database and sometimes to the developers, who create applications to interact with the database.

Object Privileges - These privileges are also called "Schema Object privileges" and allow the user to access or operate on specific objects in the database. Any data unit that is a named entity is called an object in database terminology.

There are many methods to ensure that System and Object privileges are assigned and used profitably.

- **Passwords**
Passwords along with a username can be used as the first line of defence in authorisation of users for database or object access.
- **Roles**
Individuals or groups of people can collectively be assigned roles to perform certain functions. For example, Back up operator is a role whose privilege is the ability to take backups of the database at predetermined intervals.
- **Stored Procedures**
Stored Procedures are scripts written in the Structured Query Language (SQL). SQL is an industry standard for creating, viewing, modifying and deleting database objects.
Stored procedures allow a user to perform certain operations, determined previously, in a structured way. The user executes the stored procedures to access the database, but the user cannot access the database or an object directly. The stored procedure may provide only for specific functions like querying or updating a table in the database.
- **Views**
Views are database objects that provide a mirror copy of another object. Views allow the administrator to query or modify only that part of the object that is required rather than giving privileges to the entire object.

Data Encryption

The most effective method of preventing unauthorised data access is by encryption. In encryption, data is encoded so that people who have the required authorisation key can decode the encrypted data. It has to be kept in mind, however, that database encryption is only an additional measure of security. Mostly, data is encrypted not fully, but only highly confidential data is encrypted.

Database Integrity

The concept of integrity assumes that the database holds only the most current data at any point of time. This ensures that the data is accurate and consistent. Data integrity can be enforced either by considering the integrity of the whole system or only the integrity mechanisms of the database, such as referential integrity, transaction integrity etc.

Database techniques like triggers and constraints can be used to ensure that data in the database adheres to pre-defined rules. The rules may be business rules that specify what data is acceptable in which column of the table or may be generic rules.

Referential Integrity ensures that if data in different tables are related, then a change in one table must appropriately reflect in another. In summary, it specifies rules on how relationships between data in different objects are to be handled.

Row Level Security

This approach gives the most control over what data is accessible to users. This lowest level of access control is termed as "granular access control" and provides the most security.

Access to data in tables can be restricted to data in specific rows only, based on conditions such as the designation of users, the department etc. The methods to achieve such row-level control are:

Virtual Private Database (VPD)

Modern database systems follow a three-tier approach to data access. The concept of VPD gives the administrator the ability to provide database access to users based on a well-defined security policy in a package. This security policy may be applied to the entire database or to particular database objects such as tables and views.

Label Based Access

This method works similarly to the security classifying mechanism for access to physical resources. Data is classified into certain labels and then the rows are divided into those labels based on the confidentiality of the data.

Government Organisations typically use the label access methods, while companies use it only to distinguish between information that is secret to the company and information in the public domain. Only if a person has a certain designation is he permitted to access data of appropriate labels.

Answer: [d] Row-Level Security Explanation: This approach gives the most control over what data is accessible to users. This lowest level of access control is termed as "granular access control" and provides the most security.

Question: Which type of constrained user interface does an ATM have?

- [a] Menus
- [b] Physically constrained user interface
- [c] Database views
- [d] Access control lists

Module 5- Constrained User Interface

One method of implementing Internal logical access control is through a constraint user interface. This is used along with Access Control Lists for internal access control. It imposes restrictions on users' access to specific functions in a database. The idea behind constrained user interfaces is that users can access only those system functions for which he/she has been specifically authorised. The three types of constrained user interfaces are menus, database views and physically constrained user interfaces.

Menus

Menu driven systems are one of the most commonly used constrained user interfaces. Menus enable non-technical users to understand the system and thereby reduce errors. Menus and shells restrict the system commands that a user is entitled to. A user is not given menu options for unauthorised operations. Thus the user cannot invoke those commands/functions.

Database views

Access to data contained in a database is restricted through database views. A user with access to a database will not necessarily have the permission to access all the data in the database. Depending on the content of the fields in a database and the complex access requirements that may arise views provide the required access. A database can have logical and physical views that give the necessary level of abstraction. Security considerations imposed on logical data is hidden from the users. For example, a person associated with a bank may have to know a customer's loan number but does not need to know the details of the loan amount, rate of interest etc. This is done with the help of relational algebra in a database. A database relation/table that is not part of the logical model, which is made visible to the user as a virtual relation is called a view. The view is created by specifying the query that is used to compute it. It is also given a name. The database system stores the definition of the view and not the result of the query defined by the view. Hence, updates and modifications made on views are stored dynamically as and when they change. Views simplify usage and enhance the security of the database. System usage is simplified because the user access is restricted to data that is required. A user who is denied access to a whole relation can be allowed access to a part of that relation through a view. Thus view level security will limit a user's access to precisely the data that user needs.

Physically constrained user interfaces

The best example of physical constrained user interface is an Automated Teller Machine (ATM). It presents a user with a limited list of operations. The user is prevented from escaping to any other system interface or operation, which he is not authorised to access. With an ATM the menu options permit a user to undertake a number of transactions, e.g., deposit, withdrawal, transfer.

Answer: [b] Physically constrained user interfaces.

Question: Run-to-run totals are a part of which control?

- [a] Input control
- [b] Process control
- [c] Manual control
- [d] Output control

Module 5- Application Control

Controls associated with specific applications that are related to transactions and data are termed as application controls. They are associated with transaction processing systems. Application controls are either manual or programmed. These are devised to ensure the completeness and accuracy of records and validate all entries. Computer applications for purchase, sales, manufacturing and the like make use of application controls. General controls are needed to ensure the proper functioning of application controls.

- Objectives of an application control include:
- Authorising and accurately recording, classifying, processing, and reporting all transactions.
- Ensuring that correct task data is entered into the computer system and confidentiality is maintained during processing.

Classification

Application controls are classified into input, processing and output controls.

Input controls: Input controls ensure the validity, accuracy, and completeness of data entered into an information system. They are critical to systems that involve direct and immediate processing. Input controls are subdivided into:

- Data observation and recording
- Data transcription/batch processing
- Edit tests of transaction data
- Transmission of transaction data

Processing controls: Once the input is validated, it needs to be correctly and completely processed. Processing controls help in processing data accurately and completely and ensure that no unauthorised transactions are allowed. Furthermore they help in tracing transactions. Errors that may arise during processing include programming and operational errors.

Some examples of processing control are:

- Manual Crosschecks which involve checking the work of an employee, reconciliations and the like.
- Run-to-Run Totals wherein a control is incorporated into batch transaction files to ensure that no records are omitted or changed accidentally during processing.
- File and program changes are made to ensure that transactions are posted to the proper account and programs are validated.

- Processing Logic Checks are done to perform edit, sequence and reasonableness checks.
- Audit trail linkages are provided to enable easy tracing of transactions for future reference and use.

Output controls: At the output end of a process there is a need to verify the reliability and reasonableness of the output. Prevention of unauthorised access and acknowledgement by appropriate authorities is the other objective of an output control. It also provides control over sensitive documents and stored data.

The two types of output controls are:

- Validating processing results
- Regulating the distribution and use of printed output

Some application control methods include online access controls, unique passwords and terminal identification.

Online access controls: Only authorised users having a unique user ID and password are allowed to access terminals and input transactions.

Unique passwords: Users are allocated unique passwords. They are allowed to input data into the system only with the help of these passwords. Terminal identification: Specific terminals can be reserved for input of certain data. Thereby attempts to key in unwanted details into such terminals can be disallowed.

Answer: [b] Process Control.

Module:5

Reference No:M5027

Question: Which of the following transaction type occupies the highest level of significance in application control?

- [a] Error correction transactions
- [b] Master file change transactions
- [c] Normal transactions
- [d] Batch control transactions

Module 5- Application control: Transaction Types

Application control systems are closely related to transaction processing systems since both are concerned with specific applications. Application processing falls under the purview of transactions. After establishing the objectives of application controls and their relationship with general controls, there arises another concept that needs our attention. Different classes of transactions possess varied types of risks due to errors or frauds. The most commonly encountered classes of transactions are Master file change transactions, normal application transactions and error correction transactions.

Master file change transactions

Files that contain permanent or semi-permanent information are termed as master files. Transaction files

are those that form a part of an ongoing transaction and contain only current or temporary data. Processes that are carried out repeatedly that create, change, or delete records in a master file item, table, or database during transaction processing are called master file change transactions. Master files contain two main types of data:

1. Relatively constant information. Examples are prices, addresses and the like.
2. Accumulating balances. Examples include account balance, inventory on hand, and the like.

Master files require stringent controls for changed/modified transactions. Some data is used repeatedly during processing or represents important accounting balances. The completeness, accuracy and authorisation of this data is of critical importance. Control techniques should be introduced to ensure that the most recent version of the master file is made available during the time of processing of transactions. Most of the frauds and intrusions that take place in a computer system involve master files. Also, the master record may carry coding errors unless updated carefully.

Normal Transactions

Normal transactions occupy the second position in terms of significance. They represent the bulk of the transactions processed in any information system. Even if the master files are adequately controlled, it still is necessary to ensure that transaction processing and error correction controls are adequate to control normal transactions.

Normal Transaction processing refers to controls in regular input transactions (excluding master file transactions and distribution of output reports). A computer system can include various input transaction types and several outputs. For example, a sales and accounts receivable system will have sales, and back-order transactions, credit transactions, cash receipt transactions and accounts receivable adjustments as inputs. Outputs for the same system may include sales invoices, credit notes, monthly sales summaries, customer statements and an aged trial balance of the accounts receivable.

Error Correction Transactions

All types of error transactions have the following inherent properties that make them critical -

- The potential to bypass controls that are stringently applied to other transactions.
- Error transactions are not subject to more lax control procedures than those applicable to transactions that were not in error. Due to this, master file change transactions that are in error should be subject to the same stringent controls as master file change transactions that are not in error.
- Normal business transactions that are rejected because of an error condition should not be subjected to less stringent controls than those applicable to transactions not in error.
- The need to monitor and control transactions to ensure that they get reprocessed. Effective audit trails help in error tracing and correction.
- All errors should be logged in a manual or in computerised logs to ensure that the error correction process is complete.

Answer: [b] Master file change transactions.

Question: Which of the following is not a visual programming language?

- [a] Control flow languages
- [b] Visual C++
- [c] Concurrent languages
- [d] Form based languages

Module 5- Virtual programming languages

Evolution

"A picture is worth a thousand words". Pictorial and diagrammatic expressions are always easier to understand and interpret. This concept has become the driving force behind the evolution of visual programming languages.

What is a visual programming language?

Conventional programming is represented in a single dimension. Programs and commands issued to the operating system follow a linear pattern and are in the form of text strings. Visual programming applies to any system that allows the user to specify a program in two or more dimensions. It uses graphics, icons and diagrams instead of text to express instructions.

What are form-based languages?

Form based visual programming languages include commercial spreadsheets and research systems. They are best suited for end-user computing. Form based visual programming languages provide a declarative approach to programming. By using form-based languages users create cells, and define formulas for those cells.

Categorisation

Various methods have been used to define different categories and types of visual languages and their specific attributes. One such classification includes the following four types:

- Visual programming languages that deal with objects having a visual representation
- Visual information processing languages, which process visual information. The language is text based.
- Languages with visual interaction support. They are text-based languages that deal with objects and visual representations.
- Iconic visual processing languages where the language is represented visually.

Further study and advancement in this field has led to the following three broad categories:

- Languages where graphics play the central role in programming
- Languages with graphic representations as an integral part
- Conventional programming languages with graphics as an extended feature.

Attributes

Visual languages possess the following visual attributes:

- Pictures
- Graphs
- Forms

- Icons
- Spread sheets etc.

A good program should have the following features:

- i. Friendly editing support
- ii. Easy to document
- iii. Easy to debug
- iv. Dynamic execution
- v. Code that is easy to read and understand
- vi. Easy to learn
- vii. Runs on all platforms

Visual programming languages include control-flow languages, data-flow languages, concurrent languages, form-based languages, functional languages, rule-based languages, object-oriented languages and programming by demonstration.

Answer: [b] Visual C++. Languages like Visual Basic and Visual C++ should not be mistaken for visual programming languages. They are languages that simplify programming tasks but are written in traditional text language.

Module:5

Reference No:M5030

Question: Hacking by making use of information on waste/discarded paper is termed -

- [a] Finger protocol
- [b] Ping
- [c] Dumpster diving
- [d] Social engineering

Module 5 - Hacking

The major threat faced by information systems is from insiders, i.e. employees. Though, outsiders also pose a serious threat. The motives of hackers are varied. Hackers may break into a system merely because of the challenge or for illegal gains.

Modus operandi

1. Technical techniques

Irrespective of the motive, hackers follow the same pattern. They seek detailed information about the servers of the target organisation, using existing Internet utilities and protocols. These tools include - Simple Network Protocol Management (SNMP) - It reveals details about network topologies of a target organisation by examining the routing table of an insecure router.

- Software such as *TraceRoute* and *NewTrace* are used to identify intermediate network numbers and routers that are connected to a server host.
- Whois tracks information regarding all the DNS (Domain Name Services) and system administrators.
- Finger protocol provides information about users of a target organisation. Information includes login names, phone numbers and timings when they access the servers.
- Ping (Packet Internet Groper) - It uses a short scanning program, and pings every host on

the network to form a list of hosts.

2. Non-technical techniques

Sometimes hackers also use non-technical techniques such as -

Social engineering - It is also referred to as 'people hacking'. A ploy to deceive legitimate employees, hackers use it to obtain confidential information such as passwords and the like to access target systems.

Dumpster diving - It involves going through discarded (waste) paper in an organisation to obtain useful information.

After obtaining the required information, the hacker then looks for weaknesses in the system. There are software that can scan the entire network for security holes. Software such as Security Analysis Tool for Auditing Networks (SATAN) and Internet Security Scanner (ISS) are used by the system administrator to check for weaknesses in the system, and to fix them. However, hackers misuse these software to find loopholes in the system, and gain illegal entry into the systems.

Once the hacker gains access into the system, what he does depends entirely on his objectives.

Preventive measures

An integrated security system will help to avoid hacking activities. Organisations should take following steps -

1. Information should be classified based on its value, and then protected accordingly.
2. Privacy policies should be made and communicated to employees, to nullify the attempts of social engineers.
3. All important documents should be shredded to avoid dumpster diving.
4. Most control software contain default userids and passwords, which are provided at the development stage. They should be changed immediately after the software is installed, because it can be breached easily.
5. Checks for weaknesses in the software should be done on a regular basis, and rectified at the earliest.

Most of the time, hackers adopt tried and tested techniques, thus organisations should develop safeguards along these lines.

Answer: [c] Dumpster diving.

Module:5

Reference No:M5031

Question: Social Engineering is:

- [a] Creating a team for software development
- [b] Referred to as people hacking
- [c] A technique to motivate teams
- [d] A training method software development team

Module 5 - Social Engineering

The term "Social Engineering" is used for hackers. "People hacking" is a technique used by hackers to fool legitimate employees to get confidential information like passwords and then exploit this information to target systems causing a breach in the system's security.

The best part of social engineering is that it strikes at the weakest link in the information security system- the human being. In the process it violates all security measures implemented by the organisation. The human element is considered as a weakest link as every computer system requires a human interface and therefore every computer system is open to the threat of social engineering.

Social Engineers take advantage of following personality traits-

Responsibility sharing- When employees believe that they are not the only ones responsible for certain actions, they tend to part with information easily. Social engineers may use the name of a superior and say that he has been authorised by him to do the job.

Attitude to help - Certain people like to help others. Social engineers exploit this trait. They normally seek help for login related problem from persons who handle the systems.

Social engineering use the following tactics-

Direct Request - In this form of social engineering, the hacker may simply make a phone call and ask for the desired information from the target. This is the simplest form of social engineering. However, it has very low chances of success as a direct request is often questioned.

Before a direct request is made, it is generally preceded with a lot of activity that involves collection of as much information about the target as possible. For instance "A confused and befuddled person will call a computer department and meekly request for a password". This may lead to two situations, one, the person will get the password. Second, the computer department may ask for some verification. At this point, information that is collected prior to making the phone call comes handy. The computer department may ask for the access account number, user name or any other information they think may be relevant for verification. In such situations, if the hacker is not able to answer the questions asked by computer department he is immediately viewed with suspicion and his request is rejected. . On the other had, if the hacker gets the password, then it is he can get as much information as he wants.

Creating situations - This is a slightly more advanced version of the "direct request". Here a social engineer frames a situation. For instance, he may claim that he has forgotten the password, as he was on vacation for a long time. Alternatively he may say that he wants to access his boss's machine after he has left for the day. A hacker can also pretend to be busy with handling lot of manuals and machines may request an unsuspecting employee to use his access card to enter a restricted area.

Dress to kill - Social engineering is not just about getting information over the phone. In some cases, it may involve visiting the physical locations. In this case it becomes necessary to dress appropriately, which may be in the uniform of some service person such as an electrician, a delivery person and the like. Alternatively, a hacker may act like an employee; flashing a fake ID card to pass through the checkpoint.

Personal persuasion - This refers to the ability of a social engineer to persuade the target into

revealing information.

Building trust - Social engineering to some extent may require building trust and even bonding with the target initially so that this can be exploited at a later time.

Answer: [b] Referred to as people hacking.

Question: Which is the most important step that can save a company from social engineering attacks?

- [a] Creation of helpdesk rules
- [b] Making people accountable for jobs
- [c] Including social engineering in the social policy
- [d] Using Id cards

Module 5 - Social Engineering - Security procedures

Social engineering is a technique used by hackers to exploit systems by taking advantage of the human interface. Companies that fall prey to social engineering attacks generally do not let outsiders know that they have disclosed confidential information. Every person in the system is vulnerable to social engineering attacks, including the most experienced and knowledgeable ones. Therefore there is a need for measures to be implemented that protect systems, people, and data from attacks by social engineers.

Policies and guidelines

The first step that should be taken is to include the issue of social engineering in the security policy. The management should issue a statement to employees to create awareness regarding the importance of corporate information. This should include dos, don'ts and penalties. A good policy should cover following areas -

- ***Setting up of an account and change in responsibilities*** - There should be procedures that should define how to set up an account when a new employee joins, how passwords should be given, and how he should change them. In the case of change in responsibilities, there should be procedures to revoke former access and to grant access to new responsibility holders. Similarly, when an employee leaves the organisation, all the access given to the ex-employee should be revoked and his account should be deleted. This will prevent an ex-employee from misusing the system or sharing his password with others.
- ***Help desk rules*** - Verification procedures should be in place for giving out passwords. Sometimes it becomes important to verify the location of the employee. This can be done in two ways -either by making the helpdesk have a caller id phone or by making the helpdesk call back the employee to verify the location. The policy should also contain procedures wherein high priority password can be reset only in the presence of authorised personnel.
- ***Id cards should be made compulsory*** - There should be a policy, which states that each employee should wear a photo id card. Visitors should be provided temporary visitor id cards. Also there should be a practice in the organisation where an employee can question another employee who is not wearing an id card.
- ***Privacy policy*** - There should be a privacy policy, which should state that no information other than what is needed should be given out. In some cases, phone surveys collect information by constantly asking more questions. This information will be used later on by the hacker. There should be an automatic process that routes such surveys to a designated person. Also, procedures should be in place, which allows employees to escalate the issue to higher ups if he is made to disclose more information than what can given.
- ***Surveys/Online tricks*** - If an online survey or any other online interactive features asks for a login id and password, it should be immediately clarified with the system administration. In the process of filling a survey, if a user has entered a password by mistake, then he should immediately change the password and should inform the administrator. The system administrator should also check with

users to ensure that no one else has fallen prey to such online tricks and should immediately check servers for any damage.

Ultimately one should ensure that these policies and guidelines are conveyed to employees, because no policy or guidelines is useful unless employees are educated on how to implement them.

Answer: [c] Including social engineering in the social policy.

Explanation: Including Social engineering in the social policy is an important step. The other options represent actions that are already included in the policy.

Module:5

Reference No:M5036

Question: Access Control is implemented using _____ in Windows NT and _____ in Unix?

- [a] Access control List and file system
- [b] Security Reference Manager and Syslog
- [c] File system and Access control List
- [d] Syslog and Security Reference Manger

Module 5- Windows NT vs. Unix I

The two most widely used Operating Systems (OS) in the corporate environment today are Windows NT and Unix.

Windows NT is a product of Microsoft Inc. and along with its desktop variants such as Windows 95, Windows 98 and Windows ME is the most used OS in the world. The reason for its popularity is its Graphical User Interface (GUI), which allows even users with no computer proficiency to easily learn and perform complex tasks.

Unix was developed in the early 1970s at the University of Berkeley. There are many variants of the Unix OS, such as Berkeley Unix, Unix System V by AT&T, Sun Microsystems' Solaris etc. The Unix OS is known for its powerful features and most of the Unix code is available as Open Source Software.

The security aspects of the two Operating Systems are discussed in this article.

Identification

Windows NT	Unix
An identification number, called the Security Identifier (SID), uniquely identifies users in a domain. A SID is created when a new user is added to the domain. SIDs are generated according to an algorithm that ensures that a	Unix uses a similar concept called User Identification number (UID). This number is a value assigned by the administrator when the account is created. The major difference compared to Windows NT is that the UID may

SID is never reused even long after the account has been deleted.	not be unique although it is a good policy to keep it unique. The administrator, also called superuser or root, has UID 0. Users can also be part of a group and hence a Group ID (GID) number is also used.

Authentication

Windows NT	Unix
Passwords are used to allow users to access the system. The Security Accounts Manager (SAM) is a part of the OS that stores the user passwords in the database along with the SIDs. Passwords are stored in two encrypted versions, NT-native, which uses the MD4 algorithm and LM-hash, which uses a variation of the Data Encryption Standard (DES) algorithm.	Passwords in Unix are stored in the /etc/passwd file. A password is encrypted using another variation of the DES algorithm before it is stored in the file. The /etc/passwd file can be accessed by all users and hence the general practice is to move the passwords to another file called /etc/shadow, which is not readable by all.

Access Control

Windows NT	Unix
All resources of a system or a network are considered as objects. Access Control Lists (ACL) are used to control the access of the resources to authorised persons. Every ACL has a list of entries, Access control Entries (ACEs), which associate the object with a user and specify the permissions for that user. ACEs that do not permit an action are listed before the ACEs that permit access. If a user has no entry in the ACL for an object, he does not have any type of access to that object. A Kerberos token is generated when a user is authenticated. This token is compared in the ACL for access permissions.	Every resource in Unix, including physical ones such as floppy drives, is considered as files under Unix. Therefore, it makes sense to implement access controls using the file system method. Every file has a number of properties such as the owner of the file, permission bits, UID, GID etc. The permission bits are r (read), w (write) and x (execute) and control access to the file for (i) the owner, (ii) for the group and (iii) other users in the system. A '-' indicates that the missing permission is not allowed. For example, if a file has the attributes, rwx r-x --x, it means that the owner has permissions to read, write and execute the file. Members of the owner's group have only read and execute the file while other users have only execute permissions.

Auditing

Windows NT	Unix
The Windows NT tools used for auditing are: Security Reference Manager (SRM), the Local Security Authority (LSA) and the Event Logger. All incidents are classified into pre-defined "events" and logged in the Event Log.	The kernel and the processes running on the system use a powerful utility called the "syslog" to log appropriate information in log files. C2 audit mechanisms, specified by the Trusted Computer System Evaluation Criteria,

The LSA specifies the handling of events by invoking the SRM and tells it to respond to the event according to what is specified in the Audit Policy. When an event occurs in a subsystem, it sends a request for an audit to the SRM. The SRM contacts the LSA, which hands over the Audit Policy for that event. After the audit the SRM sends the report to the LSA, which is then sent to the Event Logger for storage.	Department of Defence, U.S., is also supported in modern Unix systems.

Impersonation

Users other than the administrator may sometimes need to perform critical security tasks, but these users should not be given the entire set of permissions as the administrator. The solution is to grant permission to a user to run a particular process. The process must check that the user does not abuse this permission, by performing checks to prevent unauthorised actions. This technique of selectively granting permissions is called "impersonation."

Strict conditions must be placed on the executable file before impersonation. A user may modify the file, such that he can access resources for which he is not authorised. This can result in serious security threats.

Windows NT	Unix
Every application under Windows is broken down into small pieces called threads. Every thread is assigned one token, called "primary token." Another thread may allow this thread to act on its behalf by providing a token called "impersonation token." This token can be a full replica or a restricted version of the primary token. Unix provides not one, but two different mechanisms for impersonation. They are set-UID (SUID) and set-GID (SGID). An executable file can be configured for one of these two types of impersonations. After such configuration, that file is executed with the permissions of the owner of the file, not with the permissions of the current user.	Unix provides not one, but two different mechanisms for impersonation. They are set-UID (SUID) and set-GID (SGID). An executable file can be configured for one of these two types of impersonations. After such configuration, that file is executed with the permissions of the owner of the file, not with the permissions of the current user.

Answer: [a] Access control List and file system Explanation: In Windows NT, Access Control Lists (ACL) are used to control the access of the resources to authorised persons, while Unix uses file permissions to control access.

Question: Searching for weaknesses in the Windows NT and Unix Operating Systems is an example of:

- [a] Active attack
- [b] Security control bypassing attack
- [c] Passive attack
- [d] Tear-drop attack

Module 5- Windows NT vs. Unix II

This article uses a well-defined set of criteria to compare the security aspects of Windows NT and Unix. Windows NT is a more recent product while Unix has been in existence for a long time. Most of the security problems in Unix have already been uncovered and patched up and it will take a few years till the same can be said for Windows NT.

The attacks on any OS can be classified into one of the following three groups:

- Bypassing Security Controls: It is the process of bypassing the mechanisms put in place by the administrator to prevent unauthorised access to resources
- Passive attacks: It is the process of exploiting weaknesses in the system
- Active attacks: It is the deliberate attack of the system by misusing the permissions assigned to the user

This article compares the security features of Windows NT and Unix with respect to these three criteria.

Bypassing Security Controls

- Password attacks

Windows NT	Unix
1. Password Capturing attacks: Eight variations of password authentication schemes are possible in Windows NT. The main security problem is because the client chooses the scheme to be used, even though the server may suggest a more secure one. Such problems occur because Windows NT is designed to be used as server with other (and previous) OS's such as Windows 95 as clients. 2. Password Guessing attacks:	1. Some commands used in Unix such as those beginning with 'r' (rsh etc) and protocols like Telnet are inherently insecure since they transmit passwords in human-readable text. Eavesdropping or network sniffing can reveal the password to the attacker and since the password is not encrypted, there is no necessity to even crack the password. Unix stores passwords in the publicly readable file, /etc/passwd. Some administrators use a concept called shadowing, where the encrypted passwords are copied into the /etc/shadow

As discussed earlier, passwords are stored in two formats, LM-Hash and NT-native. LM-Hash uses an old and weak algorithm, with only capital letters used for passwords. Also, passwords less than 14 characters are padded with NULLs. If the SAM (Security Accounts Manager) database falls into the hands of the attacker, then decrypting the passwords is very simple with publicly available tools.	file. This file is accessible only by the administrator and hence provides some measure of protection. However, with poor password selection, it is quite easy to automate the process of breaking the encryption

- **Masquerading or spoofing of Programs**

If a program can be fooled into performing a task for a user who does not have permission to do so, then it becomes a very great security risk. For example, in Unix the "X terminal emulator logging vulnerability" presents a fake login screen to the user and collects the password from the unsuspecting user.

Windows NT	Unix
The same TCP/IP implementation is used in all operating systems, including Windows NT. The basic flaw in the protocol itself allows a user to generate an IP packet which seems to come from a user other than the attacker. This makes the OS to be vulnerable to the "tear drop" attack.	Unix also is vulnerable to the "tear drop" attack. Note: IP spoofing is possible in all Operating Systems with the same TCP/IP reference model.

Passive attacks

Manual and Automatic Searches

Windows NT	Unix
Manual searching for bugs (errors which can be taken advantage of) is quite difficult in Windows NT since it is only recently that attackers have started concentrating on it. Further, much is not known about the inner workings of the OS. But programs long used for other OS are now being ported to the Windows environment. The best example is that of the System Administrator's Tool for Analysing Networks (SATAN).	Due to wide availability of the OS from a long time, Unix has long been under attack from users. Searching for weaknesses manually and automated tools for the same are common in the Unix environment.

Active attacks

Denial Of Service

Denial of Service (DOS) is another name for the exhausting of the system's resources because one process consumes all of them and other processes simply wait infinitely. This type of attack has become more famous in the recent times with their application over the Internet on Web Servers.

Windows NT	Unix
As discussed earlier, every application is broken into small pieces called threads. Every thread is assigned a priority between 1 and 15. No thread is generally assigned a high priority. "Aging" is a process by which Windows NT decides when a thread has lived its life time and has to be killed. A malicious program, such as "CpuHog" assigns priority 15 to itself and then waits infinitely without doing any work. Since it is priority 15, it cannot be killed and further, no other thread will run until this is completed. The solution implemented in a patch to the OS is to allow aging to threads up to priority 15. The drawback is that it does not fully prevent resource hogging, but only slows down the system.	The major problem in the Unix environment is that one process can create (spawn) another process. By writing a program where a program creates another process, which then creates another, it is possible for the program to crash the system. The solution implemented is to limit the number of processes that can run at any time.

There is no great difference between the Security features of Windows NT and Unix, but because many consider Unix to be a difficult OS to even use it, it is felt that it is much more secure than Windows NT. However, with active security settings, both can be protected against attacks.

Answer: [c] Passive attack

Explanation: Searching of flaws in the Operating system to exploit is termed as passive attacks.

Module:5

Reference No:M5038

Question: What does the Automated Security Access Tool (ASET) (provided by Solaris) in Medium setting, do?

- [a] Checks for file permissions and makes sure standard permissions are set
- [b] It modifies permissions of certain system files (such as "ttytab" etc) and restricts access
- [c] Makes the OS highly secure by severely restricting access
- [d] Denies login attempts and checks for passwords

Module 5- Solaris Security I

Sun Microsystems has developed its own version of Unix, called Solaris. The Solaris Operating System (OS) offers an integrated set of features that help organisations control the level of

security in their networks. Some notable features of the OS are: Scripts for automatic configuration of security levels and reporting of incidents

- Secure distributed file and directory services
- Tools for developers to code secure applications
- Support for international best practices in computer and network security
- Complete support for tools from third-party vendors that increase the security of the OS

Solaris uses a four-level approach to protect resources from being used by unauthorised users. In this article, we discuss first 2 levels viz., Login access control mechanism and resource access control.

1. Login Access control Mechanisms

Passwords are the first line of defence for preventing unauthorised access to the Solaris OS. Since selection of a strong password is usually in the hands of a user, Solaris assumes the worst and provides many mechanisms to see that this feature is not abused. The "password management features" of Solaris are:

- Password Validation
- Password aging
- Disallowing old passwords
- Account expiration

Most of these features are discussed in detail in another article. Almost all operating systems have these features. However, there are a few more password restrictions that are found in certain operating systems, including Solaris:

- Timed access to resources
It is not necessary for a normal user to login to the server in the middle of the night! So, system administrators specify a valid login time for each user, say 7 A.M to 12 P.M. The system will not allow even a valid user to login at a time outside this range. This is done to prevent an attacker from entering the network pretending to be a valid user.
- Denial of Login after pre-determined number of attempts
To prevent users and programs from trying to brute-force crack passwords (by guessing), the system will not display the login prompt after a fixed number of attempts.
- Auto Logout
If a computer is not used for a certain amount of time, the system will automatically lock the computer. It can be unlocked only after the user enters the password again.
- Special Access Controls
Since administrators have full command over the OS, most attackers will try to break into that account. Solaris tries to prevent this by having special password features for administrators.

2. Controlling Access to Resources

The first level of controlling access to resources concentrates on authenticating users i.e., finding out if they are users with valid accounts in the OS. The next step is checking their authorisation. As explained in a previous article, authorisation of a user is to check whether he has permission to access a particular resource or not. Solaris has extensive features to provide authorising and auditing facilities.

The Automated Security Access Tool (ASET) is provided by Solaris to ascertain whether the current configuration is in Low, Medium or High mode. It also warns the administrator if there is any threat to the OS. The following are the functions of the ASET:

- Checks for the BIOS password to prevent users from booting in single-user mode. BIOS stands for Basic Input Output System and is built-in software that is necessary for checking the hardware and starting the Operating System. On PCs, the BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions.
- Check for the UMASK variable which holds the default permissions when a file is created by the user
- When a program is to be executed, the PATH variable is used to obtain the order of searching in directories for that program. The tool checks for improper values in this variable
- Checks for file permissions
- Checks the contents of the following files, which are important from the security perspective: .rhosts, /etc/passwd, /etc/group
- File sizes in /usr/bin and /bin are also checked. This is because viruses normally change the file size and also to check if unauthorised users have changed the configuration files

The three modes of security and their roles are:

- **Low:** ASET checks for file permissions and makes sure standard permissions are set. Checks for users logged on, remote requests, attempted logins etc. are performed and reported to administrators
- **Medium:** This mode is appropriate for most situations. ASET modifies permissions of some system files such as "ttytab" etc, and restricts access. Several other checks are performed and reported
- **High:** This mode makes the OS highly secure. Many system files are restricted or given least access. It can also disable advanced features such as "IP forwarding."

ASET is really an "asset" to the administrator. It helps save a lot of time otherwise spent in securing the OS. Such a powerful tool having all these features is not available for most other platforms.

Answer: [b] It modifies permissions of certain system files (such as "ttytab" etc) and restricts access

Explanation: This mode is appropriate for most situations. ASET modifies permissions of some system files such as "ttytab" etc, and restricts access. Several other checks are performed and reported.

Question: The default authentication mechanism in a Solaris System is Kerberos. If a third party mechanism is to be implemented instead of the default, which of the following can be used for this purpose?

- [a] Access Control Lists
- [b] Secure NFS Distributed File Service
- [c] Solstice SunScreen
- [d] Pluggable Authentication Module

Module 5- Solaris Security II

Sun Microsystems has developed its own version of Unix, called Solaris. The Solaris Operating System (OS) offers an integrated set of features that help organisations control the level of security in their networks. This article deals with the level 3 and 4 of Solaris viz., Secure Application Development and Access Controls.

3. Secure Application Development and Distributed Services

The Solaris OS provides secure distributed services through the use of the ONC+ family of products, which can be integrated into the core OS. ONC+ consists of:

- Secure NIS+ Distributed Naming Service
- Secure NFS Distributed File Service
- Secure Transport Independent Remote Procedure Call (TI-RPC)

Since many authentication schemes are available, Solaris provides a very flexible architecture that allows different authenticating mechanisms to be easily plugged into the OS. Authentication schemes such as Kerberos, Diffie-Hellman and Unix-style methods are available.

The "Pluggable Authentication Module (PAM)" provides a model that can be plugged into the OS to enhance security. Password management, multiple authentication schemes, managing of user accounts and session management are taken care of by the PAM. The major advantage of PAM is that required modules can be loaded dynamically and unloaded when not required, thus saving system resources.

Solaris provides mechanisms for "File Protection" and "Auditing" of resources.

File Protection

Solaris is a variant of Unix and hence in this OS too, every resource is considered as a file. Therefore, file protection assumes greater significance. In Solaris, this is done in two different ways: through permission settings and Access Control Lists (ACLs). Permission settings work on the principle of allotting one or more permissions (read, write and execute) for every file. The major drawback is that permissions can be granted to groups only and not to specific individuals.

Access Control Lists are a new phenomenon and have been implemented in most OS. They are lists attached to every resource and contain details of the permissions given to users for that particular resource. When a resource is transferred to another location, the ACL is also moved along with it.

4. Physical Access Controls

Threats to systems come from three sources: unintentional internal users, malicious internal users and malicious external users. The first occurs because most people do not know the security risks associated with their operations. The next two occur due to deliberate attacks.

Solaris provides powerful solutions to stop such threats. Solaris products which can be purchased along with the OS:

- Solstice Firewall-1

A firewall is a hardware or software mechanism that provides a single point security threat determination and management solution. Firewalls protect access by checking whether all communication between specified computers conform to the security policy.

Firewall-1 combines the best features of hardware and software firewalls, providing a very secure mechanism. It also provides extensive application-level screening of data, as well as packet filtering facilities. Combined with the sophisticated logging and administrative alert mechanism, it offers a complete solution to a company's security needs.

- Solstice Sun Screen

This product from Sun's stable provides an IP authentication mechanism (Simple Key Management for IP, SKIP) to firewalls. This product is protocol independent and is used in the network layer.

The "stealth" mode allows companies to set up a secure Virtual Private Network (VPN), a sort of Intranet, over inherently insecure networks such as the Internet. It is called "stealth" since it is not recorded by any attackers and hence is not identified.

Sun Screen has a centralised hardware device, called Sun Screen SPF-100 and a secure Administration Station, from where all security operations can be centrally configured.

International Security Standards such as the Department of Defence's C2 security level and E2/F-C2 Certification from ITSEC are supported by Solaris.

With such powerful features, Solaris has emerged as a major OS in the distributed or client-server OS market.

Answer: [d] Pluggable Authentication Module

Explanation: Since many authentication schemes are available, Solaris provides a very flexible architecture that allows different authenticating mechanisms to be easily plugged into the OS through the Pluggable Authentication Module (PAM).

the data of a user, even if the computer is shared between users?

- [a] Passwords
- [b] Network Access controls
- [c] Firewall
- [d] Encrypting File System

Module 5- Windows XP Security I

Microsoft's latest Operating System (OS) is Windows XP. This article presents a technical overview of the security features for Windows XP. Windows XP is available in two editions—Windows XP Home Edition for home use, and Windows XP Professional for businesses of all sizes.

Security features in the Home Edition allow users to safely transact over the Internet. Windows XP Home Edition comes with built-in Internet Connection Firewall software to neutralise security threats when connected to the Internet, especially if "always-on" connections such as cable modems and DSL are being used.

Windows XP Professional includes all of the security capabilities of Windows XP Home Edition, plus other security management features. These new security features will reduce IT costs and enhance the security of business systems.

Some of the security features offered by Windows XP Professional are:

- **Network Access Control**
The most common method of intrusion is by logging into a network that allows "guest" users. Windows XP allows very minimum privileges for this account, so anyone trying to break in by password guessing or by any other means, are not granted much freedom to explore the network.
- **Authentication**
With the widespread use of the Internet, many organisations connect their users through it, rather than through domains in a corporate network. This makes secure authentication more important than ever. To achieve a minimum level of security, all users must log on as "Guest." This prevents attackers from using a local Administrator account to log onto the network.
- **Simple Document Sharing**
As discussed above, computers using XP that connect to the network from the Internet and not through a domain are authenticated using the "Guest" account. Further, a simple Shared Documents Properties dialog box replaces the Security Properties dialog box.
- **Blank Password Restriction**
In most corporate situations, users do not use passwords to protect their accounts, since their computers are kept at physically secure locations. No intruder can access these systems, and hence it is safe from external malicious users. However, most of the attacks on corporate systems are found to be from disgruntled employees, who have physical access to the system. Further, portable computers such as Laptops may be stolen, in which case an account with no password can be very dangerous.

To prevent such threats, XP does not allow accounts with blank passwords to be used remotely over the network. This implies that unless the OS is loaded onto the system where login takes place, users cannot have a blank password.

- **Encrypting File System**
The Encrypting File System (EFS) has been introduced in XP to encrypt files in the

system. This is especially useful for mobile users with Laptops. Even if the laptop is stolen, all the data is encrypted and therefore a decryption key is required to view the files. The EFS is based on the Public Key encryption principle and hence uses the Data Encryption Standard (DES) algorithm. Alternatively, DES can be used in triple mode (3DES), which provides very high security.

In the EFS system, encrypting a directory (called folder in Windows jargon) automatically encrypts all subfolders and files inside that folder.

EFS automatically generates the encryption and decryption keys along with a certificate for the user. The prime security feature of EFS is that only authorised users and specified "data recovery agents" can decrypt files that have been encrypted using EFS. Even the System Administrator cannot decrypt files if he is not designated as a data recovery agent for the file.

In a shared system or a system where an attacker has physical access, loading or starting a different OS may bypass the normal mechanisms such as Access Control Lists. However, the EFS protects valuable files with encryption, since the above mentioned technique results only in junk characters being displayed.

Answer: [d] Encrypting File System

Explanation: The Encrypting File System (EFS) has been introduced in XP to encrypt files in the system. This is especially useful for mobile users with Laptops. Even if the laptop is stolen, all the data is encrypted and therefore a decryption key is required to view the files.

Question: Computer Forensics inspection has limitations due to?

- [a] Legal restrictions in the form of limited search warrants
- [b] CMOS information
- [c] Password Protection
- [d] Write-Protect capability

Module 5 - Forensics

Computer Forensics is the science of finding out clues when a security attack has taken place, to find out details about the crime. Forensic inspection of computers and other devices is different from the normal procedures followed in other fields. This article is intended to present a few pointers on how to inspect common computer media.

The similarity of computer forensics to forensics in other areas lies in the fundamental principles of forensics:

- Sterile media must be used
In this context, it means that the examination must be carried out through media which itself is not affected by the intrusion. For example, using an attacked system to send emails on the problem is clearly not advisable.
- Original media must not be used
The compromised systems must not be used in any way for examination. A copy must be made and all checks are to be performed on the copy.
- All material must be documented
Any material that is derived from the forensic procedure such as printouts, copies of files etc., must be clearly documented as to author, date and source.

The most common media used for preliminary investigation are:

Hard Disks

- Any storage media such as a floppy disk must be formatted to prevent viruses before being used
- Forensic software used by the examiner must be a licensed version and may belong to either the examiner or the client company
- Before the compromised system is examined, a list of the various hardware devices must be made along with the name of the manufacturer and other details. If any abnormality is discovered physically, it must be specially noted.
- A binary copy or image must be made of the hard disk and the examiner should work from it. The original should be carefully kept in a secure place
- The CMOS (a small chip in the motherboard) information, which holds the date and time in the computer, must be noted. This helps in understanding when modifications to data has been made
- Boot record holds the information about the OS booting procedure. Hence, this should be carefully recorded along with other important system files

- If files have been found to be deleted, recovery software may be used to retrieve the deleted data
- All password-protected or encrypted files must be unlocked and contents should be inspected
- Importantly, all comments of the examiner must be properly recorded

Floppy Disks

All the above points are applicable to floppy disks too. Some precautions exclusive to floppy disks are:

- Floppy disks have a write-protect capability, by which any modifications to the contents can be prevented. This facility must be used for all disks after they have been used
- The file system is examined and a description of the "entries" found in it must be noted. Floppy disks sometime contain entries in the file system directory, but the corresponding files may be deleted. This can find out whether any data has been tampered with
- Any free space is inspected for data that has been deleted or hidden

Limitations of these examinations

Sometimes, all available data may not be examined due to non-availability or legal regulations. Reasons for such exceptions must be clearly noted along with other documentation. Some of the possible reasons may be:

- Legal restrictions in the form of limited search warrants
- On-site examination, where the examination is conducted at the client's place.
- Huge amount of media to be examined, such as the entire network. In such a case, the examiner may choose to selectively inspect the resources
- Strong evidence pointing to the cause of the problem, if identified, precludes the need for further investigation
- Technical limitations, such as particular aspects of Operating Systems, hardware malfunctioning etc.

Answer: [a] Legal restrictions in the form of limited search warrants

Explanation: Sometimes, all available data may not be examined due to non-availability or legal regulations. One of the possible reasons is that the search warrants issued by courts of law may be limited in scope.

Question: In Windows XP, which component controls access to the credentials of users who are permitted to log onto the system?

- [a] Certification Authority
- [b] Credentials Prompting User Interface
- [c] Group Policy Settings
- [d] Local Security Authority

Module 5- Windows XP II

This article details services provided by the Windows XP Operating System (OS) to guarantee security and privacy to users.

Certificates

For digital signatures, a Certification Authority (CA) is required to certify the validity of the certificate and to confirm that an organisation produces safe products. Windows XP provides Certification Services as part of the OS itself, thus allowing organisations themselves to act as CAs and to sign digital certificates.

The certificates signed using public keys are stored in the personal profile of each user and can be accessed by anyone. However, tampering is not possible since the certificate has been digitally signed.

On the other hand, private keys are created using Microsoft's Cryptographic Service Providers (CSPs). The keys include Base CSP and Enhanced CSP. Since the keys must be kept highly confidential, they are encrypted. Steps for encryption:

1. A random symmetric key called the "user's master key" is generated using a random number generator.
2. The master key is then used to create Triple-DES (3DES) keys.
3. Finally, the 3DES keys are used to protect the private keys.

Credentials Management

"Credentials" refer to the authentication and authorisation of users so that they can login and perform operations on the system. In Windows XP, credential management consists of three main steps:

Credentials Prompting User Interface (UI)

A special application displays this user interface when authentication fails. The user can then enter the user name and password or select a pre-defined authentication mechanism using the X.509 digital certificate. These details may be saved by the application so that the user need not enter them every time he logs in.

Typically, only integrated authentication schemes such as Kerberos, SSL, NT LAN Manager (NTLM) etc allow the saving of authentication data. In third party stand-alone packages used for

credentials UI, the data cannot be saved.

User Information Storage

The Local Security Authority (LSA) controls access to the credentials of users who can log on to the system. Since different users may log onto different servers using the same system, the credentials are stored according to the server to which access is desired. For example, if the user wants to log on to a server called "Server1", then his credential may be stored as " *. Server1." If the same user were to connect to another server called "Server2", it would not overwrite the first one since it would be stored as " *. Server2."

If an integrated authentication package is used, the application will search for the credentials in the stored user name and password list. If there is a match, the credential is supplied by the package without prompting the user to enter the username and password. Else, the authentication package returns an error. Then the authentication package calls up the Credentials Prompting UI discussed earlier for getting the credentials from the user.

Group Policies for Security

Windows XP provides different security levels for users, which can be set according to their requirements. To make it easy for novices and convenient for administrators, XP provides a set of ready-made templates. These templates are in fact a collection of appropriate security policies for use on different systems. The security levels that can be set using these templates are: low, medium and high. These templates can be modified to suit custom requirements. Security policies are also available for standard password management features such as "Required password changes", "Minimum Password Lengths" and other access control mechanisms.

Answer: [d] Local Security Authority

Explanation: The Local Security Authority (LSA) controls access to the credentials of users who can log on to the system. Since different users may log onto different servers using the same system, the credentials are stored according to the server to which access is desired.

Question: What is the methodology used in the Novell Netware Operating System to implement the concept of Access control Lists?

- [a] File Rights
- [b] Trusteeship
- [c] Authentication
- [d] Property Rights

Module 5- Novell Security I

Novell Netware is one of the most widely used Network Operating systems in use today. It coexists along with other OS such as Windows and Unix.

The security features can be categorised into six main categories. The first three, Authentication and Authorisation, Access Control through trusteeship and Access Control through Trusteeship and Access Control through Rights are covered here:

- **Authentication and Authorisation**

Authentication or Login mechanisms are used to control access to the Server, by setting some conditions to log on. The User Name, called a "User object" in Novell Netware terminology, and a password are required to log on to the network.

The administrator creates an account for a user with the NDS (Novell Directory Service) and then assigns some properties for that user. The properties are used to authorise the user to perform operations in the network.

The selection of a good password, as in any other OS, is one of the most important and the most neglected factors in the security of a system or network. Logging onto the Novell server doesn't require a password (if configured so), but having a good password is considered a "best practice." The familiar password mechanisms such as password expiration, forcing users to change passwords etc are available in the OS.

- **Access Control through "trusteeship"**

To grant access to a file or any resource, a User or a Group must be designated as a trustee. Only when a "trustee assignment" is given to a user, access to the resource is possible.

The concept of Access Control Lists (ACLs) in other OS is available in Novell Netware too under the name of "trustee list." Further, when a resource is moved from one location to another, the trustee list is also moved along with it.

When many similar users are to be allowed access to a resource, the best and most secure solution is to group the users under a common name and add the group name to the trustee list. This gives everyone in the group access to the resource.

When all users have to be given access to a resource, assign the trustee rights to [PUBLIC] in the trustee list.

- Access Type Control through "Rights"

The trustee list specifies what type of permissions a user has to access the associated resource. These permissions are termed as "Rights." By default, every list permits all users to "Browse" and "Read". Since every user is also an object, there can be some confusion over allotting rights to users. A trustee list must contain a user object and his rights to that resource, but the resource must not be put in the trustee list of the user.

For example, if a user AAA has to be allowed to delete a file, the trustee list for the file must contain the DELETE right for the user AAA. The file must not be added to the trustee list of AAA instead.

Files, directories and other objects have different attributes and hence different type of rights have to be assigned to each of them. Novell Netware 4.0 provides a variety of rights:

Directory Rights: These specify the access rights a user has for a directory. It must be noted that if a user with directory rights, but not rights to files in the directory and the "Inherited Rights filter" is not set, the directory rights apply to the files also.

File Rights: These rights control access and the type of operations a user can perform to the files.

Object Rights: Objects are other resources in the network such as printers etc. Objects have properties that can be specified by the administrator. Object rights control the access to objects in the network. However, rights to an object are restricted to access to the object itself, but not to the properties of the object. To gain access to the properties, one must have "Supervisor" rights to that object.

Property Rights: As discussed above, rights can be specified only given to objects or to properties contained within that object. Further, access can be restricted to certain properties or given to all properties of an object.

For one user to grant another any right for a resource, he should have "Write" access to that resource. In case of objects, the ACL property must contain the user and the appropriate right.

Answer: [b] Trusteeship

Explanation: The concept of Access Control Lists (ACLs) in other OS is available in Novell Netware too under the name of "trustee list."

Question: In a network using Novell Netware, a user has full rights to a directory. The user, however, must not access one file in that directory. What feature of Netware can be used to achieve this?

- [a] Inheritance
- [b] Inherited Restriction Filter
- [c] Attributes
- [d] Security Equal To

Module 5- Novell Security 2

Novell Security consists of "trusteeship", "rights", "inheritance", "attributes" and effective "rights." This article deals with inheritance, attributes and effective rights.

- **Inheritance**

For every resource in the network, there is an associated "trusteeship list", which contains the user objects and the rights of those users to that resource. To create such lists and rights for every resource and every user can take a very long time for big networks. Hence, the concept of "inheritance" is used to simplify the process.

If a user is given rights to a resource through a trusteeship assignment, all the resources under that resource automatically inherit the rights. For example, if a user is given "Write" access to a directory, it means that he gets the "Write" permission to all sub-directories, files and objects in that directory. However, if objects are present in that directory, only objects with "All Properties" right can access the properties to that object. If rights are assigned only to certain properties of an object, then those rights cannot be inherited by all objects.

To prevent rights from being inherited for a certain resource, the Inherited Rights Filter (IRF) is used. For example, if a user is to be given rights to all files in a directory except one, then the IRF for that file must deny access to the user. In summary, the IRF denies rights, whereas inheritance assigns rights.

- **Attributes**

Certain operations must be recorded, irrespective of which user performed those actions. Further, the descriptions of a directory or a file to allow or disallow certain operations must be specified. In Netware, this is done through the "attributes" mechanism. Attributes are used only for directories and files, but not for objects.

Netware reads the attributes of a file and performs certain operations. For example, an attribute may disallow the deletion of a file. This overrides any rights given to a user to delete the file. Attributes are also set by Netware to indicate that some operations have already been performed. For example, the "last modified date" is an attribute that is set when a user changes the contents of a file.

Attributes cannot be inherited and even an administrator has no privileges to perform a prohibited operation. However, anyone can change the attribute to perform the operation.

- **Effective Rights**

When a user is put on a trusteeship list, other restrictions or privileges may modify the rights in a confusing manner. The final rights of a user after taking into account the various access control mechanisms are termed as "Effective rights". Netware determines these rights through the following criteria:

The trustee assignments to the resource

- Rights acquired by a user through inheritance from a superior resource
- The trustee assignments of the Group to which the user belongs
- Rights as specified in the user's "Security Equal To" list (discussed next)

For example, when a user wants to access a file, the rights specified for him for that file, the rights he has on the parent directory, the rights he has as a Group member and the rights in the Security Equal To list would be examined. Then the final set of rights would be determined and applied to the user.

- **Security Equal To**

When a user has to be given temporary rights to a resource, the first thing to determine the level of rights the user will have on the resource. If another user has the appropriate kind of rights to the resource, then the first user may be assigned a "Security Equal To" property. This property allows a user to access a resource with the same permissions as another user.

This property helps the administrator when evaluating the whole directory structure to decide which rights need to be assigned to which resources.

One important point is that users must not be given the right to add entries to their own Security Equal To list. Then they might add the "Supervisor" right, which then gives them the permission to change anything on the network.

The IRF can be used to block the user from adding to or modifying his own list. However, users who have permissions to manage the rights of other users must have a "Write" privilege on this property.

Another important point concerning this property is that it does not follow the principle of "Transitivity." It means that if a user AAA is security equal to another user BBB and BBB in turn is security equal to CCC, then the user is NOT security equal to CCC. An explicit security equal to relation must be configured between AAA and CCC.

The security equal to property can be dangerous if not properly configured, hence it must be carefully controlled.

Answer: [b] Inherited Restriction Filter

Explanation: To prevent rights from being inherited for a certain resource, the Inherited Rights Filter (IRF) is used. For example, if a user is to be given rights to all files in a directory except

one, then the IRF for that file must deny access to the user.

Question: What feature of the Windows 2000 Operating System provides a single, centralised security administration capability?

- [a] Active Directory Integration
- [b] Flexibility in Authentication
- [c] Consistently enforcing Authorisation
- [d] Public Key Infrastructure

Module 5- Windows 2000 I

The Windows 2000 Operating system is a product from the Microsoft family. It is built upon the tried and tested Windows NT 4.0 engine. It is built for networks connecting corporate intranets and Internet websites, requiring a high degree of security in the OS.

Windows 2000 provides a variety of security techniques in an integrated environment. The suite of services consist of features like the Kerberos Authentication Protocol, Public Key Infrastructure, Encrypted File System (EFS), Centralised security configuration, Security policies for individuals and groups and remote administration.

Windows 2000 security features revolve around three core principles:

- Active Directory

It classifies information in the form of a tree like structure, so that the resources can be administered securely. Organisations can store all confidential data within the Active Directory and implement strict access policies.

Directory containers known as organizational units (OUs) can organize accounts for users, groups, and machines in a domain. Each domain supports multiple OUs, which can be organized in a hierarchical fashion.

Windows 2000 uses Active Directory as the single sign-on means of authentication, thus making centralised administration easier. Further, network resources and other objects are grouped and displayed in the Active Directory in the familiar Windows user interface.

The most important feature or benefit for corporate customers is the ability to organise the network users and resources based on the organisations business hierarchies rather than by pure geographical constraints. This enables organisations to provide user services based on their position in the organisation rather than their physical location.

- Flexibility in Authentication

Windows 2000 works on the layered model for providing security and user-authentication. Depending on the type of users (internal or external), different authentication schemes can be used. For example, the employees may be authenticated using a password mechanism while remote users connecting over the Internet may have supply a digitally-signed certificate to login to the network.

For more security, other methods may be combined to form a multiple-factor authentication. For example, a user may be required to use a smart card along with some biometric detection for authentication.

- **Consistent Authorisation**

As elaborated in a previous article, authentication and authorisation are two different aspects. Authentication is the process of verifying whether the user is allowed to login to the system. Authorisation is the process of verifying whether an authenticated user has the permission to perform a certain operation.

Windows 2000 uses a consistent authorisation mechanism based on Access Control Lists (ACLs). Every resource in the network, including files, directories, programs and hardware has an ACL associated with them. Any user wishing to access a particular resource is checked against the ACL for that resource. Further, when a resource is moved from its location to another, the ACL is also transferred.

This mechanism prevents a hacker from getting hold of the resources even if he has managed to get authenticated. The Kerberos protocol is used along with the authorisation method, so that authorisation over a network is also secure. This provides another security layer and decreases the necessity for authorising the same resource repeatedly.

For example, if a user requests to open a file, the client computer where the user is logged on sends a ticket containing proof of the user's identity. The server compares this information with that of the file's ACL and decides whether to grant the operation or not.

This same model is used throughout the Windows 2000 OS, irrespective of the size or complexity of the network. Any number of resources, present in any part of the world is accessed in the same way through the Active Directory Service.

Answer: [a] Active Directory Integration

Explanation: Windows 2000 uses Active Directory as the single sign-on means of authentication, thus making centralised administration easier.

Question: What feature of Windows 2000 allows for delegation of security responsibilities in terms of group policies ?

- [a] Kerberos
- [b] Centralised Management
- [c] Encrypted File System (EFS)
- [d] NTLM Authentication

Module 5- Windows 2000 II

Windows 2000 provides an integrated set of security features that function more efficiently than a set of unrelated software patched together. The security services in it have been designed keeping in view organisations that have a large number of geographically distributed users. These services enable an organisation in:

- **Secure E-Business**

Business over the Internet requires a high level of security, with authentication being the prime requirement. Windows 2000 supplies the tried and tested security mechanisms such as a Public Key Infrastructure (PKI) by using the Microsoft Certification Server as a Certification Authority (CA) for creating digitally signed x.509 certificates. Protocols such as Secure Socket Layer (SSL), which can protect raw data travelling over the Internet, are also supported.

- **Cost Reduction**

Since Windows 2000 provides an integrated set of security tools to centrally configure, administer and manage the organisation's resources, there is no need to acquire costly third party tools. Further, such tools only form a disparate set and are not so tightly integrated as the Windows 2000 tools are. The centralised management feature provides for delegation of security responsibilities in terms of "group policies", which enable role-based access controls to be implemented.

If the organisation has old operating systems or mainframes, then there has to be perfect coordination between them and the latest OS. Windows 2000 is interoperable with most of the legacy operating systems. Developers can use the Crypto Application Programmer Interface (CAPI) and Security Support Provider Interface (SSPI) to develop secure Windows 2000 based applications. These API allow developers to use the Kerberos protocol in their applications to authenticate users who want to access the application.

- **Secure Mobile and Off-site Communication**

Most organisations have a large number of people travelling most of the time. These people need to stay connected with the office even if they are in any part of the world. Laptops and other mobile devices are most vulnerable to theft and using easily available password cracking tools, a hacker may break into the computer. The Encrypted File System of Windows 2000 enables users to encrypt the files on their hard disk so that no one without the proper decryption key can get confidential data.

Off-site communication, also called telecommuting, refers to the connections of users from home to the office servers, which is becoming more common in developed countries. Wiretapping, eavesdropping and snooping are the various possible attacks on the security of the telecommuting process. Virtual Private Networks (VPN) with latest security standards such as tunneling, IPSec, PPTP (Point-To-Point Tunneling Protocol) and PKI are supported by default in the Windows 2000 OS.

- **Interoperable Security components**

Most organisations have acquired systems in a loosely structured approach, with platforms ranging from Windows to Unix and Novell. Such inter-platform resources must be integrated into the organisation's plans. For example, consider a database application running on a Unix platform protected by the Kerberos authentication scheme. The organisation wishes to enable access to the database to its partners and suppliers. The partner organisation's user accesses the database over the Internet using a standard Web Browser such as Internet Explorer or Netscape Navigator. This access is to a Web Server, typically an Internet Information Server (IIS) running on a Windows 2000 Server through a SSL session. IIS first authenticates the user using Active Directory Services (ADS) and then Windows 2000 authorises the user using the same ADS. If the credentials are valid, the OS then creates a Kerberos ticket and passes it to the IIS. IIS in turn passes the ticket to the database application, which examines the ticket and authenticates the user.

If the database application is also running on Windows 2000, there is no need for the database application to separately authenticate the user as the OS itself authenticates and authorises the user.

Hence, Windows 2000, with its centralised configuration management, flexibility and integrated security tools provides organisations with the power to securely conduct business over the Internet or on a Private Intranet.

Answer: [b] Centralised Management

Explanation: Windows 2000 provides an integrated set of security tools to centrally configure, administer and manage the organisation's resources, thus allowing for delegation of security responsibilities in terms of "group policies"

Question: Which component in the Java Virtual Machine checks the compiled code to see if it matches all the rules and specifications of the Java language?

- [a] Class Loader
- [b] Security Manager
- [c] Byte code Verifier
- [d] Garbage collector

Module 5- Java Security I

The Internet has become the medium of choice for communication, since it helps people transcend the barriers of space and time. Millions of E-mail messages are transmitted every day through the Internet. The latest form of content on the Web is executable code embedded in web browsers.

Java, the programming language took the world by storm with its promises of being the first platform neutral language. Java has contributed to the growth of executable web content through its Java Applets technology. Java applets are scaled down versions of full-fledged applications and can run only inside a web browser, i.e., they do not have the power or flexibility of applications.

Along with the power they bring to the Web, Java Applets also bring some features, which are dangerous if not addressed. The security of a local network connected to the Internet can be assured by:

- Buying genuine software from reputed vendors
- Conducting physical checks on all hardware and software before use
- Using anti-virus software and updating it regularly

Unfortunately, due to its dynamic nature, Applets thwart all such defensive measures. Since an applet can run without having any visual interface, there is a possibility of it creating havoc on an unsuspecting user. However, Java provides some very strong security features that make it difficult for people to use it to cause major damage.

Memory Management

Through memory (mis)management, most malicious users cause applications to behave erratically. "Pointers" are references to memory locations and provide a lot of flexibility for application developers. But pointer arithmetic, i.e., manipulation of pointers is the most frequent method used to abuse this feature. To prevent this, Java doesn't allow pointer arithmetic in applications. Java also has a "garbage collector", which automatically frees up memory resources that are not required by Java programs.

The Java Virtual Machine (JVM) is the part of the Web browser that executes Java applets on behalf of the browser. Three important components of the JVM are:

Class Loader

Every executable piece of code in Java is present in a "class" file. The "Class Loader" is delegated the responsibility of getting the class file from the server and passing it on to the JVM. There are two types of Class Loaders present in a Web Browser:

1. Applet Class Loader, loads only applet class files. Only classes from the specified server and not from any arbitrary server can be loaded.
2. System Class Loader loads classes on the local system or network

Applets cannot create their own Class Loaders to bypass this restriction.

Byte Code Verifier

Any high level programming language has to be compiled before it can be executed. In Java, during compilation, the Java code is converted to "byte-code", which can run on any machine. The class file holds this byte code. The Applet Class Loader loads this class onto the Web browser. The Byte code verifier is responsible for checking whether the byte code in the class file follows the strict rules set by the Java language specifications. Generally, it is not possible to violate these security mechanisms since the compiler itself catches most of these attempts. However, experts may be able to write a Java compiler that does not perform any such checks and hence the Byte code verifier is included as an additional measure of security.

Security Manager

Since all security checks cannot be done at the time of compilation, i.e., in static mode, there needs to be a mechanism to check the code at run-time. The Security Manager performs this function. The JVM invokes the Security Manager to check whether any critical operation requested by the applet is permitted or not. The Security Manager puts some restrictions on the type of code that can be executed:

- When an applet is loaded from the Internet, it cannot access any resources on the local system
- The applet can establish a connection over the network, but only to the server from where the applet was loaded
- The local system properties cannot be accessed by applets
- Applets cannot create or "spawn" new processes

The Security Manager also prevents applets from using a fake Class Loader. Further, applets do not have the permission to create a new Security Manager. However, some web browsers allow applets to configure their own Security Managers, bypassing most of the controls specified by the language.

Answer: [c] Byte code Verifier

Explanation: The Byte code verifier is responsible for checking whether the byte code in the class file follows the strict rules set by the Java language specifications.

Question: Which of the following is NOT a security concern while using Java?

- [a] Intrusion of Privacy
- [b] Message digests
- [c] Denial of Service
- [d] Irritations

Module 5- Java Security II

The Internet has become the medium of choice for communication, since it helps people transcend the barriers of space and time. Millions of E-mail messages are transmitted every day through the Internet. The latest form of content on the Web is executable code embedded in web browsers.

Java, the programming language took the world by storm with its promises of being the first platform neutral language. Java has contributed to the growth of executable web content through its Java Applets technology. Java applets are scaled down versions of full-fledged applications and can run only inside a web browser, i.e., they do not have the power or flexibility of applications.

Since applets are in reality part of the powerful Java programming language, they can be used for malicious purposes. Such destructive applets have been classified into attack applets and malicious applets. The strong security features surrounding the Java environment prevent many of the attacks from being really destructive, but there are some ways by which such restrictions can be circumvented.

- Modifying System configurations

As noted earlier, the Java programming language provides powerful features including access to system memory, file system and processes. However, the implementations of these features have been less than perfect, with the result that some browsers have a faulty Java Virtual Machine (JVM). This can cause malicious applets to bypass the controls built into the language.

It has to be noted that such flawed implementations exist in very limited number of browsers and these attacks have been conducted in laboratories with no reports of them being used on the Internet.

An example of this type of attack occurred in a popular web browser that allowed an applet to create a Class Loader and bypass the Security Manager.

- Intrusion of Privacy

Since an applet can run without being visible on the screen and can also continue to run (in one particular way) even after the applet has exited, this can be used to intrude on the privacy of unsuspecting users. It can hide the IP address of the sender. For example, Java allows programmers to create their own E-Mail programs and hence applets can be used to send forged email messages.

- Denial Of Service (DOS)

A DOS attack is one where the resources of the system are exhausted to the point of system crash. Java applets achieve this by killing other applets running on the browsers, crashing the browser and sometimes the server too. Another variation is to create so many applets that the system resources are exhausted.

This topic is dealt with in detail in a separate article.

- Irritations

As the name suggests, such uses of applets can cause a lot of frustration to users by performing annoying actions like playing noisy sounds or displaying huge time-consuming graphics on the browser.

Java's Security Application Development Interface (JSAPI)

The Java Development Kit (JDK) is the primary resource for programmers to develop applications using Java. The JSAPI was intended to prevent the attacks mentioned above, and to limit their damage in case they occurred. As part of the JDK 1.1, components supplied with the API were:

- Digital Signature Support using Digital Signature Algorithm (DSA)
- Message Digests using the industry-standard MD5 and SHA-1 message digest algorithms
- Key Management for Public Key Infrastructure mechanisms and digitally signed certificates. The certificates supported are those of the X.509 standard and the encryption algorithm for E-mail message, PGP.

The JDK 1.2 version has made some additions to this API as follows:

All executable code, regardless of whether it is loaded from the local system or from another system on the network, is subjected to a "security policy." This security policy follows the familiar Access Control List (ACL), where every resource has a list attached to it that specifies who has permissions for what operations on that resource.

In addition to the components supplied with the JDK 1.1 (discussed above), JDK 1.2 includes:

- Creating and managing Keystores
- Freedom to the user to specify the parameters such as initial keys to algorithms
- Generating parameters for algorithms
- Key factory to help in the conversion of keys from one representation to another.
- Certificate factory support for generating certificates and certificate revocation lists (CRLs).

Answer: [b] Message digests

Explanation: The other three options are possible misuses of Java applets, whereas message digests are a way to allow developers to develop applications that require secure authentication.

Question: At which stage of the data process flow, from source to warehouse, is detective controls implemented?

- [a] Data migration
- [b] Transformation
- [c] Loading
- [d] Reconciliation

Module 5 - DATA INTEGRITY

Introduction

A data warehouse seeks to ensure that the data stored is not of questionable quality. Data may lose its integrity, due to the following reasons: Non-availability of data, or availability of corrupt data

- Migration failure that prevents the right data from reaching the end-user
- Failure of the data cleansing process
- Transformation failure
- Failure of the data loading process

Data Integrity

It refers to information that is complete and correct. It also ensures that data is not corrupt, when stored or processed. Very high integrity standards will not allow users to enter wrong information in the database. End user is not always sure that the information he is getting from data warehouse is correct and solving the purpose of his query. To meet end user requirement, the credibility of warehouse is to be established.

From the IS perspective, it is important to ensure that the correct data is loaded i.e. the loading process is completed without failure. The data warehouse should not accept meaningless, corrupt and redundant data. To achieve these objectives, controls should be placed in the data flow.

Data control points

As the data flows from source to destination, it passes through five stages. They are:

1. Data msing
3. Transigration
2. Cleanformation
4. Loading
5. Reconciliation

Control measures

Data integrity controls are broadly grouped into two categories: -

1. Preventive controls

2. Detective controls.

Preventive controls: It involves attempts to prevent errors from occurring i.e. integrity standards are applied, even before the data enters into the database of the warehouse. The integrity controls are incorporated at different stages of the data flow process, such as the migration stage (transfer of data from source to warehouse), the cleansing stage (the formatting stage of data), the transformation stage (process of utilising only relevant details from warehouse) and the loading stage. Preventive measures are the primary measure to control corrupt or meaningless data from entering the data warehouse, and thus making the database more reliable and user friendly.

Detective controls: It involves controlling errors that creep in after the data has entered the warehouse i.e. detecting the accuracy, redundancy, completeness of data after it has entered into the data warehouse. Integrity controls are incorporated only at the reconciliation stage of data flow process.

At each stage of the data flow process; the integrity of data has to be ensured. In the 1st, 2nd, 3rd & 4th stages, integrity controls are in place, before the data enters the warehouse. But at the reconciling stage, the data is checked for its accuracy and redundancy, after it has entered the warehouse.

Answer: [d] Reconciliation

Question: For maintaining the integrity of data

- [a] Security policy should not be integrated with general policy
- [b] Staff should be trained in validation and incident response procedures
- [c] Backup should be done only of data and not codes
- [d] Auditing is required only of operating system

Module 5 - Data integrity - security

Usually companies become concerned about security only in matters related to viruses, denial of service attacks, intrusion threats and the like. They do not take into consideration data integrity. In this article we discuss the security matters related to data integrity, which includes executable codes as well as stored values.

All security measures should be developed and implemented with a view to prevent security incident. Similarly in data integrity the techniques should be aimed at preventing an incident. Because once an incident occurs it would be difficult or rather it would be impossible to verify if the data is accurate.

Data and code

When an incident occurs or there has been breach of security the first thing to confirm is whether there has been any alteration to the data. For analysing we need information about

- When the data was altered
- What are the alterations
- By whom/ from which terminal or workstation, using which login was data altered

The details about when data was altered and by whom, helps in knowing if the alterations were valid. The details regarding alterations is usually not available unless a full change logs are maintained. This logs help to rollback inappropriate changes.

It is desirable to maintain logs at all levels and they help to know the changes that have happened. Different logs serve different purposes. For example Operating system logs gives details about who logged in, the file that had been accessed.

The maintenance of logs does not serve any purpose unless they are regularly analysed for unexpected changes.

Public documents

Data integrity should be maintained even in public documents. For example, if a company publishes a discount coupon for sale on the web or whenever it involves a monetary transaction, it should care must be taken so that a customer does not alter the amount by using the source document. The company should have some mechanism to verify whether the coupon is valid. The best way to overcome this problem would be to include the code on the coupon that can be verified by the stores point of sale system or it should be developed in a way to prevent any access to source

code. The company should implement similar mechanism in the documents where maintaining the integrity of data is necessary and important.

For maintaining the integrity of data:

- Security policies should be integrated with general policies.
- Procedures should be developed for data validation of coded documents.
- Proper code change management techniques that facilitate verification, auditing and rollback procedures should be implemented.
- Auditing should be done at all the levels whether it is operating system, application code, application execution, data files or databases. To facilitate this, audit logs should be maintained.
- Staff should be trained in validation and incident response procedures.
- Backups should be current and reliable. This includes backup of all data and codes.

Audit:

- Audit of access logs and change logs should be done at regular intervals to detect unauthorised users and unauthorised changes.

The company should try to implement procedures for handling security incidents and maintain forensic evidence following an incident.

Answer: [b] Staff should be trained in validation and incident response procedures

Question: A macro virus infections in a computer will _____.

- [a] Erases the hard disk
- [b] Clears the ROM
- [c] Destroys document files
- [d] Slows down processes on the server

Module 5 – Macro virus

Introduction

A macro is a series of instructions that are automatically executed by a computer. Macros are used to automate repetitive tasks. Many applications like word processors, spreadsheets and power point applications make use of macros.

Macro Virus: These are malicious macros having harmful instructions that are executed automatically, at a specific time or triggered by a certain action. They can also be triggered by another macro. These macros do not cause damage to the ROM or delete the whole hard disk, but they can change a particular application. Almost all MS-Word commands can be executed by macros. This implies that a hacker can do anything (open, modify, delete, save) documents. Some examples of macro viruses are concepts, nuclear, Colors, Dmv, Hot etc.

Properties

- Macro virus can cause "cross platform" infections, i.e. they can work on both Macintosh and Microsoft operating systems.
- Macros were the first viruses to take the form of non-executable files.
- They are self-replicating and can infect other computers over a network.

Macro virus can infect computers -

- Through e-mail attachments.
- By enclosing the macro virus in a HTML message.
- By downloading from an FTP server or website.
- Through secondary storage devices such as floppy, CD-ROMs, DVD etc.

How macro virus are activated

Macro viruses make use of either Internet Explorer or Outlook Express to attach them to the victim's e-mail message. When the user opens the Word or Excel file, the macro attached gets activated. Sometimes, the system's configuration may not be synchronised with the execution of macro virus. In such a case, if the user passes the document over the network, he will not be aware that a macro virus is attached to it and files on other computers can get infected. A macro virus cannot infect files that don't support macros.

Symptoms of macro virus infection

The following are common signs of a macro attack

- Users cannot print the text.
- Names or icons of documents are changed.
- Contents of documents are modified.
- Document is not visible or its location is changed.
- Automatic deletion of documents.
- The document becomes password protected.

Protection against macro viruses

- Detecting the macro virus is somewhat easy because of the fact that when the user opens the document with an inbuilt macro, MS-Word shows a dialog box to enable or disable the macro. If the user has any doubt that the document may contain macro, he can simply disable the macro.
- Delete all macros from the system, and disallow all macros from running.
- Set macro files to Read Only.
- Have anti virus packages installed on your computers to check, detect and clean macro viruses. For example Dr Solomon's, AVP and AVPLITE, F-PROT, Virusscan, Thunder BYTE, ChekMate (2.0), Integrity Master can be used.

Answer: [c] Destroys document files

Module:5

Reference No:M5052

Question: A The malicious program which put a constraint on server's activities over Network is: -

- [a] Virus
- [b] Trojan horses
- [c] Logic bombs
- [d] Worms

Module 5 - Logic bombs and worms

Introduction

A Logic bombs, worms and other viruses had left behind the technology today by their evil technology. It can change protocols, platforms and other features, by making use of their malicious code.

Logic bombs

These are malicious software programs that stay in the system in the dormant state until or unless triggered by some event (appearance or disappearance of specific data). Trigger may be any such as when the system clock reaches at certain date or time, a random number or even some specific event such as deletion of a particular employee record from payroll.

Trigger of logic bomb will do something unpleasant to the system such as changing the bites on the disk to make the entire disk unreadable. Logic bombs are usually transmitted over the

network by computer Viruses or Trojans. If the logic bomb is a part of virus then it can replicate itself and make their way to other files. The user can send those files to other computers without realising that these files are infected.

E-mails and logic bombs: Everyday millions of e-mails are send over internet and it is possible that a logic bomb makes its way through word processor or spreadsheet macro. It is activated as soon as application is opened and can wipe off all the hard disk of user. The macro is much more dangerous because it can escape from anti-virus detection

Worms

A worm is malicious computer program that has the ability to replicate itself from one machine to another through the network. It is different from virus in the sense that it needs not to attach itself with a document or executable file to replicate. They use computer time and network bandwidth to replicate. Worms do not affect isolated PC in a network because they are designed to attack the network servers.

Unlike other malicious programs worms do not destroy the data but it fills up the storage space in hard disk, which results slowing down the processing activities of computer. For example in 2001 a worm called "Code Red " had slowed down the Internet traffic by replicating itself more than 250,000 times in only 9 hours time. This worm targeted Windows NT and Windows 2000 over network and wherever the "Code Red " find insecure server. It had copied itself to that. Red Code was designed to do three works:

- Replicate itself for first 20 days of each month.
- Replace web pages of infected server with desired pages by hacker.
- Damage the web server of white house.

Countermeasures for malicious software

1. Security awareness: It is the most powerful measure to prevent such software to enter computer system.

- User should buy software only from reputed companies and data should also be accepted from trusted resources.
- User should not open suspicious mails.
- User should not visit 'hostile' websites.

2. Anti-virus scanners: These products scan files and folders for viruses or other malicious programs and inform the user about the same. Since new viruses are coming by the passage of time so these anti-virus tools should be regularly updated.

3. Integrity checkers: It checks the modifications in the file. Integrity checkers do it by checking the current checksum (A number is added when data is sent from one place to another and when it arrives to the destination, this number is checked and if matched then it ensures error free message) and comparing it with baseline checksum determined at the time of installation.

4. System hardening: It can be done by controlling system access and executing the application by minimum privileges. This will minimise the harm caused by malicious programs.

Answer: [d] Worms

Question: Which of the following statements is true about " Trojan-horse"?

- [a] It is a useful computer program
- [b] It is a malicious computer program
- [c] It is an anti-virus package
- [d] It is a powerful supercomputer

Module 5 - Trojan horses

Trojan horses are destructive computer programs that apparently perform a useful function, but are actually designed to destroy data or steal password. It is not a virus because it cannot replicate itself, but it might carry a virus with it. There are basically two types of Trojans:

- Remote access or "backdoor" Trojan. Eg. Netbus, BackOrifice
- Software bombs. Eg. Logic bombs

These types of malicious software can cause severe damage to the system. When the computer is infected with Trojan horse some common symptoms (which may or may not be visible when PC is on) are:

- Current programs not working properly
- Failure of hardware
- Programs opening simultaneously
- Change in wallpaper on desktop without any prior notice
- Automatic opening and closing of CD drives
- Pornography loaded on PC without owner's knowledge
- Password change in computer
- Problem in prompting
- Virus scanner disabled
- E-mail failure, may be due to password change

Spreading of Trojan horse

Trojans are spread by e-mail attachments and as files that mislead users into appending them to an uncorrupted file. The moment the Trojan is executed, the hacker comes to know since the victim is online at the time. The hackers can then:

- Retrieve the password and use it to access the victim's mail account or use dial up connection to trade with other hackers
- Make undesirable changes in a website of a particular victim and can change the e-mail ID and password
- Access victim's files
- Gets to know the keys used by the victim with the help of key logger. The Trojan program stores all the keys even if the victim is off line
- Turn on victim's web camera and watch him without his knowledge
- Use victim's connection to scan for other infected computers

- See, whatever is visible to victim on his desktops

Measures to remove Trojan horses

1. **Handle attachments carefully:** One should never open attachments received by e-mail, if user is not sure of the sender. It's advisable to delete such attachments.
2. **Anti-Trojan program:** Anti-Trojan software will detect the Trojan on an infected machine and then remove it. Some of the most popular anti-Trojan software are The cleaner, TDS, Tauscan, Pestppatrol and PC DoorGuard. The user should run a complete scan of the system frequently and keep the anti-Trojan software updated. Anti-Trojan software are specialised in recognising, detecting and removing the Trojans only. They are not efficient in combating any other type of malicious software.
3. **Download:** The user should download the information only from reputable sites.
4. **Backups:** User should have backups for their most important and confidential documents in some secondary storage medium such as floppy disks or CDs.

Answer: [b] It is a malicious computer program

Module:5

Reference No:M5054

Question: What feature of Linux allows a secure connection between client and server for generally insecure services such as Telnet?

- [a] Password Protection
- [b] Logging
- [c] Secure Sockets Layer (SSL)
- [d] Secure Shell (SSH)

Module 5 - Linux Security 1

To ensure total computer security, each level of the system, right from physical security to application security should be taken care of. Most attacks target one area: the operating system (OS). If an attacker gains control of the OS, the entire system is under his control.

The Linux OS is an open source OS that is based on the Unix Operating System. Developed by Linus Torvalds, the OS seeks to combine the power of Unix with the ease GUI-based Operating Systems.

This article discusses some aspects of OS security with particular reference to the Linux OS.

Security in an OS can be achieved either passively or actively. The main difference between the active and passive approaches is that in the active model a "Prevention is better than cure" approach is followed. The passive model involves monitoring the operation of the system (and the network) and believes in a, "Let's cross the bridge when we come to it" approach.

For instance, checking the server logs regularly to identify a malicious user is a passive approach, whereas installing a program to prevent the user from being authenticated is an active approach.

Although the "kernel" (the heart of an OS) and some other utilities of the Linux OS are free, users need a variety of applications. Many companies provide utilities and customer support at a certain fee. Each product of the Linux OS is called a "distribution." Major distributions in use today are RedHat, Caldera, Mandrake, Suse and Debian. There are also a number of distributions for specialised purposes like those available only for running Web Servers.

Some tools are bundled with all Linux distributions. Security tools that use the active approach are:

- Password Shadowing utilities used to authenticate and manage users by using encrypted passwords
- Kerberos v5.0, a protocol widely used to enable secure authentication over an unsafe network
- Secure Sockets Layer, a protocol that helps other services run on top of a secure channel. SSL is typically used while submitting credit card information through the Internet
- SSH, an acronym for "Secure Shell" is used to create a secure connection between a client and server for inherently insecure services such as Telnet and FTP (File Transfer Protocol)

Security tools found in Linux that use the passive approach are:

- Applications or scripts that determine whether certain system files and directories have been modified or changed. This can help system administrators to find out if an attacker has compromised the system and made changes either to cover his tracks or to make more holes in the system. An example of a common tool used to achieve this is "Tripwire."
- System administrators frequently use a set of tools to check known vulnerabilities in the OS and other services offered by the OS. Port scanners and password crackers are used to see if there are any open ports on the system and check the efficacy of user passwords respectively. Often, these tools are integrated into a suite for easy administration. One such toolset is "COPS."

Note: Active and passive methods are covered in another article, Linux Security II

Answer: [d] Secure Shell (SSH)

Question: Which of the following is a passive measure for securing the Linux Operating System?

- [a] Restricting administrator access
- [b] Logging
- [c] Running only necessary services
- [d] Application auditing

Module 5 - Linux Security 2

The Linux OS is an open source OS that is based on the Unix Operating System. Developed by Linus Torvalds, the OS seeks to combine the power of Unix with the ease GUI-based Operating Systems.

Some active security measures in Linux are:

- Restricting "root" access: The administrator account in Linux is called the "root." Through this, one can execute any command without restrictions. However, taking advantage of this, users may perform a destructive operation either knowingly or unknowingly. Hence, all operations not directly related to actual administration should be performed by creating appropriate accounts only for those operations
- Keeping track of applications: To be useful, an OS necessarily has to run a variety of applications. Most applications have vulnerabilities, but these are soon discovered and made public along with the required patches. Therefore, keeping in touch with various sources to learn about such vulnerabilities can lessen the chances of an attacker using them
- Running only what you need: Most services provided by Linux are not necessary for individuals or organisations. These services often have a number of "exploits" which are used by attackers to compromise the system. Care should be taken to run only those services that are needed and disable the rest. This also helps in conserving system resources, such as hard disk space
- User awareness: Educate users on the need to practise active security by using passwords that are difficult to crack
- File system security: Ensure that system files are placed in the right directories and permissions are not granted to read or modify them.

Passive measures for Linux security are:

- Logging: Linux provides powerful logging capabilities to record all the actions of specified users. All the operations by, say root, can be logged to a particular file and then crosschecked according to the time when the action was performed. If the administrator had not logged in as root at that time, but the logs show that certain operations had been performed as root during that time, then it is almost sure that to see if someone has intruded the system.
- Delete non-user accounts: Most administrators do not delete the accounts of users who have left the organisation, simply because there is almost no interaction between the concerned department and the system administrators. Malicious employees might use

these accounts to exploit the system.

If a Linux-based computer is used as a primary server, it is important to be careful about the "Samba Server" that comes bundled with Linux. It is a powerful tool that provides Linux with connectivity to other network operating systems such as Windows NT and NetWare. Samba lets Linux mimic the file and print services of Windows NT and similar services. It also takes the place of an NT Primary Domain Controller. The PDC acts as the central authentication server for the entire network, for global user authentication and resolving domain trust relationships. If Samba is used, it can reduce the threat level in a Linux-NT dual-boot installation.

The basic vulnerabilities of the Linux OS are: passwords, file system permissions and Denial Of Service (DOS) attacks. DOS is an attack on the system that blocks resources and legitimate users do not get to use services. The best way to prevent such attacks is to use firewalls and other software that can recognise a DOS attack. A thorough assessment of the required services and the removal of those that are not required can go a long way in securing the system.

Note: For more information, see Linux Security 1.

Answer: [b] Logging

Question: Arithmetically business risk is defined as business value x threat x vulnerability. Thus if there are no threats it means that the business risk

- [a] Does not exist
- [b] Exist
- [c] Will exist in future
- [d] None of the above

Module 5 – Cost-effective Information Security – Part 1

Every company has certain business objectives. To achieve these business objectives, now a days, companies rely on information and associated Information Technology (IT) services. If the information and associated IT services are affected then the entire business will come to a halt. While companies strive for successful realisation of business objectives, they are constrained by their budgets. Cost effective management of business processes, information, Information Technology services and hence information security is essential for both competitive edge and survivability of an organisation.

The information security to be implemented should be in accordance with the requirements. The need for information security should take into account the cost of providing the information security measure and the added value of the implemented information security measure. The decision for information security must be arrived at after taking into account the business risks that again has to be based on risk assessment.

Before we go further let us understand what is business risk and risk assessment.

Business risk: They are the existence of such threats that materialise into security incident causing damage to the information and IT services of the company. The affect of damage would depend upon the value of the assets affected.

In terms of arithmetical definition

Business risk = business value x threat x vulnerability

On this basis we can say that business risk do not arise if either threat or vulnerability do not exist. Therefore the security needs should aim at mitigating threats and vulnerabilities. Mitigation of threats and vulnerabilities should be mainly focussed on information and IT services having high business value and are exposed to significant risks.

Risk assessment: Risk assessment is the process of identifying assets that have high business value and that are exposed to significant risks. The risk assessment can be accomplished with ease by taking the inventory of information and IT services that are exposed to business risks or that are of a major value to the company, as the base.

Costs of security: The management should prioritise areas requiring security and the level of security to be implemented, as all the assets will not be exposed to the same level of risks. The cost of security should be appropriate to the assets value and the risks to which it is exposed.

There may be instances where the cost of the security would exceed the risks that the asset faces. In such situations it is better to accept the security risks.

Answer: [a] Does not exist

Module:5

Reference No:M5059

Question: Which of the following is a feature of ActiveX controls that can both be used as well as misused?

- [a] ActiveX controls can be reused
- [b] ActiveX controls can access system resources
- [c] Many pre-developed controls for performing many tasks are available
- [d] Execution of ActiveX controls can be controlled using Internet Explorer security settings

Module 5 – ActiveX Controls – Part II

This article covers one more type of security concern of ActiveX controls i.e., Running ActiveX controls and also the benefits of using them. The security features provided for safe execution are also detailed.

Running Controls

- Since ActiveX controls do not run in a sandbox, they can access the resources of the system they run on
- The security mechanisms are usually applied only in Internet Explorer. However, applications also can use the same control, but do not provide the same security mechanisms
- Even the security mechanisms provided by Internet Explorer are not comprehensive. There is no way to run a control independently of the security settings of other controls. All the security features apply on an "all or nothing" basis
- The privileges of the user executing the control are applied to the control. There is no provision to restrict the privilege of the control. For this reason, most system administrators do not use the administrator account for browsing the Internet or installing ActiveX controls
- ActiveX controls may claim to do some thing, while actually performing some other operation
- There are no proper tools to manage and audit the installation and execution of ActiveX controls
- Scripts that use ActiveX controls cannot be predicted as to how they will run, either by the developer or by the end user. Further, it is not possible to determine whether a HTML document contains an ActiveX control or not
- Scripting languages such as JavaScript can invoke operating system code, which may be dangerous

As with any other software, ActiveX have a beneficial side as well. Since the benefits usually

outweigh the risks, ActiveX controls have become popular. Some of the benefits are enumerated below:

1. *Code Reuse*: The interface between the control and the invoking application is standardised and hence any ActiveX-aware development environment can use an existing control. For instance, if a control is developed in Visual Basic, then it can be used in a C++ application without any changes
2. *More capability*: Since ActiveX controls do not run in a sandbox, they have the ability to access system resources and hence can perform more tasks than other technologies such as Java applets
3. *Wide availability*: Many ActiveX controls to perform a wide variety of functions are available. It is often cheaper and faster to purchase an existing control and tweak it rather than develop the whole thing from scratch

Security features

The security features of ActiveX are:

- *Security Zones*: Internet Explorer provides three security settings in the form of zones - high, medium and low. Installation and execution of ActiveX controls can be controlled using these three zones
- *Administrator approval*: Within each Internet Zone, there is a setting to allow only those controls approved by the administrator to run.
- *Authenticode*: It is a set of Technologies developed by Microsoft to digitally sign the controls and monitor their downloads
- *Windows 2000 Group Policy*: Windows 2000 provides a feature by which the group policy settings include ActiveX as part of the monitoring process. This means that multiple users sharing the same system do not face any risk by one user downloading an unsafe control.

Answer: [b] ActiveX controls can access system resources.

Module:5

Reference No:M5060

Question: For a threat to cause damage _____ should be present:

- [a] Vulnerability
- [b] Incident
- [c] Disaster
- [d] None of the above

Module 5 - Cost-effective Information Security - Part 2

Cost effective management of business processes, information, Information Technology services and hence information security is essential for both the competitive edge and survivability of an organisation.

The security measures should form an integral part of business process. The management should make a decision about the security measures to be implemented. Each security measure has costs

related to it. The most effective measure should be determined after taking into consideration the related cost. The management would be in a better position to take a decision if it has a complete overview of the cost elements associated with the implementation of the security measures.

Let us discuss what are the costs associated with the information security process. An overview of the information security process is illustrated for a better understanding.

The cost elements of information security are as under:

- Security policy: On the basis of business objectives the security policy is framed. The security policy provides the guidelines for framing processes and procedures.
- Risk assessment: It identifies the need for security.
- Selection of security measures: The management always aims at implementing those security measures that are cost effective. Where the cost effective security measure cannot be implemented it is better to accept the associated risk.
- Planning: After the security measure is selected, a plan should be framed for implementation of security measure.
- Implementation: While implementing the security measures, security tools, the set up of the company, development and documentation of process and procedures should be taken into consideration.
- Operation: It includes day-to-day operations of the security measures e.g. authentication and authorisation, security log evaluation.
- Audit and evaluation: Audit and evaluation is required for measuring and reporting on the effectiveness and efficiency of the security measures. The key performance indicators should be measured for efficiency i.e. cost of the security and the effectiveness.
- Improvements: Improvement should be based on the recommendations and fact-findings of the audit and evaluation step.

The above-related costs should be considered before making a decision on the security measure to be implemented.

Threat materialisation:

After implementing the security measures the management must determine the residual risk as security measures mitigate only part of all risks. Security measures do not assure that all the risks are eliminated.

The threat before it causes damage passes through vulnerability stage and incident phase. Let us understand what is meant by threat, vulnerability, incident and damage.

Threat: Threat leads to a security incident. Threats can arise out of technical or human errors. But majority of threats are a result of human and procedural errors.

Vulnerability: For a threat to cause damage, vulnerability should be present. In other words without a vulnerability, security incident may not happen.

Incident: Incident is breach of security. Depending on the business value of the information and IT services the incident may cause more or less damage

Damage: Damage that has been caused to information and IT services must be corrected.

The management must determine in which phase of threat materialisation security measures have

been implemented to estimate the damage that can be caused.

Answer: [a] Vulnerability.

Question: Session-hijacking refers to

- [[a] A type of attack where the web pages are defaced
- [b] A type of attack where the session ids of other users are guessed
- [c] A type of attack leading to increased privileges for the attacker
- [d] Using sessions to track the state of users

Module 5 - Application Security I

Although there are many reasons for compromise of network security, one critical reason is that all components of a company's IT infrastructure are not looked upon as an intrinsic whole, but in isolation. The network, Operating Systems, Web Servers, applications, back-end databases and middleware connecting databases to applications etc are either developed or acquired without assessing them as one.

Applications developed in-house or outsourced are usually developed without security in mind or according to any specific standards. Further, they are not included when a security team surveys the organisation for possible breaches. These developers may not have much experience in security attacks and defences and are recruited only for their skills in application development.

It is not generally recognised that applications having major security flaws can get through all strict defences including firewalls and proxy servers. If such flaws are detected after most of the application has been developed, it may be expensive and time consuming for the organisation to rework it or patch it up using other security measures.

A security expert must work closely with application developers and check whether the logic used is free from vulnerabilities. Further, the developers must be properly educated on the various ways an improper application may be exploited by a malicious user.

In the early days of the Web, sites consisted mostly of static HTML pages. Breaches usually resulted in defacing of websites, but there was no threat to the Web server or the system. With the advent of dynamic scripting and server side languages, the threat has increased greatly. For instance, a B2B (Business to Business) or a B2C (Business to Consumer) web site uses many applications, scripts, databases and other code with interaction among them. Malicious users can circumvent security by using the privileges of applications to perform unauthorised tasks.

Every TCP/IP connection has an associated "port." Firewalls and Proxy servers can be configured to allow only certain ports to initiate or accept connections. Typical ports allowed are 80 for HTTP (accessing the web site), 443 for HTTPS (Secure HTTP). If an internal user tries to compromise the network, adequate safety controls can be built into the operating system. However, a user using the web services to call up an insecure application can wipe out all the controls in the existing security architecture.

The ideal way to avoiding such occurrences is to promote a Security Life cycle in parallel and integrate it with the Systems Development Life Cycle (SDLC). Security must be built into the application right from the planning stage. Modularity in developing a large application can minimise

changes in the application in case there is any security problem.

To develop secure applications, it is necessary to understand the type and nature of attacks that are possible. Such attacks can be classified as:

Privilege Elevation

This refers to a type of attack where a malicious user having a low-privileges account on a system manages to get into the administrative account, usually termed "root", "administrator" or "superuser." Once this account is breached, the whole network is under threat, since it allows him to do virtually anything.

Unauthorised access to Data

Although this type of attack is normally the most popular and easily understood, there are some aspects that are not understood by a majority of people. Unauthorised access to data is one thing; unauthorised access to data that in turn can be used to access highly protected data is more dangerous. For example, consider a type of attack called session-hijacking.

When a web site wants to maintain the sessions of users after they have logged in, it uses session ids since HTTP (the protocol supporting web pages) has no provision for maintaining the "state" of such users. By guessing what the session ids can be, an attacker can easily masquerade as a legitimate user, especially if a user logs on to the server and fails to log off before he leaves. Once a session has been hijacked, the attacker can use the services of the server to perform malicious acts. The point to be noted here is that application developers using sessions for maintaining the state of their users must evolve random session ids that are nearly impossible to guess.

Answer: [b] A type of attack where the session ids of other users are guessed

Question: A hacker changes data stored in hidden form fields to reduce the price in online shopping. This type of attack is called:

- [a] Denial of Service
- [b] Dynamic Scripting
- [c] Data Manipulation
- [d] Identity Spoofing

Module 5 - Application Security II

Applications have to be developed with security in mind. A previous article covered the need of incorporating security and also the discussed two of the types of threats due to insecure applications, viz., Privilege elevation and unauthorised access to data.

This article covers Denial of Service, Data Manipulation etc.

Denial of Service

Denial of Service (DOS) refers to a technique used by attackers to disrupt the working of a large network or Web site. Any resource that is not available to legitimate users due to excessive requests by malicious users is subjected to a "DOS" attack.

For instance, if an application needs to be run under a particular account, an attacker can prevent the application from running by trying to log on to the account many times. The Operating System will then disallow the login procedure and lock the account for a certain period of time.

Another example of a real time DOS attack is that of malicious code inserted into popular applications and then distributed as legitimate applications. The Kazaa and Morpheus applications are used to share files in a peer-to-peer computing model. These are hugely popular and downloaded by many users. A hacker could insert dangerous code into such applications, termed as "backdoors", and then distribute it. When a user starts the application, the backdoor communicates all user information to the hacker without the user even knowing about it.

Since the backdoor uses the normal ports such as HTTP, this type of attack also circumvents the personal firewalls used to protect users.

Data Manipulation

This type of attack involves changing the whole or some part of data that causes a substantial loss to the owner of the data. Defacing of web pages and financial data manipulation are common examples.

For defacing web pages, an attacker gets access to the directory on the web server and changes the HTML (the language used for developing web pages). The second type of attack is possible only due to the lack of security awareness among application developers. For instance, assume that a web site sells some merchandise on its site. If a user purchases items across multiple pages, then the information about the items and the prices must be carried over till the checkout page. Developers typically use hidden form fields to propagate this data among multiple pages.

A clever attacker can view the source code for the web page, find out that there is a hidden form field and manipulate the values, say from Rs.500 to Rs.5. He therefore gets billed for a meagre amount whereas the actual bill would be much more. This type of attack could be prevented if the data is stored on the web server rather than put it in a hidden field. Alternatively, the web site has to check the prices once again at the checkout page before billing the user.

Identity Spoofing

Identity spoofing attacks are another form of masquerading. In this type of attack, an attacker pretends to be a legitimate user and performs operations on behalf of him. As explained in an earlier article, Session hijacking is one way to do this. Other ways this could happen are when users send user names and passwords in unencrypted form over the Internet or choose easily guessed passwords.

Dynamic Scripting

Dynamic scripting or cross-site scripting is a new technique that takes advantage of URL (Uniform Resource Locator – the path to a document on a server) obfuscation. In this, a malicious script is disguised as a URL variable within a proper looking URL. This is then sent as a link in an e-mail message promising the user many goodies if he clicks on it. On clicking it, the script will then run on the user's browser. This may not affect the web site as such, but the script can be written so as to collect passwords, credit card numbers and so on silently without the user's knowledge.

Answer: [c] Data Manipulation

Module:5

Reference No:M5063

Question: Which of the following is the most common type of input validation to verify the length of a number entered by a user in a numeric field?

- [a] Form-Level
- [b] Validation lists
- [c] Field-Level
- [d] Filtering Keyboard Input

Module 5- Input Validation

When a user enters data that needs to be saved, it should be entered in the correct format. Input validation methods ensure that the right data is entered. However, input validation should not be confused with "error-trapping" or correcting errors after all the data has been entered." Error trapping is time-consuming. It also causes a lot of inconvenience to a user if an error is detected and indicated after a lot of data has been entered. Input validation can be used to prevent errors before they occur and if possible, correct them too.

For example, if a field requires that all characters must be in uppercase, the program should be

written in such a way that it automatically converts all characters entered in lowercase to uppercase. If a user enters lowercase characters, he will not be prompted to correct the errors and hence time is saved.

When data is entered in some fields, there are other fields that also need to be supplied with related data. Such fields are called "conditional fields." For example, if a user checks a box that asks him whether he wishes to use a credit card or not, the credit card number field must also be filled for the process to be complete.

Some input validation methods are:

- Field-Level Validation

Fields in a data collection application correspond to fields in a database. It is also the starting point for which validation can be performed. Field level validation is used to ensure that the right characters in the proper format are entered. Further, the value entered must be among the permitted values for that field.

- Keyboard Validation

The keystrokes of a user are captured, and only the relevant ones are passed on to the application. For example, if an input field requires a user to enter his telephone number, a message is displayed if the user presses an alphabet key. Alternatively, invalid keystrokes are ignored or if possible converted to a permitted value.

- Validation Lists

This is also a very common method of input validation. In this case data that is to be entered can be chosen out of a list of predefined values. This is the best method to prevent the user from entering wrong data.

The values are placed in a drop-down list, out of which the user can select the value he wishes to enter. This might require some extra work when creating the user interface, but it is a one-time affair and provides a complete solution to preventing errors in data inputs.

- Form-Level validation

Any input validation process would be incomplete without having a form-level validation. This validation is generally done after all the fields have been entered and the form has been submitted. Most of the errors are caught at the field-level validation, but some errors can slip through this stage, hence form-level validation is necessary.

The most common form validation methods are:

Data value range checks: All values are checked to see if they fall between the accepted limits for the respective fields. For example, fields requiring a date to be entered for sending a bill may adhere to certain business rules like "the date should fall between the current date plus 28 days (credit limit)".

Data value lengths: Some fields must have a certain length for the data entered to be valid. For example, a credit card field must have 14 or 15 characters depending on the type of credit card being used.

Mandatory fields: Certain fields are compulsory or mandatory; this means they must be filled in before data can be saved.

Conditional fields: Some fields take values depending on the value entered in other related fields.

For instance, a credit card user is asked whether he wishes to purchase a product. If he says "yes", a credit card list is presented (validation list as well as dependent field), which allows him to pay using three different credit cards. On selecting a credit card, another numeric field is presented to enter the related credit card number (dependent field). Data entered is then checked for numeric characters (field validation) and length for that specific credit card (form-level validation)

Answer: [a] Form-Level

Module:5

Reference No:M5064

Question: In a Denial of Service attack, a "TCP SYN flood " attack is an example of:

- [a] Network Resource exhaustion
- [b] Memory consumption
- [c] Exploiting of the target's own resources
- [d] Configuration information alteration

Module 5- Denial Of Service

Denial of Service refers to a technique used by attackers to disrupt the working of a large network or Web site. Any resource that is not available to legitimate users due to excessive requests by malicious users is subjected to a "DOS" attack.

The most common type of attack is the "asymmetric" one, in which an attacker with a slow computer can bring down a large and highly secure network. This is partly due to the nature of networking protocols such as TCP/IP, which have no inherent security mechanisms.

The different Denial Of Service attacks are:

- Resource Exhaustion

This type of DOS attack concentrates on exhausting the resources needed to efficiently run a network of computers. Some resources are critical such as RAM (memory), hard disk space, processor operations etc. If these critical resources are hogged by one program or service to the complete exclusion of others, a DOS attack has occurred.

Resource exhaustion is again divided into the following:

1. Network Resource Exhaustion: This invariably means hogging of network bandwidth and is very frequently used against Web sites. The design of the TCP protocol is taken advantage of to mount a DOS attack. As detailed in an earlier article, TCP connections follow a three-step process. In this attack, only two steps are completed and the server keeps waiting for the client to complete the third step so that connection can be made. But the client not only refuses to complete the third step, but simultaneously initiates similar such incomplete connections. The server indefinitely waits for all the requests and the entire server space is allocated. This type of attack is called a "SYN" flood attack. Many more such attacks are possible with the "tear drop" attack being common.

2. Using the Target's resources against itself: This attack is a type of "self goal", where the attacker uses one of the computers in the target network against another system on the same network. "Smurf" and "Snork" are examples of this type of attack and use two different mechanisms, but the result is the same. Smurf uses the Internet Control Message Protocol's (ICMP) ECHO command to flood the network with useless information, while Snork exploits unpatched Windows NT systems running the Remote Procedure Call (RPC) services to raise the processor's utilisation to almost 100%.

3. Exhaustion of other resources: The Operating System (OS) uses "Data Structures" to store data about the various services it is running currently in one location. Further, other resources such as memory and hard disk space are also needed by the to perform its operations. Attacks to exhaust such resources include sending of multiple e-mail messages, creating copies of various programs, performing unnecessary tasks etc.

- Destruction of System information

If an attacker manages to modify the contents of the system files, the OS may start functioning erratically. For example, if the Windows Registry is modified, even some access control measures may not work. Sometimes, the OS itself may crash due to improper configuration of the registry.

- Physically damaging the hardware

This type of attack is very rare, because most corporate networks are physically well protected. However, due care must be given to this aspect, since any destruction to the hardware can nullify any security measures taken in software to protect the system from attackers.

Answer: [a] Network Resource exhaustion

Module:5

Reference No:M5066

Question: When data is accessed through both sequential and direct access methods the process is called:

- [a] Sequential storage and retrieval
- [b] Direct access and retrieval
- [c] Indexed sequential storage and retrieval

[d] None of the above

Module 5 - Data Storage and Retrieval Methods

While reading a novel, we start from Page 1 and go on to the end sequentially. However, when it comes to a catalogue, we can locate the information for an item we want with the help of the index provided at the beginning. The same principle holds good for the storage and retrieval of data stored in computer-usable form.

In a computerised environment, a database is thought of as a file cabinet, a file drawer can be understood to be a file and the folders inside it to be records. There are a number of ways in which we can store data. Three principal methods are:

- **Sequential storage and retrieval:** The sequential storage and retrieval method is ideal for situations in which most of the records in a file need to be accessed for performing functions like producing payroll etc. In this method, data is retrieved in the sequence in which it was recorded on the storage device. The records must be accessed one after the other i.e. the user cannot jump to any record he wishes. A magnetic tape is one of the most commonly used sequential storage devices.
- **Direct access storage and retrieval:** Direct access storage and retrieval, also called random access, is best suited for situations in which only a few records in a file need to be accessed, in no particular sequence. Airline reservations systems rely heavily on this method because there is no way one can predict which customers will call to inquire about the status of flights. Hence, individual records containing the status of the flights need to be stored in a manner in which they can be retrieved in any order. There are a number of ways to access records directly. The most common method is to use a unique data element called the key field. This field helps in unique identification of the record. For example, a bank customer is identified by his/her account number. This number is unique for every user and cannot be duplicated.
- **Indexed sequential storage and retrieval:** In a payroll system, all records are usually accessed using the employee number, (sequentially), when payroll cheques are produced. However, occasionally a clerk in the payroll department may need to check the status of a particular employee. In this case, processing the records sequentially just to access data for a single employee is not practical. To be able to access stored data either in a sequential or direct fashion, a third methodology was developed called the indexed sequential access method or ISAM.

Sequential storage and retrieval is appropriate for updating master files on a regular basis. Direct storage and retrieval is used for irregular updates having small volumes of input. ISAM is slower than direct access and the hardware and software needed for ISAM is more expensive. Also, ISAM makes less efficient use of storage space.

Answer: [c] Indexed sequential storage and retrieval

Module:5

Reference No:M5068

Question: Which is the right combination with respect to pointing devices?

- [a] Light pen and tablet.
- [b] Mouse and digitizer.
- [c] Digitizer and tablet.
- [d] None of the above.

Module 5 - Pointing Devices

Data input also involves entering commands and selecting options. Various pointing devices were designed to make this easy. Each of these devices allows the user to identify and select the necessary command or option by moving the cursor to a certain location on the screen or table and sending a signal to the computer. For this reason they are sometimes also called pointing devices and are mainly used in menu-driven programs i.e. programs that offer varying levels of menus or choices to the user to lead him or her through the program functions. Let us now see the various options available to the user.

- **Light Pen:** The light pen uses a light-sensitive photoelectric cell to signal screen position to the computer. The pen is pushed to close the photoelectric circuit thereby indicating the X-Y coordinates to the computer. Light pens are frequently used by graphics designers, illustrators and drafting engineers.
- **Mouse:** Mouse is a hand-held device connected to the computer by a small cable. As the mouse is rolled across the desktop, the cursor moves across the screen. When the cursor reaches the desired location, the user usually pushes a button on the mouse once or twice to signal a menu selection or a command to the computer. Mouse technology is often used with graphics-oriented microcomputers. With special software for graphics, the mouse can be used like a pen or a paintbrush to create figures and patterns directly on the monitor. The keyboard must still be used to type in characters and issue some commands, depending on the software.
- **Touch Screen:** Limited amounts of data can be entered via a terminal or a microcomputer that has a touch screen. The user simply touches the screen at the desired location to pass signals to the computer. For example, in widely used ATMs touch screen is the most common form of interface with the bank network. The interfaces present the options of either withdrawing or depositing cash which can be selected by touching the screen at the respective position.
- **Digitizer:** An interesting method of input that is used in map making is the digitizer or digitizing tablets. The tablets are the working surface which comes in different sizes. Each is covered by a grid of many tiny wires that are connected to the computer. Drawings placed over this grid can be traced and entered into the computer by the use of special pen or mouse like device which opens or closes the electrical circuit in the grid and thus identifies X-Y coordinates. Digitizers are also used in design and engineering businesses such as those that develop aircrafts or computer chips.

Though such devices give a whole new dimension to end user computing, traditional users still prefer to work with old fashioned keyboards as it speeds up the job. Nevertheless, these modern devices perform jobs in a manner that is easy as compared to the traditional techniques.

Answer: [c] Digitizer and tablet.

Question: Which of the following worms does the friendly "Cheese worm" counteract?

- [a] Adore worm
- [b] Sadmin/IIS worm
- [c] Ramen worm
- [d] 1iOn worm

Module 5 - Cheese Worm

Introduction

Malicious software can be categorised into Viruses and Worms. A Virus is a computer program that replicates itself as it moves from one file to another file within the same computer. It usually spreads through e-mails. On the other hand, Worms can transfer themselves to other computers without any human interaction. Once it gets onto a network, the worm scans various computers and attacks that particular application for which it is designed. Hence, worms spread faster than viruses.

Lion (or 1iOn) worm

It is a malicious worm written using the Linux Operating System (OS) and released onto the Internet. Machines having BIND version 8.2 are vulnerable to this worm. After making its way onto a computer, it installs the 't0rn rootkit', . Lion then creates a backdoor route using the Transmission Control Protocol (TCP) Port 10008 and waits for data to pass through the port after which the hacker can easily gain access to the computer.

Cheese Worm

Unlike other malicious worms, Cheese worm is a friendly worm and adds security to the system by closing the backdoor holes created by the Lion worm. It is a self-spreading patch that penetrates into the system via the backdoor established by 1iOn worm at port 10008. Cheese worm scans all the machines on the network and installs itself on infected machines through the TCP port 10008. The Cheese worm also stores itself in the /tmp/.cheese directory of the infected machine. This directory acts as a working directory for the cheese worm and different commands can be executed from here. The "cheese" script can do the following:

- Change the process name to httpd.
- Removes the "go" script.
- Interpret /etc/inetd.conf and write once again, excluding all the text containing /bin/sh;
- Check for the Anti-Defamation League (ADL) file. If it exists then "cheese" exits, else the file is created along with the ADL string. Then the timestamp is included to match the timestamp of system's /bin/lis file.

Pros and cons

It is not possible to protect every PC from being attacked, however, the Internet can be made resistant to malicious attacks. The Cheese worms play a very important role in achieving this. Also most PC users do not update their anti-virus packages regularly. This makes the system vulnerable to attacks.

Cheese worms clean up the Internet after an virus/worm outbreak.

The Cheese worm has a few limitations:

- Inetd and xinetd (a secure version of inetd) are daemon Internet services. Both support a different type of file configuration. So each configuration requires a different worm.
- The Cheese worm scans all the machines on a network. This increases the amount of traffic on the network, thus slowing down data transfer rates.
- The above problem also affects Ethernet networks. Ethernet networks work on Carrier Sensing Multiple Access/Collision Detection (CSMA/CD) i.e. any computer over network will not transfer data if any other machine is communicating at that same instant. The machine has to wait until the other machine has completed the data transfer.

Answer: [d] 1iOn worm

Question: On-Line Analytical Processing (OLAP) is a much better solution than data warehousing as OLAP supports:

- [a] On-line access
- [b] Decision making
- [c] Relational databases
- [d] Large amounts of data storage

Module 5 - On-Line Analytical Processing (OLAP)

Introduction

In the last decade, corporate have sought to migrate to relational databases because of their efficiency in operations and control, especially in transaction processing. In such a scenario, relational database vendors sold their software as a tool to build a data warehouse.

The Online Analytical Processing system is an alternative to Data Warehousing. The difference between these two technologies lies in the fact that data warehouses are supported by relational technology while OLAP makes use of multidimensional views in aggregating data. This allows managers and analysts to know the intricacies of corporate information through a fast, consistent and interactive access. OLAP also provides different views for the information since it has the capability to fetch detailed and effective information. OLAP therefore assists managers in decision making and predicting future activities.

Data Warehousing and OLAP complement each other. While a Data Warehouse stores and controls data, OLAP converts the data into strategic and useful information.

Application of OLAP

OLAP applications are prominent in diverse areas like:

- **Finance:** Used for capital budgeting, financial performance analysis (balance sheet and profit & loss account), and financial modelling.
- **Sales and distribution:** Used for sales analysis and forecasting.
- **Marketing:** Used for market research, promotional and customer analysis.
- **Manufacturing:** Used for production planning, defect analysis etc.

OLAP is able to assist in all the above fields because of its capability to provide whatever information is needed.

Features of OLAP

1. **Multidimensional views for data:** It is a representative of the business model since most of the business models are three-dimensional. A multidimensional view of the data provides the bases for analytical processing through flexible access to the data. The OLAP software system must have a consistent response time, irrespective of the complexity of the query.
2. **Complex calculations:** The performance of OLAP is largely measured by its ability to perform complex calculations. Simultaneously OLAP should be capable of analysing the results from its calculations. Algebraic equations are equated for calculations. For example, a sales forecast requires trend algorithms like 'percentage growth' and 'moving average'. OLAP must provide non-procedural methods for computation. This will provide

flexibility in any system thus saves time.

3. **Time Intelligence:** Time is a crucial part of any analytical application. Since business performance is always analysed for a definite time frame (current year Vs last year etc.), the OLAP system should identify the sequential nature of time. Queries like year-to-year and month-to-month or one period over other period should be easily defined by OLAP system. Other concepts like 'balance of payments' should also be taken into account by OLAP.

Benefits of OLAP

1. The flexibility of OLAP has made the user more self-sufficient. This increases the productivity of the business process.
2. Reduction in response time and more control over strategic information has increased the effectiveness of the decision-making process.
3. By using software that is especially designed for OLAP, developers can deliver applications to the user at much faster rate.
4. The above feature has helped reduce network traffic on a network system or data warehouse.
5. A more efficient use of human resources allows the organisation to respond quickly to the market demand, thus improving the revenue and profits of the company.

Answer: [b] Decision making

Module:5

Reference No:M5071

Question: For secure exchange of data, database has to ensure ACID properties. A property of database that avoids conflict between two or more transactions running simultaneously is: -

- [a] Atomicity
- [b] Consistency
- [c] Integrity
- [d] Durability

Module 5 - ACID Properties

Introduction

ACID properties play a very important role in database, applicable to both Object Database Management System (ODBMS) and Relational Database Management System (RDBMS). These properties ensure data integrity and safe sharing of data. The acronym stands for:

- Atomicity
- Consistency
- Integrity
- Durability

Atomicity

Atomicity ensures that either all or none of the operations in a transaction are reflected in a database. It means that a fragment of the operation cannot be placed in a database. The database system keeps track of old values of any data on which a transaction performs a write operation and if the transaction does not complete its execution, the old value is restored as if the transaction never occurred. Atomicity should be maintained in a database even in presence of:

- Deadlocks
- Database software failure
- Application software failure
- CPU failure
- Disk failure

Transaction-management component of database ensures the atomicity of data in a transaction.

Consistency

It involves execution of transaction in isolation i.e. with no other transaction executing concurrently (simultaneously). This will preserve the consistency of database. For example, if 'X' amount is transferred from account A to account B then the sum of account A and B should be same before and after the transactions.

Isolation

The need for isolation comes when there are concurrent transactions i.e. more than one transactions taking place simultaneously. Isolation is the safety measure used by database management system (DBMS) in order to prevent conflict between the two transactions. During such situations, the database makes use of serialisability. Transactions are serialisable; when there is no adverse effect on the database, either the transactions are executed in serial or interleaved manner. Serialisability does not imply that, the first transaction to execute will be the one that gets terminated before the other transaction starts. Degree of isolation indicates how one transaction responds to the other. There are four levels of degree:

- Degree 0:** A transaction running currently will not overwrite the data updated by some other transaction ("dirty data").
- Degree 1:** It includes features of degree 0; in addition a transaction will not commit any data until it completes all its writes till the end of transaction.
- Degree 2:** It includes features of degree 1 plus a transaction does not read "dirty data" from another transactions.
- Degree 3:** It inherits properties from degree 2 and other transactions do not overwrite the data, before the transaction is complete.

Concurrency-control component of database ensures isolation process in a transaction

Durability

Maintaining an update in the committed transaction is very important in a database. Once the execution of transaction is successfully completed, it must be ensured that any failure will not result loss or change of data. Durability guarantees the existence of all updates even after the completion of transaction. . The most striking property of a durable database is that it recovers the elements (after every recent successful commit) even if:

- database software fails
- application software fails
- CPU fails

- data disk fails

Ensuring durability is a responsibility of database and recovery-management component of database does that.

Answer: [c] Integrity

Module:5

Reference No:M5072

Question: Which of these devices can be used to evade the firewall?

- [a] Routers
- [b] Modems
- [c] Switches
- [d] CPU

Module 5 - Security Threats

Securing information is crucial for any business i.e. protecting the system against unauthorised entry. Attackers or hackers try to destroy or capture confidential information by using various tools, techniques and methods. Threats to security can be categorised as:

1. Natural disasters
2. Human threats

Natural disasters: Natural calamities like earthquakes, floods, lightning, and fire can disrupt computer terminals and the information stored in it. The best way to cope with such exigencies is to have contingency plans at the respective places where the systems are installed and backup storages exist. Other threats like riots, wars, and terrorist attack are also taken into account.

Human threats: Malicious threats to the system may be due to internal (employees) or external factors (by outsiders). Internal attacks are more dangerous because employees are the ones who are most acquainted with the intricacies of the system and its applications. Malicious attackers have specific goals and targets for attack and they do this by cracking passwords, exploiting known security weaknesses, network spoofing and social engineering. Non-malicious threats are often caused due to untrained employees with low technical proficiency in security, operating the system.

Methods, tools and techniques used for attack

A hacker can gain access to the system in the following ways:

1. **Viruses, Trojan horses and worms:** These are harmful codes spread via e-mails, and disks. They can destroy files, and can even clear the hard disk.
2. **Cracking the password:** The hacker can access the system through another user account. Users often choose easy passwords, which can be guessed based on facts about the user.
3. **Denial of service attack:** These are the most common form of attack as the Net is easily accessible and hackers can continuously communicate with the web server to keep it busy and to over load it.

4. **Impersonation:** As e-mail addresses can easily be altered are therefore cannot be trusted i.e. the sender can change its e-mail address.. Some hackers directly connect to SMTP (Simple Mail Transfer Protocol) port to access e-mails
5. **Eavesdropping:** The header and contents of an e-mail can be sent without encrypting. This can result in hackers altering the message over the network by modifying the header.
6. **Packet replay:** This refers to copying and retransmission of packets (data) when they are sent over the network. Packet replay is often undetectable, but can be traced by Packet Time Stamping (PTS) and Packet Sequence Counting (PSC)
7. **Social engineering:** It is stealing information by cracking password. The attack may be internal or external.

Security vulnerabilities

These are pitfalls or loopholes in security through which the hacker can attack to achieve his goal. Some of the loopholes are:

- **Password:** Users often employ passwords that are easy to guess, such as date of birth, sun sign and the like. Hackers can easily guess such passwords by gaining researching the victim's personal life.
- **Telnet protocols:** Telnet client is used to connect UNIX systems to Microsoft or vice versa. At such times, the user name and password are explicitly visible in the text format.
- **Device administration:** Passwords are associated with switches and routers that are controlled by HTTP interface or command line interface. A hacker can take control of these devices and find the password.
- **Modems:** Modems are standard features for many desktop computers. The drawback with these modems is that the firewall can be bypassed easily. Hackers use 'war dialer' tools to get the telephone number of the modem and 'password cracker' tools to find out user passwords, to gain access to the system.

Answer: [b] Modems

Module:5

Reference No:M5073

Question: Implementing a firewalls is not the best solution for Virtual Private Networks because:

- [a] Firewalls cannot detect spoofing attacks.
- [b] Firewalls cannot be installed on VPNs
- [c] Firewalls cannot alter data over a network
- [d] All of the above

Module 5 - Virtual Private Network (VPN)- Security

VPN

It is a connection of two or more computers or private networks. Although a VPN is quiet similar to a Wide Area Network (WAN), VPNs make use of public networks like the Internet instead of

depending solely on expensive private leased lines.

VPN security

Protecting data and preventing attacks is a critical issue in VPNs. Data can be secured through encryption and authentication. The Internet Engineering Task Force (IETF) has developed a set of IP security (IPSec) protocols for data authentication and privacy.

Firewall products, especially used for VPNs, like NetScreen, Watchguard and NetFortress are simple solutions for network security. VPN can make up of any number of LANs depending upon the need. However, these solutions are costly. Determining which solution to use depends on the specific security and networking needs of a company.

It is a widely accepted fact that firewalls are the perfect solution for Internet security.

However, in the case of VPNs, firewalls are inadequate due to following reasons:

- Firewalls cannot check changes in data that moves over network in the form of packets.
- Firewalls cannot detect spoofing attacks (the source address is changed so that it looks as if it is originating from a different location).
- Firewalls work only on certain standards. VPNs installed today are either non-standard or need more sophisticated firewalls.
- The management port of a firewall can be used by a hacker to change the configuration of a database to access the network easily.

Data security

The feasibility of a VPN depends upon the following:

1. **Information privacy:** For keeping data confidential, it should be encrypted. The International Standard Encryption Algorithm (ISEN) acts as a benchmark for selecting a suitable encryption for VPNs. The ISEN is important for:
 - o Testing
 - o Interoperability
 - o Liability with encryption
2. **Reliability of data:** When data is sent over the Internet in the form of packets, it is possible for the source address to be modified, or the data to be changed in a spoofing attack. "Packet authentication" is the technique by which data can be protected from such attacks. IETF has defined standards like Encapsulated Security payload (ESP) to protect data packets. It prevents data packets from being attacked while being transported over the Internet. More sophisticated ESP includes Message Authentication Code (MAC) that uses encryption to generate the authentication code, which prevents a hacker from altering any data in the packets.
3. **Source of data:** Once the secure transfer of data from source to destination is ensured, the identity of the sender needs to be verified (user authentication). The simplest and most commonly used method for user authentication is a password. However, passwords have very limited security. The alternative lies in "two-factor" authentication in which a concept called "the user has" and "the user knows" is applied. User tokens (smart cards, random number generator and the like) and pin numbers are associated with this.
4. **System control:** It refers to managing all aspects of security for the successful completion of the system's activities. This includes configuration management, access management, key management, internal control management, and managing firewalls. There

should also be complete control while revoking privileges from the user.

Answer: [a] Firewalls cannot detect spoofing attacks.

Question: The management must take various security measures to mitigate the risk. Which of the following measure aims to minimise the damage and prevent the reoccurrence of incident?

- [a] Reductive measure
- [b] Detective measure
- [c] Repressive measure
- [d] Corrective measure

Module 5 - Cost-effective Information Security - Part 3

Cost effective management of business processes, information, Information Technology services and hence information security is essential for a competitive edge and for survival of an organisation.

The management must take various security measures to mitigate the risks. The security measures that the management can take at each stage can be depicted with the help of a diagram.

Source: Sans Institute - Cost-effective Information Security (Information Security from a business perspective) June 6, 2001

Let us discuss each of the security measures that the management can take in detail

Preventive measures: Preventive measures are the steps taken by the management before a security incident takes place. The aim of such measures is to eliminate the risks and vulnerabilities. Examples are Configuration of operating systems, firewalls and vulnerability assessment.

Reductive measures: The purpose of these measures is to minimise the damage when the incident occurs. They are also taken before the incident occurs. Examples are regular backups and creation of contingency plans.

Detective measures: Detective measures sense the security incident before any significant damage is caused. They can also be undertaken before the incident takes place. By implementing the detective measures the corrective measures can be minimised. Example is intrusion detection systems.

Repressive measures: These should follow the detective measure, since without detection of the incident it would not be possible to take the repressive measure. The measures are taken before the occurrence of the incident but the actual execution is done after the occurrence of the incident. The aim of this measure is to minimise the damage and to prevent the reoccurrence of the incident. Example is automatic locking of user accounts after a specified number of unsuccessful log on attempts.

Corrective measures: On the basis of detective measure a decision is made whether a repressive measure or a corrective measure is to be taken. The aim of this measure is to repair the damage and restore the original status i.e. status as it existed before the damage. Example is making use

of fallback scenarios and restoring backups.

On the analysis of the above we can say that preventive measures are the most efficient, as they aim at eliminating the risks and vulnerabilities. They also reduce the need for reductive, detective, repressive and corrective measure. But the cost of the measure should be taken into consideration before they are implemented.

After knowing about the security measures one thing that comes in mind is "Do we really benefit by undertaking all the measures?" No measure comes free. It involves cost. But it should be remembered that the security incidents also involve cost, the cost of which would be higher than the cost of the measures. The management should make a choice between budgeting for security measures and absorbing the cost of security incidents as a consequence of not implementing security measures. In order to make a balanced choice, the management must have the knowledge of the need for security.

Service Level Agreements (SLA): When the company thinks of entering into service level agreement for security services, the decision pertaining to implementation of security measures must be based on the documentation prepared by the company on the security demand for Information Technology. The SLA must incorporate the security measures to be taken by the IT service organisation. The audit process helps to evaluate the efficiency and effectiveness of security services provided by the IT service organisation. The report of the audit process will provide information whether the security services that are delivered meets the actual business needs.

The interfaces between SLA and SLA based reporting when a part of the security management process is subcontracted can be explained with the help of a picture, which is as shown below

Source: Sans Institute - Cost-effective Information Security (Information Security from a business perspective) June 6, 2001

Conclusion: The benefits of security measures and the cost effectiveness can be measured based on the accurate knowledge of security needs and accurate feedback on the efficiency and effectiveness of security measures taken.

Answer: [c] Repressive measure

Module:5

Reference No:M5077

Question: For successful implementation of the preventive security it is necessary that

- [a] Preventive security should be implemented based on activities of the company
- [b] Preventive security should always remain the same
- [c] Preventive security should not be related to the cost
- [d] Preventive security need not be based on any policy

Module 5 - Preventive Security

Security concerns are of utmost importance to the company. Any compromise on it can lead to a damage, which may take several million dollars to rectify. It must be realised that there could be certain lapses while designing writing or installing the program or while configuring the system, and last when using the software. Such shortcomings may lead to the breach of security. Certain defects may prove to be a source of risk and hence it is important to pay adequate attention to the security.

Preventive Security:

Preventive security must prevent any breach of security. The techniques that are adopted for implementing the security measures must spot the breaches that were previously known or any new security breach. After identifying them, efforts must be made to put any attempted breaches on hold. Also the security designed should be such that can be easily implemented and managed.

Caution: Many times insecure practices lead to security holes. This provides an opportunity to unauthorised personnel to play havoc with the system. The preventive security should provide for automatic closure of any temporary holes that are created.

Components:

The preventive security relies on two main components viz. human and technological.

Human component: The human component can be categorised into three

1. **Authorisation:** It should be determined as to who should be allowed to use what resources and the level of usage.
2. **Policy:** The security policy should state what activities should be allowed and which denied.
3. **Management:** There should be proper mapping of policy for its effective implementation and management.

Technological component: The technological component implements different type of controls over the system. These controls can be categorised into three

1. **Authentication:** Only authorised persons are able to access the system.
2. **Behavioural control:** Once logged in the system after authorisation and authentication, the user is expected to behave/ follow specific procedures. Behavioural control establishes this. E.g. if a user tries to access some information for which he is not authorised there should be a display saying, "You are not authorised to view this information".
3. **Access control:** These controls assure that the usage of the data by the users is as per the security policy.

Successful implementation of preventive security:

The success of the implementation of security rests on the following:

1. The security policy is always current and up to date.
2. Authorisations are reviewed at regular intervals especially when people are hired, laid off and the like.
3. Behaviour and access controls are reviewed when new applications or new versions of an application are added or when any changes are made to the existing application.
4. Preventive security being implemented must be based on the activities of the company.

When the company is constantly updating its software it will be required to undertake more preventive security activity than a company which does not update its software frequently.

The demand for preventive security will increase as long as the computers, business, customers are interdependent because of the need for a secure computing platform.

Answer: [a] Preventive security should be implemented based on activities of the company

Module:5

Reference No:M5078

Question: Hackers avoid detection of attacks by changing the URL such that it is difficult to write programs to detect the attacks. This is done through:

- [a] Spoofing
- [b] Physical attacks
- [c] Smurfing
- [d] Hexadecimal encoding of URLs

Module 5 - How Hackers avoid detection - I

Hackers are not only clever in how they invade servers; they are also devious in how they disguise their attacks. Malicious attackers use a variety of evasive techniques, so administrators must be prepared to detect and respond to them.

Another article discussed some of the most common types of attacks against Web servers, and the evidence they leave in Web server logs. Some tricks hackers use to avoid detection and the evidence they leave behind are examined, which make attacks more difficult to detect. The attacks are examined with respect to the two most popular Web Servers, Internet Information Server (IIS) from Microsoft and Apache.

Hexadecimal Encoding

One of the easiest ways to disguise attacks is through changing the URL request. Administrators generally search our log files looking for certain strings, or collections of plaintext characters. Resource requests are parsed for strings that match known vulnerabilities. For example, when the following pattern is found in a log for IIS, it is clear that someone is looking for the MDAC remote vulnerability in IIS:

```
GET /msadc/ 302
```

To see how attackers attempt to circumvent pattern matching, the request from the malicious attacker's perspective is examined. To determine whether or not the msadc directory exists, an attacker might type the following:

```
GET /msadc HTTP/1.0
```

This would yield the log file as above. The attacker can change the request by encoding it as hexadecimal ASCII characters. In the above example, the string msadc would become 6D 73 61

64 63 using hexadecimal ASCII encoding. The Windows Charmap program can be used to do a quick ASCII-to-hex encoding of characters. The above HTTP request, rewritten with the string msadc encoded in hexadecimal, appears as follows:

```
GET /%6D%73%61%64%63 HTTP/1.0
```

The log file for IIS shows:

```
07:10:39 10.0.2.31 GET /msadc/ 302
```

Note that this is exactly the same log that is created when the URL is not encoded in hexadecimal. So in this case, encoding did not help the attacker. However, a look at the Apache logs for a similar attack tells a different story. The command an attacker would use to check for the existence of a particular CGI script is listed below, followed by the same command with hexadecimal encoding:

```
HEAD /cgi-bin/test-cgi HTTP/1.0
```

```
HEAD /%63%67%69-bin/test-%63%67%69 HTTP/1.0
```

Now let's take a look at the access_log file:

```
"HEAD /cgi-bin/test-cgi HTTP/1.0" 200 0
```

```
"HEAD /%63%67%69-bin/test-%63%67%69 HTTP/1.0" 200 0
```

Note that in both cases the 200 status code tells us that the command completed successfully. However, in the second case, the hex values rather than the plaintext values appear. If the detection were relying on pattern matching to detect this attack, it would likely fail. Many intrusion detection systems also use unintelligent pattern-matching capability, and some do not convert the hex-encoded URLs in order to perform the pattern matching. All administrators should be aware of this well-known trick, and of whether their intrusion detection software is smart enough to convert hexadecimal code.

Modern web-servers, however, will attempt to clean up input before executing a request. For example, when presented with a request that looks like "a/b/../index.html", the web-server will convert it to the proper "a/index.html" before executing the request. Removing the "../" parts of the URL are an important security measure. Most attacks against web-servers involve adding too many "../.." components to the filename, breaking out of the disk reserved for the web-server, allowing the intruder to read or execute other files.

Answer: [d] Hexadecimal encoding of URLs

Module:5

Reference No:M5079

Question: Hackers cover their tracks by masking their IP address. This is done through:

- [a] Proxy chaining
- [b] Denial of Service
- [c] Secure Sockets Layer hacking

[d] IP spoofing

Module 5 - How Hackers avoid detection - II

Proxy Servers

While concealing an attack may be crucial to an attacker, obfuscating the source of the attack is just as important. If a malicious attacker can spoof the source IP address, he can hack without worrying about legal problems. One way for attackers to mask their source address is through the use of proxy servers.

Proxies are used to send requests to other computers through a single access point. In corporate LANs, users go through a proxy server to access the Internet, giving network administrators the control over the filtering rules for inbound and outbound access. A user connects to the proxy server, which then forwards the connection request to the intended destination. The destination server records the address of the proxy server as the source address of the connection, rather than recording the address of the system that originated the request.

Unfortunately, proxy servers are sometimes inadvertently placed on the Internet. These servers are sometimes misconfigured so that any Internet user can connect to the proxy server. When an Internet user connects to a server via the proxy, the proxy's source address, rather than the address of the Internet user, is recorded in the server logs. A malicious attacker may appear in a victim server's log files with a source address belonging to an "innocent" proxy rather than with the attacker's actual address.

In the attack/log file combo below, we see the attacker request information, and we see the request appear in the log file:

Attacker with IP address 202.13.1.57 gives the following request:
HEAD / HTTP/1.0

Log file
202.13.1.57 - - [18/Oct/2000:03:31:58 -0700] "HEAD / HTTP/1.0" 200 0

In the following attack/log file combination, we see the attacker achieve the same goal, except that the attacker uses a proxy server.

Attacker uses proxy 216.234.161.83 80
HEAD http://10.8.8.8/ HTTP/1.0

Log file
216.234.161.83 - - [18/Oct/2000:03:39:29 -0700] "HEAD / HTTP/1.1" 200 0

Note that in this example, the source address that appears in the Web server log file is that of the proxy server (216.234.161.83, proxy.proxyspace.com), not the attacker (202.13.1.57). In this case, the attacker has successfully hidden the IP address of the source of the attack from the victim. The network administrator can track down the ultimate source of the attack if the administrator of the proxy server cooperates. Most proxy servers keep very detailed logs, so the source address of the attacker should appear in the log files of the proxy server. Unfortunately, attackers can "chain" proxy servers so that the attack is propagated through multiple proxy servers. In order to determine the source address of the attacker, administrators or law enforcement officers need the cooperation of the administrators of every intermediate proxy

server, sequentially. The process of chaining proxy servers is well known in the hacker community, and an automated software tool that performs this process is SocksChain for Windows. With the Internet becoming more widespread, hackers are chaining proxy servers across countries, most of which do not have any laws about computer security.

SSL

It should be carefully noted SSL-enabled servers are not monitored by network intrusion detection systems. If given a choice, most attackers would prefer port 443 (HTTPS- Secure HTTP) over port 80 (HTTP). This is not really a dirty trick, just a side effect of using encrypted communications. However, an administrator can use the Web server log files to monitor requests to port 443.

Techniques such as hexadecimal encoding are not only used for deceptive log file entries; they can also deceive a Web server's URL parsing mechanism, which may lead to vulnerabilities such as source code disclosure. Attackers sometimes use multiple proxy servers for scanning and attacking, making it very difficult for administrators to trace the real source of attacks. And of course, SSL sometimes paves the way for "secure hacking."

Answer: [a] Proxy chaining

Module:5

Reference No:M5080

Question: Which of the following is an advantage of Hardware-based Keystroke logging over Surveillance cameras for observing data input?

- [a] Physical access to the equipment
- [b] Electrical interference does not affect the functioning
- [c] Technical skill is not required
- [d] Independent of the Operating System

Module 5 - Keystroke Logging

Keystroke logging is collecting of valuable key information for use in later attacks or information gathering exercises. Keystroke logging, through the data it captures, can also remove the restriction to use a brute force attack against encrypted information, as pass phrases are typed and then recorded by the logger in the clear. Keystroke logging has been around since the days of the first mini-computer systems and it is still effective today as a first step data capture utility.

Key Stroke Logging Techniques and Devices

A simple technical technique to observe keyboards and monitors is the careful placement of a camera or cameras. One or more cameras can be used to monitor and record all keys entered and played back slowly so that correct key sequences can be captured. If such recording is done multiple times, it can increase the level of detail and thereby accuracy. The display monitor and the keyboard can be placed under the camera so that the application that the captured data is pertinent to also can be recorded.

This method has the following disadvantages:

- Physical access to the building must be obtained for placement of the cameras
- Replacement of the storage media
- If transmitter based cameras are used, electrical interference may interfere with the signal degrading the quality
- Discovery of the camera(s) may alert the target

The advantages are:

- Independent of any Operating System or application
- Much technical skill is not required
- Can be used as legal evidence, if a proper warrant has been issued
- Easily defeats encryption systems as the login information is captured in the clear
- Links keystroke data to application if monitor is being captured as well

Hardware-based Keystroke Logging

With advances in encryption and easily available free encryption products it is getting harder for law enforcement and other authorised groups to access criminal data. One way to by-pass the requirement to undertake a brute force attack, to decrypt the targeted data, is to capture the keystrokes that make up the login information.

Hardware keystroke loggers are attached between the keyboard port of the motherboard and the keyboard itself. Hardware loggers can work in two ways: the first is effectively eavesdropping, where the signal sent from the keyboard it is detected and recorded. The second is store and forward where the signal is received recorded and then forwarded to the motherboard.

The delay introduced by both methods is so small as to be undetectable. Only careful observation of the keyboard cable may discover the hardware device, but the devices are made such that they are easily overlooked. The hardware device can either store the information on board or transmit it via wireless technology to a receiving station. A number of hardware keystroke capture and recording devices are also now commercially available.

The advantages of hardware capture devices are:

- No accounts are required for installation
- No change to the operating system or use of any system resources and therefore undetectable by anti-virus and other security vulnerability/scanning software
- No technical skill required and can be installed by anyone with a little training
- All key strokes captured and recorded
- This method will capture even the BIOS passwords before boot up
- No effect of any software upgrades or changes
- It is independent of the Operating system being used.

The disadvantages are:

- Limited storage, if onboard memory used
- Access to the PC required for installation and data collection.

Answer: [b] Electrical interference does not affect the functioning

Question: Which of the following is **NOT** a feature of Software Keystroke loggers?

- [a] They are difficult to detect
- [b] No physical device is needed to be installed
- [c] They can transmit the keystrokes externally via the network
- [d] They cannot record BIOS passwords

Module 5 - Keystroke Logging

Keystroke logging is collecting of valuable key information for use in later attacks or information gathering exercises. Keystroke loggers can be of two types: hardware-based and software-based. The former have been covered in Part I and the second is covered here.

Software-based Keystroke Capture

Most software keystroke loggers these days are targeted at PC users, and these have some limitations. The software keystroke logger has to be installed on the target system by a user who has create and modify permissions. Unfortunately for the DOS based operating systems, this is everyone but with newer operating systems such as Windows NT and Linux, users can be restricted in their permissions.

While well-written software keystroke loggers will install without producing any errors, poorly written programs may cause memory conflicts that may not even give the user a clue what is wrong.

Software keystroke loggers store the captured data in various ways:

- By writing the data to a log file which seems similar to a valid systems file
- By emailing the key strokes to a pre-configured recipient
- By putting the keystrokes into valid data packets, which are then transmitted to the malicious user

Advantages of software keystroke loggers are:

- Difficult to detect
- No physical device is needed to be installed
- Can transmit the keystrokes externally via the network
- Can be installed and used remotely

Disadvantages of software keystroke loggers are:

- Anti-virus programs or specialist keystroke logger detection programs can detect most well known programs
- They have to be installed by a user with create and modify permissions
- They cannot capture BIOS passwords
- Special technical skills maybe required for its deployment

- They are Operating system dependent
- The captured data by network maybe blocked by the firewall, when being transmitted to the attacker

Hackers frequently employ programs that on the surface appear to be a helpful utility, but which, in reality, are designed to secretly inflict damage. Some actually attempt to open up holes in network security systems. Such programs are called Trojan Horses - a reference to the wooden Horse used by the Greeks to defeat the city of Troy.

Keystroke loggers once again are becoming an essential tool for capturing primary data to allow access to the full data store. There are a large number of software key loggers available and also a small number of hardware key loggers. However, most of the major anti-virus packages will detect the majority of Trojan keystroke loggers. Further, there are specialty key logger detection packages available but unfortunately the only way to detect hardware key loggers is observation.

As a first step data capture technique, key logging is still one of the best methods for capturing user ids, passwords and pass phrases.

Answer: [d] They cannot record BIOS passwords

Module:5

Reference No:M5083

Question: Which one of the following statement is not true with regard to physical security?

- [a] Examining the age of the cabling is not significant
- [b] Lack of proper cooling facility may cause hardware failure
- [c] Locked gates, entrances, parking places are properly lit
- [d] Employees have to undergo training in physical security

Module 5 - Audit of Physical Security

A physical security audit assesses the operating environment, staff, server locations, network wiring and equipment to ensure that they are protected from external threats. Auditors have to consider the following aspects to evaluate different types of risks, and check if:

Unauthorised access to facility:

1. Employees have undergone a training programme to protect physical infrastructure, in case of a fire, a bomb threat or the like.
2. The ownership of the facilities is vested with more than one person. In such a case, security procedures undertaken by each of them should be clearly written, documented and followed.
3. The mode of access to the facility like keys, codes and cards has been authorised, and is regularly changed to avoid unauthorised access.
4. Adequate protection has been provided in case a facility is located in an area with a high crime rate.
5. Proper lighting has been provided at the gates, parking lots and entrances. Ensure that normal streetlights and floodlights (sodium vapour) are also used outside the premises to

prevent internal visibility.

Cables and wiring:

1. The cabling has been replaced periodically to prevent leakage of power.
2. The stock of cable is kept safely with authorised persons.
3. The map that reveals how the cabling is done is accessible only to repair personnel.
4. The external cabling is protected from weather conditions.
5. Cables are put in construction free areas.

Power supply:

1. Measures are in place to ensure uninterrupted power supply.
2. Safety measures are written, documented and communicated to everybody.
3. Power lines pass through low traffic areas.

Hardware failure

1. Backup cooling sources have been made available, for this is a major cause of hardware failure.
2. Temperature and ventilation for hardware to function effectively conform to standards.

Unauthorised access to programming areas, control room, storage areas and communication closets

1. Access logs are kept to record persons entering sensitive areas.
2. Entry to programming rooms has been restricted to only authorised persons.
3. Only authorised programmers have access to the computers that are used for programming.
4. Controls are in place for guests who access the programming rooms.
5. Proper measures have been taken to prevent piggybacking.

Sensitive documents: All date sensitive documents have been properly disposed off. Confidential documents should be classified, marked and stored safely. The procedures adopted for mailing confidential documents also have to be checked.

Telephone resources: Proper control is exercised over the utilisation of telephone resources.

Portable devices: Physical security of the portable devices is tested, and a proper control exists on ordering, issuing and inventories.

Common risks: An appropriate policy exists to monitor, detect and protect the hardware against common environmental risks.

PC protection: PCs are protected against information loss/thefts, and authorised persons monitor the maintenance.

Access to physical areas of operations: Only authorised persons are allowed to access restricted areas. Security measures are constantly examined and reviewed.

Answer: [a] Examining the age of the cabling is not significant

Question: Kerberos is a user authentication mechanism. Which of the following methods does it not use, to establish a secure connection between the client and the target server?

- [a] Tickets
- [b] Secret key
- [c] Password
- [d] Encryption

Module 5 - Kerberos

Introduction

Programs like telnet or rlogin are commonly used to connect one computer to remote computer over a network. The identity of the user is authenticated automatically with the help of passwords or a '.rhost' file. Both the methods are vulnerable to 'eavesdropping' (intrusion or access to unauthorised party). In case of login, when the user types the password, the number of characters in the password are transmitted over the network, which makes it easy for a third party to interpret and decipher it. On the other hand, authentication through an .rhost file relies on the IP (Internet Protocol) layer, which is vulnerable to attacks such as "IP spoofing". In order to prevent such problems, a popular authentication mechanism known as kerberos is used.

Kerberos

It is a user authentication mechanism, which makes use of "tickets", secret keys or cryptography to sustain a secure communication channel between the client and the server. Once the connection is established with the help of kerberos, all the data communicated between client and server remains encrypted. Kerberos also replace many UNIX network utilities like telnet, ftp, rlogin, rsh, etc.

Implementation of kerberos depends on Key Distribution Center (KDC). It consists of two logical parts- an Authentication Server (AS) and a Ticket-Granting Server (TGS). Although, these two are logically different functions, they can reside in a single physical server.

Characteristics of kerberos

1. Authentication

Kerberos authenticates the user's identity but does not reveal anything about what the user does after logging in.

2. Secure

- Passwords are not transmitted over the network except when they are changed.
- Kerberos provides enables two-way cryptographic authentication i.e. it allows both the server and client to identify each other.
- Kerberos is so designed that every client trusts a particular central server.

3. Single Sign-On

This feature will enables users to type the password only once in a day. It is done by getting 'ticket granting ticket' (TGT). The life of TGT can be configured but usually it is one day. The function of TGT is to get tickets that authenticate the user's identity to

the application server.

How kerberos works

Kerberos authenticates user identities in four steps:

- **Step 1**
Authentication exchange: In this method the client requests the Authentication Server (AS) for a ticket. The AS enquires about the client from its database and then creates a session key (SK1) for use between Ticket-Granting Server (TGS) and the client. Now, kerberos encrypts SK1 by making use of the client's secret key. The AS also uses a secret key for TGS, known only to AS and TGS. These are used to generate "ticket-granting ticket (TGT)", which is send to user.
- **Step 2**
Ticket granting service exchange: The client now decrypts the message and uses it for generating an authenticator that contains the user name, IP address and time stamp. He then transmits this authenticator along with TGT, to TGS. The TGS decrypts TGT and then uses SK1 inside the TGT in order to decrypt the authenticator. TGS after verifying the information in the authenticator allows the request to be processed. Then a new session key (SK2) is generated by TGS for the client and the server. Kerberos encrypts it using SK1 and transmits it to the client. TGS also sends a ticket with the client's name, network address and a time stamp. All these are encrypted with the help of the target server's secret key.
- **Step 3**
Client/Server exchange: The client computer decrypts the message and obtains the SK2. He generates the new authenticator, which is encrypted with SK2. The client now sends this along with the session ticket to the server. The target server decrypts the ticket and checks the time stamp, authenticator and client address.
- **Step 4**
Secure communication: The server now knows the identity of the client and both of them can now share the encryption key to avoid any vulnerability in the communication. Since both client and server share this key, it is obvious that the message, encrypted with this key, originates from a secure party.

Answer: [c] Password

Module:5

Reference No:M5086

Question: Which of the following checks is set up in an application to avoid transposition errors in the input?

- [a] Range checks
- [b] Limit checks
- [c] Check digit
- [d] Size checks

Module 5 - Data Input Checks

Control of data input is the first step in ensuring the integrity of the data available from the information system. Data input controls consists of three basic activities.

1. Controlling the access to the system i.e. a mechanism to restrict unauthorised access to the system.
2. Data edit checks to ensure that data entered is accurate.
3. Audit trails to ensure that control mechanism is existing and functioning completely.

This section deals with the data edit checks in particular.

Data edit checks are control mechanisms, which ensure that only correct and complete transactions are processed. These are basically software-based controls. These include 2 categories:

- A. **Data validation techniques:** These techniques ensure that data entered into the system are reasonable (not necessarily accurate). For example setting the field length, type, input masking and the like.
- B. **Data verification techniques:** These techniques ensure that data entered into the system are accurate. For example check digits, control totals, hash totals and the like.

A. Data validation techniques

Some of the common data validation techniques are

Size checks: This check limits the size of the word or the data to be entered. For instance if the invoice numbers are of four digits, then the application is set to reject all those entries which have more than 4 digits. The same thing applies to alphabetical entries.

Limit checks: These are used for numerical fields. A minimum or a maximum limit is set wherein the system refuses to accept all the entries beyond the limit. They are useful wherein the entry involves; say for instance amounts in banks and financial institution.

Range Checks: These checks are similar to the limit checks. But here instead of setting limits, a range is set. For instance in a field which contains the invoice numbers a range may be set for each period to ensure that a correct invoice number is entered.

Format Checks: Here the fields are set to receive only particular characters of entry. For instance a field may accept only numerical characters or may accept alphabetical characters. . These are also called character checks.

Check digits: A calculated numerical value is added to the numbers entered to ensure that the original data is not altered. This is useful in identifying transposition or transcription errors. For instance, a unique number is added to the cheque number that is entered to ensure the correctness of the number entered.

Existence of data: The data that is entered here is cross-checked with an already existing data or criteria. For instance employee numbers, invoice numbers entered are cross-verified with already existing lists of invoice numbers.

Arithmetical accuracy and tolerance levels: Here the numeric values in a field are retotaled or

recalculated for arithmetical accuracy.

Date-driven Edits: Here the date fields are used for validation. The common date driven validation are range checks.

(B) Data verification techniques

Some of the common techniques to ensure data accuracy are automated inputs likes bar codes, scanning and the like. These reduce the transcription errors. Batch input and processing is used so that batch control totals can be used to verify the accuracy of the data.

Answer: [c] Check digit

Module:5

Reference No:M5087

Question: The first step in any security administration is

- [a] Implement good access control mechanisms.
- [b] Develop a good security policy for the organisation.
- [c] Ensure that each user has a separate login.
- [d] Ensure that good backup procedures have been set up.

Module 5 - Security administration - Part 1

Security administration involves ensuring three basic requirements of an organisation. The three requirements are:

- **Information Confidentiality:** This indicates that only authorised individuals have access to the data.
- **Information Reliability:** This implies that, the data available to the users are accurate and can be relied upon for decision making
- **Information Accessibility:** This requirement indicates that data is available to the users when required.

This is the first of a two part series on the rules that constitutes an efficient security administration. In this article we discuss the first four rules of system administration. The subsequent article contains the last five rules.

Rule 1: Security must be an authoritative mandate in the organisation

Voluntary measures for security compliance cannot be relied upon. Security of information systems must be given adequate authority for a proper enforcement of the same. The management must get actively involved in the development of a comprehensive security policy. Thereafter, security measures must be implemented as per the security policy.

Rule 2: Security measures adopted need to be convenient also

Security measures should not lose sight of the basic objective of the computer systems, that is, to assist the company in its operations. Security measures must be complimentary to this basic objective and a balance is to be maintained between the two. The measures should not be so stringent that it hampers the basic activities. Also they must be convenient enough for the users to adopt. It is a good policy to inform the users the reason behind a measure before implementing it.

Rule 3: Any programme or software loopholes, bugs, vulnerabilities must be fixed at the earliest.

Weak links should be identified and should be taken care of immediately. Despite the network being well secured, the software could have a bug in it. Such vulnerabilities are always susceptible to exploitation. Hence it is always prudent to fix a bug as soon as it is detected. Many programming tools are available in the market, which can detect the bugs and can also rectify it.

Rule 4: Every computer must be secure first to install further security fixes/checks.

Although rule 3 indicates that vulnerabilities have to be fixed immediately, it doesn't help much if the system is not secured in the first place. For instance if the system does not have some basic security measures like password protection, user based logins cannot be implemented in the computer systems. Hence, this aspect needs to be looked into first before leaping into bug detection and rectification procedures.

Article 1	Laws on security administration part 1
Article 2	Laws on security administration part 2

Answer: [b] Develop a good security policy for the organisation.

Module:5

Reference No:M5088

Question: Which of the following is a guard against unauthorised access to the computer systems?

- [a] Having a trustworthy system administrator
- [b] Having a sound encryption policy
- [c] Having a good password policy
- [d] All of the above

Module 5 - Ten Commandments Of Computer Security - Part 2

This is the second and concluding part of the series on essential rules of good computer security design. In the first article we discussed the first four rules in detail. In this article we discuss the remaining six rules.

Rule 5 Have a strong password policy

A strong password policy is necessary to prevent unauthorised access to the computer system in the organisations. Not only should passwords be mandatory, they must be complex too. Preferably it should be alphanumerical with commas and full stops in between. Passwords should also be considerably lengthy to make it more complicated. Also the password chosen should be handled and stored suitably to prevent misuse of the same. Smart cards, biometric products like fingerprints, retina scanners can also be used to prevent unauthorised access.

Rule 6 Have a trustworthy system administrator

System administrator is a person who has complete control over the system. Hence the organisation should always follow a rigorous policy while hiring network administrators. The credentials must be checked thoroughly. The background check should also be conducted at regular intervals during the tenure of the administrator. Diversification of the task policy should be followed. Finally audit trails should be established for all the actions undertaken by the administrator. The audit trails could be made 'write only' and such other mechanisms to make it fool proof.

Rule 7 Have a strong, well-protected, well-stored decryption key

Any encryption based security mechanism is as strong as its decryption key. Storage of the decryption is very important. Always try and use offline storage for keys. If possible memorise it. Otherwise store it in a floppy disk.

Rule 8 Update the virus scanner regularly

Remain alert for virus threat. All viruses create extensive damage when they are new and when not much is known about it. So keep the virus signature file updated for any new virus. And also keep updating the virus scanner for any new techniques that the developer has created.

Rule 9 Ensure a well-behaved net surfing to protect privacy on net.

Although complete anonymity is not possible, privacy of data can be maintained while surfing the web sites. Read the privacy policies on website before using it. Use only certain websites from public domain. Use different ISPs. Disable cookies before using websites but most importantly avoid arbitrary and haphazard netsurfing.

There are a lot of techniques available for maintaining anonymity, network address translation to mask the IP address being one.

Rule 10 Understand that security consists of both technology and policy and needs to be upgraded regularly.

Last but not the least, it should be understood that a perfect security plan is not possible. But using the latest technology efficiently can provide security to an extent. But more importantly, a good security policy requires a high degree of awareness and exercise of sound judgement. Lots

of resources are available to help the same.

Article 1	Ten commandment of computer security Part1
Article 2	Ten commandment of computer security Part 2

Answer: [c] Having a good password policy

Module:5

Reference No:M5089

Question: One of the methods to prevent malicious programmes creeping into the computer systems is

- [a] Authentication of programmes by quality assurance team
- [b] Ensure that programmes are from trustworthy source
- [c] Ensure that programmes are thoroughly tested before use
- [d] All of the above

Module 5 - Ten Commandments Of Computer Security - Part 1

Introduction

The term computer security is a generalised term corresponding to various tools and techniques used to secure the data on the computer. In this electronic age where most of the data originates and is modified, transferred, transmitted and stored electronically, protection of data assumes paramount significance. Given below are the list of ten essential rules that any organisation needs to consider while designing and maintaining its computer security. This topic has been dealt in 2 parts. The first part discusses the first four rules. The next six rules have been dealt in the subsequent article.

The rules have been discussed below in detail

Rule 1 Never use a program from an untrusted source.

Today, computer programmes are capable of creating havoc on any computer system. There are a variety of programmes available which can practically do anything and everything to a computer system. They could overwrite the entire contents of the database, disable the hard disks, erase the entire data on the system, and stealthily monitor confidential data that is being generated regularly. Hence it is always advisable to run or download a program from a trust worthy source. This ensures that the data is relatively safe from such threats.

Rule 2 Make sure that system files like operating system documents are well protected.

Operating system files are the most trustworthy files in a computer system. They are designed to maintain the entire computer network of an organisation. Hence segregation of duties is very important so that the users of the system do not have access to system files. This ensures that no unauthorised alteration or modification takes place to the system files. In particular since the operating system controls the security measures of the system like password protection, control of users and the like, the access rights and the privileges normally should not be given to the users.

Rule 3 Have good physical access controls to your computer system.

It is always important to ensure that the computer is physically protected from any unauthorised access. It should be ensured that the organisation has a good physical access control mechanism that is consistent with the value of data held by the computer. Some of the common physical access control mechanisms include keeping the servers domain controllers in a separate room to which only a few authorised personnel have access. The individual computers can be similarly controlled. It is also necessary to ensure physical security of mobile products like laptops and notebooks.

Rule 4 Never allow unauthorised uploading of software into the company's website

If the organisation runs a website, the company should take adequate preventive measures to ensure that unauthorised programmes are not being uploaded onto the website. This task is all the more daunting when the website is hosted on a shared server. Any abuse in the site can endanger the server itself, on which the site is hosted. If so all the other website that are hosted on the website are also prone to danger. Hence it is always good to know the server administration policies before hosting a website on a shared server. And also adequate preventive measures are necessary before it is open to the public.

Article 1	Ten commandment of computer security Part1
Article 2	Ten commandment of computer security Part 2

Answer: [b] Ensure that programmes are thoroughly tested before use

Question: In entity-based system architecture, the end system implies which one of the following?

- [a] The workstation and operating system
- [b] The Internet
- [c] The administrative authority
- [d] The network topology

Module 5 - Security architecture entities part 3

In one of our earlier article we had dealt with the concept of Security Architecture Entities. We had discussed that in order to frame a good security design we need to break down the entire network of systems into separate entities. We had indicated five basic entities that comprise the system.

In this article we will briefly describe the security issues pertaining to each entity

End system entity: this is the basic entity of a network. End system entity refers to a computer with an operating system. The computer could be either a workstation or a server. Even in the server category there may be different servers like application servers, controllers etc.

The primary objective is to protect permanent data and other services that are related to the operating system.

In order to design a security mechanism, computers need to be classified based on their operations, sensitivity of the operations, data they hold etc. Based on this classification, computers can be given a security ranking.

Classification of each computer into different levels is done in order to identify systems with high risks and weak points, those that are more prone to threats and attacks. For instance, servers are generally perceived to fall under the high-risk category because of their value. However, a workstation can also be classified as high risk based on the type of operations it can undertake. For e.g. people can download and work offline, and this may damage the system. Also workstations being the links to the servers, a weak access mechanism can put the entire network in jeopardy.

The items in the end system entity that are analysed for security risks are

1. Local account policies
2. Event logging
3. Groups with restricted access or rights
4. Registry security
5. Files security
6. Services security

After the risks have been identified, then the appropriate counter measures can be taken up. They could be set up either by the necessary configuration changes independent of the type of the system, or the set configurations based on the needs of the individual system.

Local communications entity: the next level of security is the data that is being transmitted through network. A number of devices are available for communication like modems and remote access servers. The risks associated with transmission include data capturing, data reading or data modification. The operating system cannot protect the data once it is transmitted. Various protocols are available today to safeguard the data from unintended obtrusion. The objective of security during transmission is to ensure that data is not read or modified before it reaches its intended destination, that it should arrive from authorised sources, and should follow authorised tasks.

Administrative authority entity: A centralized management is required to oversee the entire enterprise system since end, systems and local communications cannot be managed effectively otherwise. Changes, if any, in the configurations can be monitored from a single centralised authority called the administrative authority. This administrative authority entity plans all the changes required centrally after taking into consideration the complexities involved.

Private networks entity: when the data in an organization's network is shared with another company's network it is called a private network. A separate administrative entity is given authority to monitor a set group of accounts in an external network. Security issues involved include which accounts should be made available to a remote source or a private network, and how the network should be structured to prevent direct access by other remote administrative authorities.

Internet: when corporate data is connected to the Internet, it becomes a separate entity. Since the data is now available through an untrusted domain and is exposed to various risks, this entity needs to be separated from other entities. For reasons of security, data accessible to the external sources is located in separate servers called de-militarised zones. These are usually guarded by firewalls from both sides, which prevent intrusion into the internal corporate network. Inside the boundary, access control, end systems and local communications are guarded by separate internal mechanisms.

Article 1	Security entity building block architecture-introduction
Article 2	Data analysis and the concept of security entities
Article 3	Security entities

Answer: [a] The workstation and operating system

Question: ----- when exploited by threats can cause damage to the business assets

- [a] Confidentiality
- [b] Vulnerability
- [c] Availability
- [d] Integrity

Module 5 - Security Strategies

Data in any organisation is vital and vulnerable. The major issues of data include making the right data available to the right people at the right time. In other words, it involves maintaining the confidentiality, integrity and availability of the data.

Objective

The objective of this document is to help readers devise an effective security strategy. Although the requirements may vary from organisation to organisation, the principles of a good security strategy remain the same. These principles have been dealt with below to provide the readers a methodology to compile a good security strategy.

The methodology consists of six steps.

1.Reviewing the current policies

The current status of the policies should be examined in order to identify the vulnerabilities of computer assets. The objective of the review should be to determine the areas where policies are lacking, and examine current documents for improvements. The documents that need to be reviewed are as follows:

- Physical security policies
- Network security policies
- Data security policies
- Management co-ordination and planning
- Contingency plans
- Staff training and awareness
- Other sensitive documents include

Access control passwords, BIOS passwords, router passwords and the like.

2. Identifying assets and vulnerabilities of known threats

Identifying vulnerabilities includes identifying the types of assets that the organisation has. This assessment will help the administrator in identifying vulnerabilities to threats. The assets of the organisation include

Hardware	Clients, servers, communication devices, hubs, switches, peripheral devices,	

	UPS etc
Software	Network and client OS, application tools, software under development
Data & Information	Organisation data: database, emails, spreadsheets, word processing etc Network data: user access rights, passwords, audit trails, configurations and settings User data: personnel processed data, user owned files etc

Vulnerabilities are weaknesses associated with assets. These may include lack of security procedures, insufficient preventive maintenance, insufficient training etc. Vulnerabilities when exploited by threats can cause damage to the assets of the organisation.

3. Identifying likely attack methods

Listing threats will help the security administrator identify the various methods and techniques used in attacks. Threat is anything that causes loss, damage or harm to the assets of the organisation. Examples of threats include user errors, deterioration of storage media, hardware failure transmission errors, natural threats which include incidents caused by fire, flood, earthquakes, extreme temperature, power fluctuation etc.

Attack methods could range from viruses and worms to password cracking and email hacking.

4. Establishing proactive and reactive strategies

Proactive strategies are a series of steps undertaken to assess the existing vulnerabilities and formulate contingency plans. This strategy also includes estimating the possible damage that these attacks could cause to the system.

Re-active strategies are steps taken to assess the damage caused by the attack. They also include rectifying the situation, implementing the contingency plan and getting the business running as soon as possible.

5. Testing

Testing involves simulating the securities strategy in a test lab or a virtual environment to assess the effectiveness of the policies adopted. Although it may not be possible to test scenarios of natural disasters in a test lab, it is suggested that these situations may be simulated to the extent possible to ascertain the readiness of the security team to tackle such disasters.

6. Incident response team

Many organisations have incident response teams as part of their security strategy. The functions of the incident response teams are-

- Identifying software tools to combat security events and incidents
- Conducting research on viruses and system attacks
- Conducting staff training programs, developing security tools etc.

After the security policy has been formulated, the security administrator normally hands over the security maintenance to the incident response team. However, this does not mean that the security administrator is absolved of his duties. He continues to maintain the overall responsibility for the security administration of the company's assets.

Answer: [b] Vulnerability

Module:5

Reference No:M5092

Question: Which of the following is not the reason for the use of Single Sign On (SSO)?

- [a] Use of different systems and applications
- [b] Social engineering
- [c] Labour turnover
- [d] Password synchronisation

Module 5 - Single Sign On

In today's computerised environment the user is greatly facilitated as all his jobs by the computer are accomplished at an amazing speed. No sooner does he press the key on his keyboard all the calculations are done by the computer. But the user has to remember the passwords of all the applications and operating systems used. Many users forget their passwords and find difficult to login. According to The Securities Industries Association the users spend an average of 44.4 hours a year logging on to an average of four applications a day.

Single Sign On (SSO)

SSO is the process whereby a single authentication and authorisation of the user would give him access to all systems and applications. Thus there would be no need to enter the password every time for each application. SSO takes care of the authentication, access control and password synchronisation.

SSO application can be integrated into the existing database or through a proprietary database. These databases will contain all the information about the user. The SSO procedure can be easily integrated with any application or system. The SSO procedures are kept in a central server. The server verifies the information submitted by the user with the database. If the information matches, then the user is given an access to the system and various applications.

Authentication:

Authentication is the process of identifying whether the user is what he purports to be.

Authentication can be of different types viz.

Single factor authentication: When the user is required to give only single information for authentication it is called single factor authentication. Examples are passwords and biometrics

Two factor authentication: Here, two factors are combined before the user can be authenticated. The two factors can be a combination of what the user has, something that he knows and something that he possesses.

Access control: The user is given access control based on the access control list of the user on the server. For example in a SSO facility for web server, the user after authentication is given access to the areas where he has access permission as per access control list. SSO can be scripted or integrated.

Scripted: User id and passwords are stored in the scripts in the central server as variables. When the user logs in, these variables will be drawn from the central server. User key strokes are sent

to the application when it is launched.

Integrated: The applications integrate with the SSO. Scripts are not used. The application takes the information about the user directly from SSO.

Password synchronisation: Passwords are synchronised throughout the company's network. When the user logs in, his password is captured from the database and distributed to the entire network through the central server. When the user logs in to the other applications he need not key in the password again. The central server provides the password to different applications. Once the account is disabled the user is automatically logged off the other accounts too.

Need of SSO: The following are the few of the cases that highlight the need for SSO

- Use of different operating system, application and security databases, which require different passwords to login
- Social engineering - As the user needs to remember different passwords he will tend to forget few of them. He needs to contact help desk every time he forgets the password. There are chances that unless there exists a strong guideline to authenticate the user, the help desk could actually be helping an attacker.
- Labour turnover - Labour turnover in the companies makes it difficult for the administrator to deactivate and delete the accounts of the employees who have left the company.

Advantages:

- The user has to remember only one password
- All the information about all the users will be stored in one place
- Easy to manage all the user accounts
- Authentication in application, which are less secured can be enhanced with two factor authentication.

Answer: [d] Password synchronisation

Module:5

Reference No:M5093

Question: Sometimes, the business requirements of the acquisition may clash with the security considerations. In such a case

- [a] The security needs to be given first priority irrespective of cost.
- [b] Business requirements need to be given first priority irrespective of security.
- [c] A trade off -needs to be made between complexity and security.
- [d] None of the above

Module 5 - Security Administration - part 2

This is the last article in our two-part series on the rules for security administration.

The rules are as follows:

Rule 5- Security needs continuous observation

Having adequate security measures in place before the system has been put into production is an important part of security administration. High security ensures a continuing vigilance over the network. The network is always open to threats from external sources like hackers. For instance, malevolent users could try to intercept the network by flooding the server with a large numbers of legitimate requests or try to enter the system by guessing passwords etc. Hence, a constant supervision and monitoring is required. There are various tools available in the market today to continuously monitor the information systems.

Rule 6-Have a good password policy

A good password policy is an absolute necessity for good security administration. A weak password always compromises even the best security set up. Therefore, it is always important to have a good password policy. Some of the essential features of a password policy are- fixing minimum length, defining the complexity and change routines for the password. Users have a habit of writing down the password- this is one of the biggest mistakes. Other access control mechanisms are magnetic card readers or smart cards, which use the combination of a PIN and physical availability of the card to ensure authenticity, biometric techniques like fingerprints, retina scanners etc.

Rule 7-Security requires good network administration

Network administration is the crux of security administration. Some of the most common and successful examples of the security attacks include the exploitations of network misconfigurations, improper troubleshooting procedures, laxity in creating user accounts etc. The main reason behind this is improper network administration. Network administration should include well-documented procedures, which are as specific as possible.

Rule 8-The more complex the network, the more complicated the security

Complex networks pose high levels of difficulty for administration. Some of the complexities involved could be a partnership with another company, which allows it to access your network, creating a public FTP or web server complex trusts relationship between domains etc. The network should be simple. But keeping in mind the business requirements, a trade off needs be made between complexity and security.

Rule 9-Risk cannot be avoided, but it can be managed

Certain situations may arise wherein the business requirements of the organisation may clash with the security considerations. Therefore, the only way to secure the network is to accept risks and mitigate them. There is always the possibility of network security being compromised, so always a recovery plan should be ready.

Article 1	Laws on security administration part 1
Article 2	Laws on security administration part 2

Answer: [c] A trade off -needs to be made between complexity and security.

Module:5

Reference No:M5094

Question: Which one of the following activities help in preventing Denial of Service attacks?

- [a] Detailed audit trails
- [b] A complete understanding of the configuration
- [c] Good interdepartmental standard and emergency procedures
- [d] All of the above

Module 5 - Best Practises for Preventing Denial Of Service Attacks (DoS)

Most of the organisations have suffered from illegal Denial of Service attacks. (Separate articles have been written on the concept of denial of service/distributed denial of service).

In this article, we will focus on certain preventive measures that can be adopted by an administrator to prevent these attacks. These are some of the measures and procedures that could be adopted.

Best Practises

1. **Audit Trails:** Audit trails maintained by an administrator should be comprehensive enough to contain all the details of all changes made and the causes behind them. This helps in analysing the causes and taking measures to prevent them.
2. **Interdepartmental Standard and Emergency operating procedures:** The organisation needs to have a good cross-group communication built into the standard Operating Procedures and Emergency Operating procedures. These procedures should clearly indicate the steps one needs to follow in case of an emergency. Whom to contact in other segments etc. The administrators need to be aware of the impact their changes have on other segments.
3. **Proactive measures-**network administrators cannot afford to be complacent about emergencies. They need to be constantly alert and be able to visualise serious failures even for their most secure segment or component.
4. **Complete understanding of the configuration-** complete information regarding the network including details like programs, devices, hosts, routers, and various interfaces must be made accessible to all administrators so that better interpretation of the report is made possible. Knowledge sharing needs to be made the essential part of the network administration.
5. **Local and Internet testing-**The functioning of the website needs to be simulated by the team to check if the customer's needs are being met. This will help in understanding difficulties (if any) faced by the customers and will go a long way in ensuring a good customer relationship with the organisation.
6. **The critical element-**It always helps to have a critical element in the team to ensure that the processes are being constantly challenged. This helps in a sceptical evaluation of the system to avoid network outages.
7. **Share knowledge of old configurations and their objectives-**The administrator should always follow the procedure of sharing information about the network configuration with the new inductees. This keeps control settings from being ignored.
8. **Keep track of abnormal activities-** when auditing the configuration; the administrator

needs to ensure that the network designs of all employees follow a standard and pattern. In the case of any abnormal design, he needs to be investigative rather than justifying the change made by that particular employee.

9. **Simplicity, cost and survivability**- When designing the network, we need to keep in mind the advantages of a simple network over a complex design. However if the business requirements demand a complex network then it is always better because the gains of a complex network system is much better than good fault tolerant systems and redundancy. Also, simplicity is capable of imposing many unforeseen problems.
10. **Protect from hackers**- The best way to anticipate and prevent hacking is to try hacking the system yourself. This will help you discover loopholes that are visible in your system and in auditing the weak points of the network

Answer: [d] All of the above

Module:5

Reference No:M5095

Question: Which one of the audit settings is most likely to indicate a hacking attempt on the server?

- [a] Failures of log off attempts
- [b] Successes of log on attempts
- [c] Successes of log off attempts
- [d] Failures of log on attempts

Module 5 - Audit trails part 1 -system audit trails

Audit trails in the context of a computer system represent the sequential recording of events that occur in a computer system. It is a means of evaluating/gauging the system against predefined settings.

The applications of auditing are many-

1. It can be used as a security mechanism.
2. Audit trails may indicate security violations if any
3. They can provide an assurance of how well the security mechanisms are working
4. Audit logs provide accountability for each individual's actions.
5. Audit logs are also used as evidence for administrative/legal purposes.

Audit trails take a lot of time to implement and they take up a lot of resources. Therefore, it is always important to decide which events are going to be audited and trailed. Various operations of a computer system can be audited. Some of the common events/processes that are trailed are as follows

System audit-this contains basic system level operations like logon, logoffs, etc.

File and directories auditing- This provides information about which files and directories and what resources are being accessed

Registry Auditing- registry holds some important system configurations. Hence any changes that are occurring to the registry needs to be kept track of.

Printer/peripherals auditing-Here the accesses to the various printers/peripherals can be tracked. This will help in analysing whether the company resources are being utilised against the policies set or if unauthorised users are accessing the resources of the company.

Remote Access Server Auditing- this audits accesses to remote access servers.

System audit trails

Some of the most essential audit settings for system audit are follows:

(Note-these are only indicative guidelines. The organisation may choose to follow its own settings based on its requirements.)

Server logon and log off activities - logon and log off to the server are important activities which establish control over activities that need to be trailed. Some organizations may only trail the failure of logon procedures because continuous failure to logon may indicate that some hacker may be trying to guess the password and illegally gain entry into the systems.

User rights -This can be used to track access to the user database. The user database defines the rights of the individual users and the access rights given to each user. Auditing events related to user rights may give an indication to the administrator when a user is trying to gain access to resources that are beyond his privilege. Normally users are not given access to this database.

Security policy changes - for the same reason as above, changes to policy statements successful or not may be audited.

User and group management -enables auditing of attempts to access the user database for modification, deletion and creation of new users.

Access to files or directories - auditing may be set for access to certain important files or directories, which may be crucial for the organization.

Restart-shut down for servers -only restart and shut down for server may be audited. As it is very common for workstations to restart and shutdown, it does not have any security implication.

Answer: [d] Failures of log on attempts

Module:5

Reference No:M5096

Question: Which of the following is not a technique of error control?

[a] Error detection

[b] Stop and wait automatic repeat request

- [c] Retransmission after time out
- [d] Positive acknowledgement

Module 5 - Error Control

Information exchange takes place through transmission of signals. They pass through several media links and devices. The signals sent should reach the recipient accurately. The procedure, which coordinates transmission, is called line discipline. The data link layer in the Open System Interconnection (OSI) model takes care of line discipline, flow control and error control. This article describes error control.

Data are sent in blocks. These blocks are called frames. During data transmission, certain errors may occur which may distort the information. Error controls are used to detect and prevent such errors.

Two types of errors are possible during data transmission.

- **Lost frame:** In this case, the frame does not reach the other side. It gets lost in between. If the receiver were not expecting any data he would have no inkling of the error. But the sender on the other hand would expect an acknowledgement within a specific time frame. In certain other cases even though the frame is received, and an acknowledgment sent, the latter may be lost before it reaches the original sender.
- **Damaged frame:** Here although the frame is received some of the bytes could be in error i.e. some of the data is distorted.

Strategies:

There are mainly two strategies that are popular for error control. They are Forward Error Correction (FEC) and Automatic Repeat Request (ARR).

Automatic Repeat Request strategy allows retransmission of corrupted data as well as detection and prevention of errors. It is usually preferred to FEC as number of bits that are used for error detection are less than the number of bits that are required to correct the errors. Forward Error Correction is used when retransmission is impossible or impractical. It only corrects errors. The transmitter along with the original bits sends any redundant information. The receiver of the information tries to find the errors and correct it.

Techniques for error control:

- **Error detection:** Here, an additional bit is added to the data, using algorithm so that the receiver at the other end would know if the data has been received as it was transmitted or has been distorted. This additional bit, known as error detection code, is added by the transmitter. The receiver also does the same calculation, compares the results to know if the data has been corrupted or is error free. E.g. Parity check, cyclic redundancy check
- **Positive acknowledgment:** The receiver acknowledges the receipt of error free data.
- **Retransmission after time out:** The frame that is not acknowledged is retransmitted after a predetermined period of time.
- **Negative acknowledgment and retransmission:** If in a frame an error is detected the destination returns it to the source with negative acknowledgment.

ARQ Standards:

- **Stop and Wait ARQ:** Two types of errors occur. The frame that reaches the destination could be damaged. The receiver checks for errors using the error detection techniques. If

error is found the frame is discarded. The second type of error is damaged acknowledgment.

- Go-back-N ARQ: When there are errors the receiving end acknowledges the receipt of the frame with a negative acknowledgment. Unless the frame is correctly received all the future frames will be discarded.
- Selective-reject ARQ: Frames with negative acknowledgement are retransmitted.

Answer: [b] Stop and Wait Automatic Repeat Request

Module:5

Reference No:M5097

Question: The degree of security level to be achieved is related to

- [a] The risk acceptance level
- [b] Value of the data to be protected
- [c] The exposures of risk
- [d] All of the above

Module 5 - Security Entities Building Block Architecture -introduction

Objective

The objective of the article is to provide the readers a methodology for planning and implementing security mechanisms in an organisation. Computer architecture is becoming increasingly complex and new and improved techniques and tools are available today to manage information systems. These technologies can be utilised effectively when the organisation has a detailed security plan for its computer.

Security Issues

Several Issues need to be tackled before deciding a security structure for an organisation. Some of them have been listed below-

1. What are the objectives of a security plan?
2. The trade off between security levels and costs?
3. How to analyse what is to be secured?
4. What are the entities that need to be secured?
5. What should the system be secured against?
6. Data Availability
7. Redundancy
8. Popular security concepts
9. Building block structure
10. Security Policies

11. Security analysis

Security Objectives

The objectives of security mechanisms are three fold

1. To make the resources of the organisation available to the right users under optimal performance conditions.
2. To ensure that the resources of the organisations are unavailable to unauthorised users
3. To maintain the integrity of the data

The users of data in an information system include both internal users like employees and external users like customers. The best examples of external users are e-commerce customers for various financial and commodity companies. Technology advancement has made communicating very simple today. But technological advancement has also made it easier for hackers to realise their evil designs. Therefore, various security mechanisms are available today to prevent such attacks.

Security levels and costs

The best and the most reliable security mechanism is to simply switch off the computer. But obviously, that doesn't serve any business purpose. To what extent should we secure the computer? The degree of security levels that are to be implemented is a function of three variables. They are

1. The value of the information that is to be protected.
2. Threats that the information is subject to.
3. The risk level that the company is ready to accept.

The degree of security is directly proportional to the value of the information and the threats associated with it. The higher the value and the threat levels, the greater the degree of security. And, the degree of security is inversely proportional to the risk level that the company is willing to accept. High risk levels lower the degree of security.

Another important variable involved is cost. For every security mechanism implementation, there is a direct increase in the cost. This could include equipment, software, maintenance and training costs. Security designs also increase processing costs.

Therefore before deciding on the degree of security levels the administrator needs to have an optimal balance of performance, protection and price.

Article 1	Security entity building block architecture-introduction
Article 2	Data analysis and the concept of security entities
Article 3	Security entities

Answer: [d] All of the above

Question: Which one of the methods can be used to prevent spoofing?

- [a] Adding packet filters to routers.
- [b] Blocking packets with obviously spoofed addresses.
- [c] Applying an access control list to the Ethernet from the terminal card
- [d] All of the above

Module 5 - Source Address Spoofing

What is source address spoofing?

Source address spoofing is modifying a packet's (small chunks of data) return address to indicate that it has originated from a source different from the actual sender.

Which are the services most vulnerable to such attacks?

There are still many software services that use source addresses as security mechanisms to protect their services. For instance SNMP, Unix r Commands, and TCP wrappers all include source address (or system names) as a part of the access control. Such services are vulnerable to spoofing attacks. These services are more vulnerable in an unswitched network environment as the packets can be easily sniffed in such an environment.

Why do people spoof source addresses?

Spoofing is mainly done for the following reasons:

1. To access resources that are available to certain source addresses only.
2. To conceal the attacking source.
3. "Blind Spoofing"

Access resources that are available to certain source addresses only

This can be better explained with an example. For instance, a SNMP agents (a separate article has been written explaining this concept), is configured to respond to requests- (for information or change) from only a specific address (say 10.2.1.98). Using a tool, which is used for the transmission of IP packets, the hacker can spoof a request from 10.2.1.98 and send it to the selected agent.

So, when the SNMP agent replies, it sends back the reply to the address 10.2.1.98, but not to the attacker. The manager at 10.2.1.98 will ignore the response because it had not sent any request to the 10.2.1.98, but the hacker waits for the response. The hacker now sniffs the response on the way to the real SNMP manager to succeed in the attack. Another way of obtaining a response could be by overriding the control of routers. (Routers are devices that are used to control the path of a packet.)

Worse still, if the hacker is not able to sniff the packet on its return path, he can also change the contents. The attacker can also pretend to be the real manager of the above IP address.

Conceal the attacking source

Concealing the source method is always used in distributed denial of service attacks. Source addresses are spoofed to mount a flood of attacks on various commercial sites.

It makes more sense for a DOS attacker to use source address spoofing, because it allows him to cover his tracks, and it reduces the chances of blocking his own network.

Blind spoof

This method is used to gain access into systems, which use source addresses as their security mechanisms. The attacker is not interested in getting a response from the source that is spoofed.

How to prevent spoofing

One of the basic methods to prevent spoofing is to ensure that ISPs filter packets with spoofed source addresses. Today, with better router designs, it is possible to block such packets.

A router is a device, which controls the path of the packets. To do so, routers use destination addresses and the routing information. It can also be used to examine and determine, if the packet came through the same interface.

Terminal servers can also block spoofed source addresses. This can be done by applying access control lists to the Ethernet connection originating from the terminal server.

Another option is to block the obviously spoofed source addresses. Most firewalls are configured to do this. Packet filters also block packets from entering the external interface with internal source addresses.

Answer: [d] All of the above

Module:5

Reference No:M5099

Question: Which one of the following statements is true with regard to data analysis for framing a security strategy?

- [a] Only incoming data needs to be protected during transmission
- [b] Only outgoing data needs to be protected
- [c] Both incoming and outgoing data needs to be protected during transmission.
- [d] None of the above.

Module 5 - Security Entities Building Block Architecture -Analysing data flow and entity architecture

The Planning approach

In this article we have defined the security planning approach which consists of 2 major steps.

- Analysis of data flow
- Defining entities in a computer environment that need to be secured. Here the concept of **Security Entity Building Block Architecture (SEBA)** is introduced.

Data Analysis

As defined in a previous article, the best security solution is a compromise between productivity, performance and price. Instead of securing the entire system we need to identify those locations which are more vulnerable to security threats. For this we need to trail the data from its originating source over the transmission medium and to the destination storage location. In this context the analysis of the data flow can be categorised into 2 classifications.

Data stored in a location: For data located on a computer the main service provider is the operating system. Hence the operating system needs to be configured with the adequate security mechanisms.

Data under transmission: data travelling across a transmission media needs to be secured. various components that need to be secured are shown in the matrix below. "Yes" in the table means it is to be secured.

Particulars	Incoming data	Outgoing data
Protection of data during transmission	Yes	Yes
Receiving system to be protected from network threats	Yes	Yes
Data performs Authorised tasks	Yes	Yes
Authorised sender	Yes	Yes
Authorised receiver-privacy of data	Yes	Yes

Encryption is the technology used to protect data during transmission.

Network connection

There are various types of networks available for data transmission. They are

- 1.The corporate network that is connected to a private network of another organisation
- 2.The corporate network with web servers located at the ISP
- 3.The corporate network connected to the Internet via a Dial Up medium
- 4.The corporate network connected to the Internet through a permanent connection

Considering the above network topology, the security mechanism should be a step-by-step mechanism originating from the source of data, to protection of data through its intervening points and finally concluding with a connection to the Internet

To facilitate this step-by-step implementation, adequate security analysis and determination of a structural design of the system is required. The structural design is explained below.

Defining security architecture entities

In the security building block architecture, the entire network of systems is broken down into individual components called entities. These entities are both physical and conceptual. Based on this structure, the security aspects of each entity can be determined, and suitable security mechanisms can be designed. In this concept, we have identified five basic entities that comprise the entire network architecture.

End system entity-in common terminology this comprises of a computer system with an operating system. It could be a server or a workstation. It also comprises hardware devices connected to a computer (communication devices like modem etc not included.)

Local communication system entity-this encompasses the entire infrastructure for the transmission of data. Or in other words, it includes the network architecture with its related peripherals.

Administrative authority entity

Private network entity-these exist when two or more companies share their networks.

Internet block entity-this includes a corporate network permanently connected to Internet.

Article 1	Security entity building block-introduction
Article 2	Data analysis and the concept of security entities
Article 3	Security entities

Answer: [c] Both incoming and outgoing data needs to be protected during transmission.

Module:5

Reference No:M5100

Question: _____ are the law-abiding people, who find after detecting any the flaws in the software and network and report to the owners.

- [a] White hats
- [b] Black hats
- [c] Gray hats

[d] All the above

Module 5 - Cyber Threats

Business organisations are exposed to unpredictable challenges due to sensitive IT security issues. Therefore it is necessary to evaluate the efforts of businesses in combating these threats. The following are the causes behind cyber threats and types of hackers.

Causes behind Cyber threats

1. **Complex systems:** Higher the complexity of the system greater the threat of exposure to cyber risks.
2. **Involving new external parties:** New parties viz., new partners, customers, employees bring in new applications, networks, databases, and hardware but at the same time they also bring in security problems like new viruses, attack tools and vulnerabilities.
3. **High-level connectivity:** With the increasing dependence on wireless and networking, businesses are exposed to the risk of malicious code and hacking.
4. **Internet:** Greater the use of Internet, higher the number of cyber-abusers. Internet has become the main tool of attack for cyber-abusers.
5. **Anonymity of hackers:** Hackers are drawn to illegal activities due to advantage of anonymity in cyberspace.

Types of Hackers

White hats are law-abiding people who find and report the flaws in software or network to the owners.

Black hats are malicious individuals who misuse the loopholes for the financial benefit. To halt the networks, they steal the credit card numbers or deliver a distributed denial-of-service.

Gray hats are those who act differently in different situations. They may either exploit the loopholes or may inform the organisation.

The following are the key steps that organisations have to take to prevent, detect and recover from cyber threats.

Assess the impact of vulnerability

Identify the effect of cyber attacks on financial position, reputation and regulatory sanctions of the organisation. Recognise the potential threats and estimate the damage that these threats may cause to critical information assets. Based on the analysis, formulate a cyber attack protection strategy and risk management plan consistent with the organisations security objectives. The risk tolerance profile and implementation cost should match in the plan. The information and analysis should be properly documented for future reference. In case of changes or in event of new vulnerabilities, strategy should be modified.

Prevention and detection controls

The following are the key prevention and detection controls that management should undertake:

1. **Develop a security policy:** A security policy has to be prepared by considering the security requirements and standards. Employees must be provided adequate training on the policies.
2. **Design security architecture:** Design and integrate the security architecture framework

with security policies, standards, technology and risk profile. Monitor the framework for regular perfection.

3. **Authentication:** Fraudulent attempts can be identified with predetermined authentication methods like passwords and biometrics.
4. **Intrusion and virus detection:** Ensure that the real-time intrusion and virus detection tools are effective in protecting the organisation against downtime and confidential data loss.
5. **Encryption:** Ensure that encryption, a process of securing data, is used in relation to the risk exposed.
6. **Testing:** Determine the actual operational vulnerabilities through sudden and regular penetration testing. Top management should be informed of the weaknesses.
7. **Modem sweep:** Ensure that modems are not attached to the system without security personnel knowledge, which otherwise may provide a chance for hackers.
8. **Background checks for users:** All the users of information systems like employees and contractors should pass through the background checks. The list should be continuously monitored and updated.
9. **Complete record:** Ensure that records relating to users, activation, systems, networks and applications are properly documented and maintained to facilitate security measures development.
10. **Vendor performance:** When outsourcers are involved, evaluate the performance and financial condition of vendors. Clearly define the network security responsibilities in the contractual agreement.

Recovery steps

The following are the key recovery steps, which management should take after detecting the cyber attacks:

- Develop an incident response program to determine the response of organisation towards cyber-attacks.
- Employ cyber-forensics soon after the attack to detect criminals.
- Develop a business continuity plan to recover the critical components of infrastructure.

Answer: [a] White hats

Module:5

Reference No:M5101

Question: Who has the authority to delegate the operational responsibility of an organisation's security?

- [a] Data owner
- [b] Senior manager
- [c] Data custodian
- [d] Data user

Module 5 - Layers of Responsibility

Layers of Responsibility for organisation security

Organisation security is the responsibility of the whole organisation. Each layer of management has a role to play in organisational security. They need to select the best practices and procedures for the required level of protection. Three layers have been identified according to their functions.

Top management clearly defines the goals and objectives of an organisation.

Functional management has a clear understanding about the work of individual departments. They also know the effect of security on the department.

Operational management the last layer in the organisation and are involved in the actual operations of the systems. They have knowledge about the technical information, procedural requirements and system usage.

Data owner, data custodian and the user play specific roles in the organisation's security.

I. Data owner: Data owner is a person generally from the top management. His functions include data protection, data usage and classification of data, alteration of classifications and delegating the operational responsibility to the data custodian. He has to carry out all these functions carefully and diligently. In case of any corruption of data, he will be held responsible.

II. Data custodian: The network administrator and other IT department staff perform this role. The data custodian's main duty is maintenance and protection of data. His functions include:

- Data backup creation
- Security mechanism implementation
- Data integrity validation
- Data restoring
- Following security policy, standards and guidelines.

III. User: Operational staff are the users. A user is a person who can access the data to perform his operational duties. His functions include protecting data confidentiality, integrity and availability.

Others include

Senior manager who has the ultimate responsibility of security,
Security professional who act as per the senior manager's directives, and
Auditor who verifies the security practices of the organisation

Essential requirements for effective security

1. Establish a senior level committee to gain senior management attention.
2. Strategic security procedures that can define the security needs. Chief Information Officer and the senior management should together draft these procedures.
3. Business managers should identify the level of protection required.
4. Security administrator must create new system user accounts, implement new security software, test security patches and issue new passwords.
5. Information security specialists should not be given the responsibility of decision-making. Though they have the technical knowledge of security implementation and configuration they are not suitable for decision-making.
6. Security function should be undertaken at all levels of management. It should follow a top-down approach. If undertaken at the security administrator level alone, there are chances

for improper risk analysis, risk unawareness and funds shortage for security.

Resources, activities, people and practices of an organisational environment affect the success of a company's security programme. Personnel and structure are the key components. Therefore, they should be properly managed.

Personnel: Human errors, frauds and lack of training are the main causes for security failure. Recruiting qualified staff, providing training facilities proper controls over access and detailed job descriptions are some of the preventive measures that can be taken.

Structure: The structure should provide a clear understanding of responsibilities and authority. Job description should be clearly specified. Separation of duties is one technique that circumvents frauds. In this process, one employee is not allowed to perform more than one work. In this way, work performed by one is automatically checked by another.

Answer: [a] Data owner

Module:5

Reference No:M5103

Question: Which of the following security tool cuts down the content of e-mail inbox to ensure security?

- [a] Encryption
- [b] Content filtering
- [c] Cyber vaults
- [d] Bastion hosts

Module 5 - Security tools

One of the main functions of IT managers for protection of information resources is to predict the imminent threats and vulnerabilities and to take the necessary preventive measures for avoiding their occurrence. These preventive measures may include hardening the system to protect itself from attacks, establishing a fault tolerance mechanism to avoid disturbances in system functioning in case of failure and maintaining key data backup. The following are some of the preventive measures.

Coping with denial of service attacks: The process of making the organisation's web and network servers dysfunctional by sending unnecessary traffic is referred to as denial of service attacks. Packer flooding is the most common type of attack, in which large amount of packets are sent to the target to consume maximum transit network bandwidth. *Ingress filtering* and *egress filtering* are the two DoS mitigation techniques. The former technique disallows any packets from untrusted source addresses and the latter sorts out the legitimate and illegitimate packets.

The following are some of the guidelines for system administrators:

1. Individual and group user identities are established and the web server configured appropriately.
2. Determine protection required for files, devices and objects related to web servers. For example, providing "read only access" for users, service logs for administrators and the like.

3. Minimise the resource usage by separating directories and assigning priorities to processes on web service.
4. Establish time-outs and other controls to avoid attacks.
5. Public web content should not contain any links to files stored elsewhere.
6. Define and implement the web server software access controls.
7. Web server should not respond to the requests of file directory listings.

Content filtering: It helps to cut down the spam in e-mail inbox using filtering. Filtering also helps in reducing web bugs that comes with mail. Thus the risk is minimised. Web content filtering products are essential to exercise control over web content, implementing content restrictions, authorisation and authentication functions and conducting content analysis. This is because, misuse of network resources may cause several security problems.

Filtration of unnecessary services: Sometimes servers may turn on the unnecessary services by default. For instance only SMTP is required for an e-mail server hence Telnet, DNS and others should be turned off. Border routers ensure this. Regular revisits are required to ensure that it permits only the required services, interact with necessary servers only and allow outgoing connections from appropriate systems.

Encryption: The data is translated into a secret code under encryption process. Symmetric and asymmetric encryptions are the two types of encryption.

Offsite data storage: Another way to protect important data from system failures and thefts is to transfer the data to an offsite protected location. There are several web-based backup services provided by vendors, which transmits the data to powerful remote vaults. Data protection and retrieval becomes easy when a large volume of data is stored on optical disks.

Cybervaults: Cybervaults help in protecting the data integrity and systems in case of problems arising due to intrusion detection, firewalls, and anti-virus programs. It also protects security services like firewalls and PKI systems. Application vaults, operating system vaults and data vaults are the three varieties of cybervaults.

Bastion hosts: Bastion hosts are designed to protect internal network against external attacks. It can be undertaken as a single complete security measure or can become one of the security layers in a complex environment.

Firewalls: A firewall may be a program or a hardware device, which ensures the security by filtering incoming and outgoing data. It examines all the incoming and outgoing messages and stops those messages, which do not meet security criteria. These can be applied either in hardware or in software. Packet filtering, application gateways, proxy servers, circuit-level gateways, NAT boxes, reverse firewall are the different firewall techniques.

Virtual private networks: Sometimes a public Internet may provide significant cost reductions to the organisations. Because a wide area network is not always a safe and low-cost source to transmit business related data. Virtual private networks ensure the secure transfer of data. For this, it uses various security techniques. It also authenticates the parties involved and encrypts the data to confirm its integrity and confidentiality. Speed, scalability, security and availability are the aspects to be considered while selecting a VPN.

Firewall and VPN applications: VPN and firewall capabilities are being combined in a single appliance by many vendors to cater to the needs of small organisations and telecommuters. It also

reduces the costs and brings in increased convenience in usage.

Answer: [b] Content filtering

Module:5

Reference No:M5107

Question: One of the primary objectives of security measures is

- [a] To prevent unauthorised use of information
- [b] To ensure legal compliance
- [c] To ensure contractual compliance
- [d] To ensure availability of the information

Module 5 – Control objectives for implementation block

Security management-management controls

Introduction

Security features are a significant component in the development or acquisition of new systems or modification of existing systems. Features like logical access controls need to be considered during initial design phase itself to secure the information that will be generated and stored in the new system. This has been dealt in two parts. This is the first in the series.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To prevent unauthorised use, presentation, or modification of the information.	To ensure confidentiality, integrity, availability and legal and contractual compliance of the system.	1. Authorisation, authentication and identification procedures 2. Identification profiles 3. Cryptographic key management 4. Incident management 5. Virus prevention and detection 6. Firewalls 7. Monitoring tools 8. Intrusion management-testing & reporting 9. Security administration 10. Training	• Data • Technology • Support • Human factor

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **Security management:** The essential components of a security management include
 1. Consideration of risk assessment results for security plans.
 2. Implementation of security measures.
 3. Updating security measures as per changes
 4. Monitoring of implementation
 5. Keeping the security plans in line with other business plans.

Following are the areas wherein the management is expected to provide general policy guidelines. The detailed operational guidelines with respect to specific environment/platforms should conform to the general management control guidelines. The part II of this topic shall cover the operational controls.

- **Access controls-general:** The basic access controls of identification, authentication and authorisation mechanisms should be put in place. These mechanisms should minimise the use of multiple sign-on. The procedures should also ensure the effectiveness of such controls. The identity of the system and the owner should be established in a unique manner, which is central and is consistent with global standards.
- **Online access controls:** The online access security controls measures should be based on the user's need to view, add, change or delete data.
- **Account management:** The procedure established for user account management should have the following components:
 1. Timely establishment of granting and closing or suspending of user accounts.
 2. Approval should be made mandatory for granting access privileges.
 3. Third party arrangements to include security considerations contractually.
 4. Periodic review of user access rights by management.
 5. Comparison of resources with accountability.
 6. Control of normal activities by users of their individual accounts.
- **Security monitoring:** Security administration should consist of monitoring mechanism. All security related activities are to be reported and violations are to be alerted and acted upon immediately. The access to the security information that is logs and other things should be granted based on the principle of least privilege.
- **Data classification:** Classification of data needs to be undertaken for data management. The following issues have to be taken into regard for data classification
 1. The data is to be classified in terms of sensitivity
 2. Owners should decide on the issues of sharing data, programs and files to be maintained, archived or deleted.
 3. Reclassification policies
 4. Organisation's security and legal compliance issues.

Answer: [a] To prevent unauthorised use of information

Module:5

Reference No:M5108

Question: The components of a cryptographic key management include

- [a] Revoking of keys
- [b] Destructing of keys
- [c] Archiving of keys
- [d] All of the above

Module 5 - Control objectives for implementation block

Security management-operational controls

Introduction

Security features are a significant component in the development or acquisition of new systems or modification of existing systems. Features like logical access controls need to be considered during the initial design phase itself to secure the information that will be generated and stored in the new system. This has been dealt in two parts. This is the first in the series.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To prevent unauthorised use, presentation, or modification of the information.	To ensure confidentiality, integrity, availability and compliance of the system.	1. Authorisation, authentication and identification procedures 2. Identification profiles 3. Cryptographic key management 4. Incident management 5. Virus prevention and detection 6. Firewalls 7. Monitoring tools 8. Intrusion management-testing & reporting 9. Security administration	• Data • Technology • Support • Human factor

		10. Training	

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

II. Operational Controls

- **Incident management:** An incident management capability should be established by the company to address security issues. It should be centrally available platform with quick and secure communication links. It should ensure timely and effective response to the security incidents.
- **Accreditation:** It should be ensured that re-accreditation of security is regularly performed.
- **Counter party trust:** The security policies adopted by the organisation should ensure authenticity of the counter party providing information. This could be done through passwords or cryptographic keys.
- **Transaction authorisation:** The security policies adopted by the organisation should ensure that controls are available to validate the authenticity of the transactions. This requires the use of cryptographic technology.
- **Non-repudiation:** The policies adopted by the organisation should prevent denial of transactions by either parties. The controls should provide for non-repudiation of origins, submission or receipt of transactions. This could be done through digital signatures, time stamping and the like.
- **Trusted path:** Procedures adopted by the organisation should ensure that any sensitive information is exchanged only through a trusted path. This could be done through encryption technology between users and systems.
- **Cryptography:** Procedures should be adopted to generate, change, revoke, destruct, distribute, certify, store, use and archive the cryptographic keys. If keys are compromised then the information should be publicised through certification revocation lists.
- **Malicious software:** Procedures should be adopted to prevent, detect and correct malicious software like viruses into the systems.
- **Firewalls:** If the corporate network is connected to the Internet, firewalls should be built in to protect data against denial service attacks or any other unauthorised intrusion or access to the internal resources. The control procedures should be applicable for data flows in both directions.
- **Electronic value security:** The management should adopt mechanisms to protect the integrity of online or electronic transactions through cards, PINs and the like. It should protect the integrity of cards or any other physical mechanisms used to protect the financial data or other sensitive information.

Answer: [d] All of the above

Question: RAID (Redundant Array of Independent Disk) is a good protector against

- [a] Power failure
- [b] Disk failure
- [c] Human mistakes
- [d] Virus threats

Module 5 - Data loss prevention

Data stored in the computer system is very important for any business. If such a data is lost, business may have to incur huge amount of time and money on its recovery or recreation. Sometimes, it may affect the company's competitive advantage. Human error, poor handling, deliberate vandalism manufacturing defects, viruses and natural disasters are common causes for data loss. If the impending problem is identified it becomes easy to prevent.

The following are some of the symptoms of data loss:

- Drive will turn off or won't spin
- Drive will not turn on
- Physical damage
- Documents once accessed become inaccessible
- Unusual noises from hard drive
- Messages stating errors
- CD drives inability to read disks
- Error message that the data is corrupt
- System message on memory errors
- Several types of viral attaches.
- Software do not load

Recovery plan

Prevention is better than cure. Business strategy to adopt a recovery plan will depend on its ability to spend time and money. A real-time fault tolerant system, which gets connected to another server in case of failure, can prevent the data loss and reduce the downtime. It involves heavy investment and the recovery process is also not efficient. Though it is called real-time, many a case the system may not be perfect and would not operate real time. An unsophisticated system may take much time to recover the deleted data from back-up set. On the other hand, a short-time fault tolerant system comes at low cost and well suited to a business that can accept 2-3 hours downtime.

The following are some protective measures against specific failures:

Human mistakes

Human error is a major cause for system failures. Care should be taken while saving or deleting a file. Working under tired conditions may result in accidental mistakes and hence should be avoided. Eatables should be kept away from system. The working area should be clean.

RAID (Redundant Array of Independent Disk)

RAID, if organised properly could serve as a good protector against disk failure. The data is spread across the set of disks and protects against individual disk failure.

Power failure

Power supply is one such disaster for which the business has solution in advance. Uninterruptible power supply (UPS) will reduce the system failure due to power fluctuations and failures. The selection of an appropriate UPS should be based on the business's requirements. It can protect the system for several hours till the generator is on.

Natural disasters

Complete backup strategy is essential to protect the data against flood, fire and other natural disasters. Full backup, differential backup, incremental backup are different strategies which the business can adopt depending on its requirement. Backup copies should be stored in a safe place.

Hard disk failure

Utilities like Power-Quest's Drive Image Pro 3.0 can protect against hard disk failure by transferring the disk contents to another drive. They further act as back-ups since they restore the hard drives.

Virus threats

The use of Internet and e-mail has increased the threat of virus. The attachments received from an unknown sender may contain virus and affect the data. Adoption of anti-virus software, which examines all the attachments, could be a preferable solution. Regular updating and provision of anti-virus training to employees is also essential.

Accidental deletions

Sometimes, a single file or document may be deleted accidentally. Undelete packages can help in recovering such files.

In spite of all measures like recovery plans, UPS, hard disk back up a business may loose data due to some natural disaster. Recovery utilities may not work at that time. Taking the help of data recovery specialists becomes inevitable. Professional data recovery specialists are well known for recovering the data, which is inaccessible, by any other mode.

Answer: [b] Disk failure

Module:5

Reference No:M5110

Question: Which of the following method would help in preventing wireless eavesdropping?

- [a] Using a code known only to the receiver
- [b] Using a paper shredder to destroy all paper documents that are not needed
- [c] All entry points to the building must be guarded with electronic locks
- [d] Computer must be locked if employee is not at his desk

Module 5 – Information Stealing Methods and their Prevention – II

Knowledge of the common methods of information stealing can help managers and auditors prevent it from happening in the first place.

Part I dealt with "Dumpster diving", "Electronic spying" and "Guest spies". This part discusses some more methods and some suggestions to prevent them.

- **Computer Break-ins**

The entire operations of organisations are now computerised as a result of which, the traditional information stealing methods like trash trawling have become slightly redundant. Information is now stolen from computers through "hacking", whereby an unauthorised person gains access to the computer. The first rule to protect electronically stored information is to educate all users on the precautions to be taken.

Recommendations

- Guests must be allowed only monitored access to computers. Computer maintenance personnel are one primary source of information leakage. A trustworthy person must always accompany any person who is not a full-time employee.
- Laptops are a common source of information pilferage. Physical protection is one area of laptop security. More importantly, laptops must be logged off and strong passwords must be used. Some operating systems for laptops have the Encrypted File System, which encrypts all the data.
- Floppy and CD disks, backup tapes and the like store valuable information and hence must be given the same consideration as computers. This is often overlooked and is another vulnerable device.
- All computers must be logged off or locked if an employee is not at his desk.
- All file deletions must be done using special delete software that completely erases data. Alternatively, the hard disk may be partitioned into small drives and then formatted when files are to be removed

These are not the only security measures that have to be taken to prevent hacking. There are many technical and control aspects to secure corporate systems as discussed in other articles.

5. Wireless Eavesdropping

With mobile Telephony becoming very popular, telephone conversations through cellular phones are now common. It is however, not realised that a cell phone conversation can be picked up by a suitable receiver over a wide area without affecting the quality.

Computer-aided call monitoring has brought down eavesdropping level to zero within the specific target area. Calls from airline telephones, satellite-transmitted phone calls and microwave transmissions can also be monitored.

Recommendations

- Avoid mentioning any confidential information
- Use any "code" known only to the receiver
- Caller and receiver must not associate themselves with a company or other "identification" tags

- Use cordless phones, which are in 900 Mhz frequency range, to receive the call and then immediately transfer it to a regular land line

5. Technology and Devices

Technology has helped us communicate better and faster with devices such as answering machines, fax and dictation machines. However, malicious people can use these devices to gather confidential information. Some examples are:

- Voice operated devices such as answering machines and voice mail can be monitored and passwords broken, since they have only a three-digit code as password. Latest machines also have a "remote access" feature that allows the owners to listen to stored messages from a remote location. Unfortunately, this can be misused by hackers to retrieve information
- Fax Machines are another source of information leakage that is uncontrolled. Many fax machines have back up rolls that contain complete snapshots of all received messages. Also, any fax messages received when a trusted person is not around can lead to integrity loss.
- Microphones, especially of the wireless type, can be received with absolute clarity over a mile. Conferences and meetings where confidential information is exchanged must not use any microphones or even any sort of wireless device that does not have encryption.

Answer: [a] Using a code known only to the receiver

Module:5

Reference No:M5111

Question: Which of the following is not a method of information stealing?

- [a] Dumpster Diving
- [b] Bugging and wire tapping
- [c] Delphi method
- [d] Guest spies

Module 5 – Information Stealing Methods and their Prevention – I

Corporate espionage or information stealing of confidential matters can cause huge amount of loss, in terms of time and money. While the company invests a huge amount in R&D to develop new products, a competitor on the other hand, may rob and get those results without spending anything.

Knowledge of the common methods of information stealing can help managers and auditors prevent it from happening in the first place. Some methods and recommendations are discussed below.

1. Dumpster Diving

Also known as trash trawling or more sophisticatedly, "waste archaeology", it refers to a technique whereby a person searches through waste paper, garbage and papers lying around to glean information. For instance, a small bank statement about a trivial purchase may reveal credit card numbers, account numbers and the like.

Regarded as the first step in information stealing, the persons involved are however not liable to legal prosecution. This is because, information contained in garbage cannot be considered confidential.

Prevention

- Use paper shredders to destroy all paper documents that are not needed
- Papers must be destroyed before being recycled. They should not be sent without shredding thinking that "anyhow they are going to be recycled."
- Electronic documents such as emails also are prone to this attack, especially with rapid computerisation. Deleting documents does not mean completely scrapping it; only the name is deleted.

2. Bugging and Wiretapping

These electronic spying techniques get information through the communication channels such as telephone, computer networks and the like. By attaching a special device on the data transmission route the attacker can listen to it.

Recommendations

- If there is any suspicion of electronic spying it is advisable to report the matter to the senior most employee of the company immediately.
- Contrary to the advertisements, "fix-it yourself" solutions to counter the information theft do not usually work. Only a professional team has the equipment and expertise to detect the surveillance devices and also the person. The corporate security chief is better qualified to do the search for such a team. If there is no such person, a reputed security organisation may help.

3. "Guest" spies

Organisations may hire temporary employees in computers, HR or design who will have considerably good access to sensitive data rather than low-level operations staff like maintenance. All temporary employees have to be monitored according to a single policy. Besides this, an organisation, especially those with large staff and premises, expects guests or business contacts. Every care must be taken to guard sensitive information in such cases.

Recommendations

- A thorough authentication of credentials by a competent permanent employee is necessary. The person must produce an identity card that indicates the nature of work, the department, the person who has authorised him and the physical location, where he must perform his duties. It must be noted that the last mentioned is seldom done, with the result that such temporary employees are found in all locations of the building.
- An employee must accompany all temporary personnel or guests while in the premises. Low-level or maintenance personnel must be taken to the employee who has requested the service. That employee is then responsible to take him to the place of work, stay till the work is completed and see him out of the office. In case of personnel being hired for a longer period, an appropriate ID card must be issued.
- All entry points must be guarded with electronic locks that open only when a magnetic

card is used. The employee ID card may be used for this purpose.

Answer: [c] Delphi method

Module:5

Reference No:M5112

Question: Which of the following need not be considered before hosting a new online privacy policy?

- [a] Business practices
- [b] Nature of the site
- [c] Proposed users
- [d] Business partner

Module 5 - Net Privacy

Today, the Internet has virtually bridged all geographical barriers. It has simplified communication and business. Technology nevertheless, created some difficulties too. Invasion of online privacy is being one of them.

A lot of personal information has to be submitted to the Internet companies to avail of their services. This information is in turn distributed to other web based companies. Result? Unwarranted mails, junk information, malicious software, and the like apart from invasion of personal privacy! This can lead to serious implications like theft of identity or impersonation.

A website collecting information from another country, is bound by the laws of that country. Additionally, if a website collects information from the citizens of another country, the information collected will be subject to the latter's laws. Site owners should conform to the privacy policy of the site. A privacy policy normally states how the information collected from site visitors will be utilised. In many cases, companies violate their own privacy laws though.

Hosting the privacy policy

Websites have to be cautious in evaluating the new online privacy policy prior to hosting it. The cost and benefits must be assessed in the light of business practices, nature of the site and the proposed users. The option to host a privacy policy depends on the extent to which the site collects and shares the personal information like names and e-mail addresses. Unless the website clearly states the intended use of the information in the privacy policy, users may not be willing to visit the site.

Users of the site are well aware of the technical faults related to privacy issues. Hence, companies should also reveal the policies developed for information collection (which may be collected either through voluntary or involuntary means) to the users. This helps the companies to capture user confidence and pose a viable presence in the market place. Failure to develop privacy policies may on the contrary cause huge damage to the companies.

Concerns requiring special attention

Mergers: Problems may arise when a merger takes place between two Internet companies. One company may share and reveal the user related information against the other company's policies. Companies often do not give much importance to privacy issues. They must review the practices followed by other companies before implementing mergers.

Outsourcing: Companies must inform the outsourcers about the policies and practices at the time of undertaking contract to avoid violation of privacy policy.

Companies should not overestimate the importance of developing a detailed privacy policy in the scenario of increasing public awareness about the privacy issues. They should consider the key issues pertaining to the Internet privacy to avoid the risk of liability.

Answer: [d] Business partners

Module:5

Reference No:M5113

Question: Which of the following details should be included in the reports on security breaches?

- [a] Authorised access to system resources
- [b] Unauthorised access to system
- [c] Unauthorised attempts to change security definitions
- [d] All of the above

Module 5- Audit working guideline

Security Management

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Security management	1. Security management 2. Access controls-general 3. Online access controls 4. Account management 5. Security monitoring 6. Data classification	1. Incident management 2. Accreditation 3. Counter party trust 4. Transaction authorisation 5. Non-repudiation 6. Trusted path 7. Cryptography 8. Malicious software 9. Firewalls 10. Electronic value security

Audit Process

The audit process has been covered in four parts. This article is the first part, and deals with a preliminary understanding. Preliminary analysis has been partly covered in this article; the rest has been covered in the subsequent article.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. Security management head 2. Security administrator 3. Database administrator 4. IT senior management 5. Application project team management	1. Policies and procedures of the entire organisation and IT relating to • Information security • Access management • Account management • E-Commerce security standards • Data classification scheme • Access control software • Physical environment details • Physical access points to IT resources • Change management procedures regarding security • Problem management procedures regarding security • Security breach and exception reports • Encryption devices • Outside parties having access to system resources • Third party service providers and the related contracts • Security testing • User signed security documents • Training material • External party audit and investigation reports

Preliminary analysis

The next step is analysing the effectiveness of the control measures adopted and the degree of reliability that can be placed on these measures. This can be done through ensuring that the security management plan/procedure adopted by the organisation consists of /provides for the following details:

1. A security strategy plan to control information flow and user security
2. A security team to manage proper accesses to information and resources related to IT
3. A data classification scheme
4. All systems and information have an identified owner
5. User security levels that have been determined and adherence to the principle of 'least access'
6. Induction of new employees including security awareness and the responsibility of the individual owners
7. Security breach and exception reports -these include unauthorised accesses to system and resources, security policies and definitions, access attempts beyond the privilege etc.

8. Cryptographic key management procedures and standards
9. Change control procedures for security software consistent with the other system development and maintenance procedures

The subsequent articles focus on the remaining processes- test of controls and substantive testing.

Answer:[d] All of the above

Module:5

Reference No:M5114

Question: Which of the following features does the authentication mechanisms include?

- [a] Single use of authentication data
- [b] Single authentication mechanisms for all resources
- [c] Any number of concurrent sessions for single user
- [d] None of the above

Module 5- Audit working guideline

Security Management

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Security management	1. Security management 2. Access controls-general 3. Online access controls 4. Account management 5. Security monitoring 6. Data classification	1. Incident management 2. Accreditation 3. Counter party trust 4. Transaction authorisation 5. Non-repudiation 6. Trusted path 7. Cryptography 8. Malicious software 9. Firewalls 10. Electronic value security

Audit Process

The audit process has been covered in four parts. The first part covered a preliminary understanding and part of preliminary analysis of the process. This article is the second part, and focuses on the rest of the preliminary analysis.

Preliminary analysis-contd

This step consists of analysing the effectiveness of the control measures adopted and the degree of reliability that can be placed on the control measures. This can be done through ensuring that project management plan/procedure adopted by the organisation consists of /provides for the following details:

9. The authentication mechanisms should have the following features:
 - Prevent multiple use of the same authentication mechanism
 - Enable usage of multiple authentication mechanisms
 - Applicability of separate authentication for different events
10. Restrict the number of simultaneous sessions the same user can enter into
11. Display of a warning message regarding the usage of the hardware and software after logging on.
12. On gaining access to the system, the history of successful and unsuccessful attempts to access must be displayed to the user.
13. The password policy should have the following components:
 - Pre-defined minimum length of the password
 - Frequency of password changes
 - Protection for emergency passwords
14. Problem resolution management should enable the following:
 - Suspension of user ID after a pre-defined number of unsuccessful logon attempts
 - Display of the details of unsuccessful attempts including the date, time and number of unsuccessful attempts to authorised users.
 - A maximum time limit for authentication.
15. Dial-in procedures should include the following components:
 - Dial back
 - Enable frequent changes in dial-up numbers
 - Firewall mechanisms
 - Enable frequent change of passwords
 - Deactivation of former employee passwords
16. Physical access controls to locations housing the systems.
17. Logical and physical access controls to voicemail and EPABX
18. Security policies for personnel in key positions. They are normally required to be away for a certain period every year. During this period, the person's mail ID is substituted by a replacement. The replacement is required to report any abnormalities occurring during the suspension period. This replacement is normally done unannounced. Similarly, surprise job rotations are also undertaken for security purposes.
19. Access to security related information, hardware, and software is limited
20. Use of trust paths to transmit non-encrypted data
21. Prevent DOS attacks through junk faxes, by revealing fax numbers to outsiders only on a need basis and restricting the usage of lines only for business solicitation.
22. Control measures for virus detection and prevention
23. Adequate control to protect E-commerce transactions

24. State whether adequate physical security measures have been adopted.

The subsequent articles focus on the remaining processes- test of controls and substantive testing.

Answer:[a] Single use of authentication data

Module:5

Reference No:M5115

Question: For physical and environmental security which of the following policies and procedures should be framed?

- [a] Layout of facilities
- [b] Independent assurances
- [c] System Development Life Cycle (SDLC)
- [d] None of the above

Module 5 – Audit working guideline

Physical and environmental security Part 1

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Physical and environmental security	1. Access to IT area 2. Physical controls 3. Environmental controls 4. Health and safety measures 5. Continuous supply of power	The operational controls should ensure that the physical and environmental controls along with health and safety measures are implemented.

Audit Process

Audit process has been covered in four parts. The first part deals with the preliminary understanding . Preliminary analysis is dealt in detail in the second part. Test of controls is dealt in the third part. The concluding part deals with substantive testing.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. Facilities in charge 2. Security team 3. Risk assessment personnel 4. Operations team	1. Policies and procedures with respect to • Management of facilities • Layout of facilities • Entry and exit points • Security measures • Security contracts • Access to facilities • Maintenance of facilities • Health and safety measures • Restriction on visitors • Environmental controls • Inventory of facilities • Regulatory requirements 2. Organisational policies and procedures related to • Management of facilities • Layout • Security measures • Safety measures • Inventory of fixed assets • Acquisition and leasing of facilities and assets 3. Details of personnel who have access right to facilities and floors where facilities are kept 4. Performance expectations of resources in case service level agreements 5. Continuity plan

Preliminary analysis

The next step is analyse the effectiveness of the control measures adopted and the degree of reliability that can be placed on the control measures.

The preliminary analysis has been classified into environmental and physical facilities. The environmental facilities are analysed through ensuring that

- Appropriate appliances for detection of fire, electric fluctuation, alarm procedures are installed
- Air conditioners and humidity control equipments are in place
- Additional infrastructure facilities are available in case of failure of facilities viz., uninterruptible power supply (UPS), rerouting of telecommunication lines, air conditioners, humidity control equipments, water, gas and the like
- Procedure exists for handling expected circumstances for various level of emergencies that may occur
- The above mentioned facilities are reviewed
- Environmental regulations are adhered to

Answer: [a] Layout of facilities

Question: Which of the following features does an auditor need to ensure, for a firewall mechanism?

- [a] Exchange of traffic at the application layer
- [b] Applicability of firewall controls only from external to internal network traffic
- [c] Different control measures for application and network layers
- [d] Protocol discontinuity at the network layer

Module 5- Audit working guideline

Security Management

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Security management	1. Security management 2. Access controls-general 3. Online access controls 4. Account management 5. Security monitoring 6. Data classification	1. Incident management 2. Accreditation 3. Counter party trust 4. Transaction authorisation 5. Non-repudiation 6. Trusted path 7. Cryptography 8. Malicious software 9. Firewalls 10. Electronic value security

Audit Process

The audit process has been covered in four parts. The first three parts covered the preliminary understanding, preliminary analysis and part of test of controls. This article is the fourth part, and focuses on the concluding part of test of controls and substantive testing.

Tests of controls -contd

19. All traffic (from outside to inside and vice versa) must pass through the firewall
20. Only authorised traffic should be allowed to pass through
21. The firewall should be immune to penetration
22. Traffic should be exchanged at the application layer only
23. The firewall control measures should be combined both at the application and network layer
24. The firewall should provide for change of protocols at the transport layer
25. Strong authentication mechanisms should be used for management of firewall components
26. The firewall should cover up the internal network architecture

27. Audit trails should be available for all communications that pass through the firewall and an alert mechanism should be available for reporting any unusual activities.
28. The firewall should defend itself from any direct attacks.
29. All .exe files should be scanned before they are let into the network

Substantive testing

This step is undertaken to substantiate the auditor's viewpoint that control objectives are either not being met, or do not exist. The shortcomings in controls and its consequences also should be documented. The auditor can also:

1. Identify comparative benchmarks from similar organisations, and industries.
2. Perform a detailed review of the
 - Security, internal controls and audit trails of the systems, including the penetration review of the logical and physical security
 - Security awareness level among new employees
 - The access privileges of users and determine if they are being reviewed regularly by management

Identification of shortfalls

The auditor should identify

- Inapt user access privileges
- Inconsistencies in the network, security schema like missing access links etc
- Deficiencies in the contract with regard to security and data integrity during transmission
- Illegitimate users or accesses of former employees
- Informal requests to access system resources
- Software that does not record security breaches
- Improper/inadequate control features and audit trails
- Deficient key management protocols
- Non-updates of virus detection software
- Non-compliance with third party services agreement
- Non-compliance with contract programming terms and conditions
- Products which were accepted without adequate facilities testing, system testing, and accommodation testing
- Products which were accepted without technology testing, functionality testing and work load trails
- System failure

Non-compliance with contract terms and conditions.

Answer:[a] Exchange of traffic at the application layer

Question: Data structures refer to

- [a] Memory locations in the hard disk that store data
- [b] User programs that handle data
- [c] A particular format of storing and handling data
- [d] A collection of data in a sequence

Module 5- Data Structures- Part I

Definition

Data structure refers to a specific format for storing and handling data. A *format* is a specific layout for data that specifies the input/ output form of the data, how the data is stored in the memory, how many bytes it occupies and what kind of operations can be performed on the data. Some of the examples of data structures are array, file, linked lists, record, table and trees. Data structures systematise data in order to serve specific purposes, so that they can be easily accessed and operated. Data structures are implemented in programs in order to store the data efficiently in terms of memory utilisation, access time and program implementations.

Purpose of data structures: Data is stored in a specific format so that the program that uses the data knows how to handle them. Standard format for data (or data structures) helps the programmer to identify the size of the data and the operations performed on them, thereby enhancing the performance of the program.

Further, computer storage devices like hard disks, floppy disks and the like have formatted / prescribed memory storage patterns (i.e. they are divided into tracks, clusters or sectors). Thus, mapping the data in to the memory becomes simpler with the use of data structures. This way the programmer will know how to reach each bit of data that is stored in the computer hard disk.

Elements of data structures

Arrays:

Arrays are data structures that store data of the same size and type, in succession. For e.g. array of integers, array of characters, or array of pointers. The characteristic property of an array is that each element is of same type and is referenced by the same name (the 'array name') but with a different subscript. For e.g. we can declare an array of say 100 integers and assign the name A1, A2, A3 and so on till A100. This kind of reference increases the readability of user programs.

Arrays can be single or multi dimensional.

In physical terms, arrays refer to consecutive memory locations in RAM.

Limitations: Arrays can be used only when the maximum number of data entries is fixed. It does not support dynamic memory allocation (i.e. arrays memory allocation is static or fixed).

Files:

File is a collection of data or records, with a name to refer it. Different types of files are text files, program files and the like. The type of data stored by these files makes each one different from the other. E.g. a text file stores data in text form, while an image file stores images and a directory file stores files. Operating systems attach a suffix with the name of the file in order to distinguish each type of file from the other. The suffix, also known as file extension, is based on the type of file. E.g. in windows, text files have .txt as their extension, word documents have .doc as file extension and so on. The different ways in which the user accesses files are sequential access, indexed-sequential access and random access.

Some more elements of data structures have been discussed in 'Data structures-II'.

Answer: [c] A particular format of storing and handling data

Module:5

Reference No:M5124

Question: Policies are defined and documented in which of the following IT Security Maturity Levels?

- [a] Level III - Implementation
- [b] Level I - Policies
- [c] Level II - Procedures
- [d] Level IV - Test

Module 5 - Security Maturity Levels - Introduction

Introduction

The five maturity levels in IT security are Policies, Procedures, Implementation, Test and Integration. These maturity levels are important while reviewing the criteria. All the maturity levels are interlinked and must be attained in the order specified i.e subsequent levels can be achieved only after the previous levels have been achieved. The following is a detailed description of the five levels.

Security Maturity Level I

Policies: This is the primary level, in which policies are documented and circulated to the employees. It provides guidelines for risk assessment, implementation and monitoring. Policies pertaining to all the core assets are written and agreed upon by the concerned parties. The structure of the IT security management, and the responsibilities of the IT security staff along with the performance measuring techniques are defined in the policies. Further they also state the necessary actions to be taken in case of any deviations in the policies.

Security Maturity Level II

Procedures: Procedures to execute security controls stated in the earlier level are documented and supplied in level II. Procedures clearly state the time, place and person required to perform them. It lays down the responsibilities of the owners, users of the assets, data processing personnel, security administrators and the information resources management team. It gives the references of contact persons in case of any requirement. It also provides guidelines for security controls implementation.

Security Maturity Level III

Implementation: Under implementation maturity level, relevant personnel are informed about the procedures and controls that need to be applied and consistently implemented wherever applicable. The necessary training is provided to implement the procedures. Controls are tested to ensure their operation. Ad hoc approaches are discouraged.

Security Maturity Level IV

Test: Tests are conducted to evaluate the effectiveness of policies, procedures, controls and their implementation in order to ensure that they are maintaining IT security at the accepted levels. In case any weaknesses are identified, corrective measures are taken immediately. Further, agency staff or contractors can conduct self-assessment on a routine basis. A General Accounting Office, and the Inspector General of an Agency can carry on Independent audits which act as a check on the performance of an agency. Test results provide an effective means to recognise security threats well in advance. Frequency of tests is based on the level of risk.

Security Maturity Level V

Integration: Integration is the last security maturity level. Here continuous improvements are made to the policies, procedures, implementation and test procedures. The IT security programme at the enterprise level, which is an essential part of the culture, ensures the cost-effectiveness of security controls. Controls are modified according to changes in the environment and in case of security vulnerabilities. The cost-effectiveness of the IT security is measured and alternatives are evaluated. Status metrics are developed. Cost and risk elements along with the mission are considered in decision-making.

Answer: [b] Level I - Policies

Module:5

Reference No:M5125

Question: Which of the following criteria deals with the separation of duties when evaluating Policy levels in Security Maturity Levels?

- [a] Security controls review
- [b] Personal controls
- [c] IT roles and responsibilities
- [d] Documentation rules

Module 5 - Policy - Security Maturity Levels - Part I

The introductory section dealt with the five Security Maturity Levels . This article dwells on the critical aspects that need consideration while evaluating the criteria at the Policy level, which is the first level.

Level I: - Policies:

A topic-wise categorisation of the critical aspects to be considered:

1. IT roles and responsibilities

The policies must necessitate the incorporation of separation of duties, accountability controls in the IT operations and describe and assign the security roles to individuals. There must be appropriate policies for division of sensitive functions like system administration, financial administration among key personnel. Different individuals must carry on the support functions.

The duties of personnel managing access control and those managing audit trail must be identified

and stated in the policies. The policies must outline the IT responsibilities in the organisational structure. Recognising the key functions and assigning roles must be mandatory. Policies should recognise all the related programmes with which the high-risk programme interfaces.

2. Security Controls review

Policies for security controls review, periodic reviews and independent reviews in case of any changes must be available. Policies must necessitate the operating system review to protect security software. They should also demand implementation of security actions, consistency of security controls with regard to the IT and implementation of corrective measures. Review of audit trails and authorisation for temporary access must be stated in the policies. Policies should also state the automated tools used for examining audit records.

3. Behaviour and documentation rules

Policies must clearly state the development of behaviour rules, their enforcement and protection. They should also provide for updation of documentation in case of any changes to the security controls. Policies must be framed for password usage, its security and distribution and software or equipment usage. Policies must also demand IT backup, emergency procedures and operational and security procedures. Existence of policies for hosting a privacy policy on the web must be ensured.

4. Performance evaluation and feedback

Regular self-assessments must be obligatory and necessitate the regular testing of important security controls like network scans, router, etc. They must insist on the scrutiny of security alerts to assess its severity. Policies must provide for identifying and reporting security weaknesses and state the corrective actions and evaluate their effectiveness. Policies must establish enterprise wide performance metrics, which should evaluate the cost effectiveness of the controls.

5. Protection of critical infrastructure

Policies must demand identification of critical assets, high-risk programmes and the resources supporting them. They should also demand Infrastructure Protection plan development. Documenting and communicating the contingency, protection and recovery plans should be the requirement of the policies. Policies must necessitate plan updation and documenting the changes. The interconnection agreements with business partners, security information contained in the agreements and its review and audit must be covered in the policies.

6. Personnel controls

There must be policies for position review, job description (separately for high-risk programmes), defining user responsibilities, job rotations and training for managing accounts that reflect hiring, termination and transfer of personnel. Policies should demand personnel screening before allowing them to access ??in the absence of effective controls. Policies for allowing maintenance and repairs, approval and authorisation of access must exist. Policies relating high-risk programme access and access denial or removal should also be stated.

7. Programme specific controls

Programme specific controls must be developed and configured on the basis of standard rules and specific requirements.

Answer: [c] IT roles and responsibilities

Question: Which of the following criteria deals with the corrective actions and access controls while evaluating Procedure level in Security Maturity Levels?

- [a] IT roles and responsibilities
- [b] Behaviour and documentation rules
- [c] Performance evaluation and Feedback
- [d] Security controls review

Module 5 - Procedures - Security Maturity Levels - Part II

This article analyses the critical aspects to be considered while evaluating the criteria for the second level, the Procedures level.

Level II: - Procedures:

A topic-wise description of critical aspects:

1. IT roles and responsibilities

Procedures should be available for:

- Separation of duties, accountability controls, security roles and individual responsibilities, division of key function among responsible persons and key programme functions
- Recognition of support functions and responsible persons.
- Incorporating IT security responsibilities into the organisational structure.
- Distinct delegation of duties among personnel managing access control and those managing audit trial.
- Recognition of related programmes with which the high-risk programme interfaces.

2. Security Controls review

Procedures for the following with regard to the review of security controls need to be stated:

- Examination of security controls for systems and programmes, periodic reviews, periodic programme reviews besides periodic independent and operating system reviews.
- Specification of management's role in executing security actions.
- Consistency of security controls with internal IT architecture
- Corrective actions and access controls
- Review of audit trials and automated tools used for audit record review.

3. Behaviour and documentation rules

Procedures regarding behaviour and documentation rules for the following should be clearly detailed:

- Modifying system documentation in case of any alteration to security controls
- Development of behaviour rules, their enforcement and protection
- Password usage, its security and prevention of unauthorised access
- Creating documentation showing methods of system usage
- IT backup, emergency, operational and security procedures
- Exercising controlled log-on signs

- Privacy policy placement

4. Performance evaluation and feedback

Procedures for the following pertaining to performance evaluation must be defined:

- Managing routine self-assessments, regular testing of important security controls.
- Examining security alerts, identifying weaknesses, developing corrective actions, and their implementation.
- Establishing metrics for system security programme, its usage in performance evaluation, costs and benefits assessment of security controls.

5. Protection of critical infrastructure

Procedures for the following in relation to protection of critical infrastructure need to be outlined:

- Recognising the critical operations, high-risk programmes and resources supporting them.
- Identifying critical assets, their inter-dependencies and documentation.
- Recognising and recording the critical failure points and establishing recovery and communication plans.
- Creation and updation of Critical Infrastructure Protection plan, contingency plan and documenting the plan.
- Altering the plans in case of any changes in assets.
- Development, review and audit of interconnection agreements with business partners and their security requirements.

6. Personnel controls

Procedures pertaining to controls over personnel must include:

- Job descriptions reflecting individual responsibilities, job rotations, defining user responsibilities, training the personnel for managing accounts that reflect hiring, termination and transfer of personnel.
- Personnel screening before allowing them to access??, and the conditions under which it is essential. Approval and authorisation of access and its review
- Maintenance and repairs
- High risk programme access, and a statement of individual responsibilities.

7. Programme specific controls

Procedures for the recognising programme specific controls must be clearly stated. They must be configured on the basis of the standard rules and specific requirements.

Answer: [d] Security controls review

Module:5

Reference No:M5127

Question: Which of the following is evaluated in security controls review in the implementation level of the Security Maturity Levels?

- [a] Separation of duties
- [b] Security controls for systems and programmes
- [c] Job description and individual responsibilities

[d] Behaviour rules

Module 5 - Implementation - Security Maturity Levels - Part III

The introductory articles of this series discussed the five Security Maturity Levels. This article analyses the critical aspects to be considered while evaluating the criteria for the Implementation level.

Level III: - Implementation:

Critical aspects to be considered at the Implementation Level are:

1. IT roles and responsibilities

The following must be implemented with regard to IT roles and responsibilities:

- Separation of duties
- Accountability controls
- Assigning security roles and individual responsibilities
- Division of key functions and programmes among responsible persons
- Recognition of support functions and responsible persons
- Incorporating IT security responsibilities into the organisational structure
- Duties of the personnel managing access control and those managing audit trail must be separated
- Recognising the related programmes with which the high-risk programme interfaces

2. Security Controls review

The following must be conducted to evaluate the security controls:

- Periodic reviews, periodic programme reviews, evaluation of security controls for systems and programmes, independent reviews and operating system review periodically
- Evaluation of management role in executing remedial security actions
- Evaluation of security controls to ensure their consistency with internal IT architecture
- Corrective actions and access controls
- Examination of audit trails and automated tools used for audit record review

3. Behaviour and documentation rules

Before implementing behaviour and documentation rules:

- Ensure the modification of system documentation for any deviation from security controls
- Evaluate the protection of password usage, its security and prevention of unauthorised access
- Ensure that the method of system usage is properly documented
- Development of behaviour rules, its enforcement and protection
- Examine the adequacy of IT backup, emergency and operational and security procedures
- Check whether a standardised log-on sign is placed on the system
- Determine the existence of privacy policy on the web

4. Performance evaluation and feedback

Ensure the implementation of the following pertaining to performance evaluation

- Routine self-assessments
- Frequent testing of important security controls
- Corrective actions after identifying weaknesses from the security alerts review and their

effectiveness

- Metrics for system security programmes
- Metrics to evaluate the performance and assessment of the costs and benefits of security controls

5. Protection of critical infrastructure

Ensure the following to evaluate the protection of critical infrastructure:

- Critical operations, high-risk programmes and resources supporting them are recognised
- Critical assets, their inter-dependencies and documentation are identified
- Critical failure points are recognised and recorded. Further recovery and communication plans are established
- Creation and updation of Critical Infrastructure Protection plan, contingency plan and its documentation.
- Changes are incorporated in the protection plans
- Interconnection agreements with business partners are developed, reviewed and the security requirements are audited

6. Personal controls

The following must be examined to evaluate the personal controls:

- Job descriptions reflecting individual responsibilities
- Requirement for job rotations
- Procedures that define user responsibilities
- Management of personnel accounts that reflect hiring, termination and transfer of personnel
- Execution of personnel screening before allowing them to access
- Approval and authorisation processes for access controls
- Controls over maintenance and repairs
- Authorisation of anonymous accounts

7. Programme specific controls

The programme specific controls must be recognised and configured on the basis of standard rules and specific requirements.

Answer: [b] Security controls for systems and programmes

Module:5

Reference No:M5128

Question: Which of the following aspects does evaluation of IT roles with regard to responsibilities in the test level of the Security Maturity Levels ensure?

- [a] Effectiveness of separation of duties, security roles and individual responsibilities
- [b] Security controls for systems and programmes
- [c] Modification of system documentation in case of any alteration to security controls
- [d] Third party review of the routine self-assessments

Module 5 - Tests - Security Maturity Levels - Part IV

The earlier articles discussed the five levels with regard to Security Maturity Levels. This article

elaborates the critical aspects to be considered in evaluating the criteria for the Test level.

Level IV: - Test:

A description of the critical aspects categorised topic-wise:

1. IT roles and responsibilities

Test and verify the following to ensure the adequacy of implementation of IT roles and responsibilities:

- Effectiveness of separation of duties, security roles and individual responsibilities
- Appropriateness of the division of key functions among responsible persons
- Responsible persons for support functions to ensure there is a distinct distribution of duties among them
- Alignment of IT security responsibilities into the organisational structure
- Review of separation of duties among personnel managing access control and those managing audit trail
- Review of related programmes with which the high-risk programme interfaces

2. Security Controls review

Check the effectiveness of security controls for systems and programmes, independent reviews, periodic programme reviews and operating system reviews. Also ensure that the recommendations made for improving the system are undertaken. Effectiveness of management's role in correcting deficiencies must be ensured. Temporary access must be authorised and tested. Third parties should review audit trails regularly and their recommendations must be followed. Automated tools used for audit record review should be checked. Ascertain that the consistency of security controls with internal IT architecture is reviewed properly.

3. Behaviour and documentation rules

Ensure the modification of system documentation in case of non-compliance to security controls. The behaviour rules must be consistent with the present conditions. Make sure that illegal usage is prevented and documentation regarding access is reviewed. Documentation showing the method of system usage must be checked and ensured. IT backup, emergencies and operational and security procedures also should be periodically tested. Ensure that the system displays the controlled log-on sign while accessing the systems.

4. Performance evaluation and feedback

Check whether the third party reviews the routine self-assessments. Review the testing of important security controls regularly. Third parties must check the security alerts and undertake corrective actions. Appropriate tests must be conducted to determine the effectiveness of the metrics developed for system security programme to improve performance, costs and benefits assessment of security controls.

5. Protection of critical infrastructure

To ensure effectiveness of third party review, test

- Critical operations, high-risk programmes and resources supporting them
- Critical assets and their inter-dependencies
- Existence of Critical Infrastructure Protection plan and contingency plan
- Critical failure points, recovery and communication plans
- Alteration of plans in case of any changes in assets must be appropriate
- Review and audit of interconnection agreements with business partners

6. Personal controls

Ensure that the following are tested and reviewed accurately

- Review of job descriptions, job rotation, user responsibilities
- Personnel screening before allowing them to access and under what conditions they could allow guest access
- Approval and authorisation of access to systems
- Controls over maintenance and repairs personnel
- High-risk programme access

7. Programme specific controls

Review and ensure that the programme specific controls are clearly stated and are consistent with the rules and requirements specified.

Answer: [a] Effectiveness of separation of duties, security roles and individual responsibilities

Module:4

Reference No:M5130

Question: Which of the following is not true of a network database model?

- [a] A network DB model specifies three types of record sets viz. system-owned, recursive and multimember
- [b] In a network model, two records of the same type can be linked
- [c] In a network database, a record can have more than one parent record
- [d] The parent records of a child in a network DB should not be of the same type

Module 4 – Network database model

Definition

A network database model refers to a collection of databases or records connected with each other in such a way that each record can be linked to every other record in the database using a relation (unlike in a hierarchical model). In a hierarchical model, the links have to maintain a level of hierarchy throughout the database (i.e. in form of parent records and child records). In a network model, even the child records (in the same hierarchy level) can be linked.

The Database Task Group, popularly known as DBTG conceptualised the network data model in 1971. In fact all the rules for data modeling in a network database are conceived from DBTG rules.

Every record in a network database model is analogous to an E-R model, i.e. each record has a number of fields (similar to an entity) containing only one data and a link can be formed between any two records (as an E-R relation).

Network database is an improvement upon the hierarchical model. The network model surpasses the efficiency of a hierarchical model in terms of data retrieval and reduction of data redundancy.

Structure and features of a network model

- Unlike the hierarchical model that uses a tree concept for organising data, a network database represents data in terms of logical records, each record having its own set of attributes. In fact it is due to this logical representation that a network data model (NDM) can form links between any two

records in the database using an E-R (entity-relation).

- Further, in a network database model, a child record can have more than one parent record. A network database model defines a record set (which refers to a set of related records) and a set type (which refers to a one-to-many relation between record sets)
- There are three types of record sets
 - o System-owned: The DBMS itself owns a system record set. All other sets are connected to the system-owned record set. It has a singular entry i.e. there can be only one system-owned record set for a particular database.
 - o Multimember: As the name suggests these record sets support multiple members or attributes. For example, a 'faculty' record set may store two different attributes viz. subject name and the number of teaching hours per week.
 - o Recursive: When the same record set plays the role of both member and owner, it is referred to as a recursive set. For example, the relation between a 'faculty' and 'principal' of an educational institution illustrates a recursive set as the 'principal' goes under the 'faculty' attribute.

The following diagram illustrates a conceptual model of a network database:

In the above diagram it can be observed that both the parent records share child record 3. Further, the records are linked in such that each record can reach every other record.

Integrity constraints pertaining to a network model

The two chief constraints in network data-modeling are:

- Two records of the same type cannot be linked
- A record can have more than one parent record, but cannot have more than one parent record of the same type. For example, a student may be studying different subjects, but cannot be enrolled for different courses.

Merits of a network database model

A network database model has greater

- Flexibility in handling complex relations
- Inter-operatability

Answer: [b] In a network model, two records of the same type can be linked

Module:4

Reference No:M5131

Question: Which of the following is not an integrity constraint for a hierarchical database model?

- [a] A parent can exist independently
- [b] No two child records at the same level can be linked
- [c] A child record may be deleted without deleting the parent record
- [d] Every root should have only one child

Module 4 – Hierarchical database model

Definition

A hierarchical database model as the name suggests organises data in a pyramidal structure. The data is organised in such a way that each data element bears a relationship with the elements above (parent) and below its level (child). Typically, a tree structure for data representation illustrates a hierarchical model. Structure of a tree and the manner of data organisation in a tree have already been discussed in the article on data structures.

The structure

Hierarchical database model starts with a single data element (or a database), which is known as a root. The root in turn is linked to one or more databases beneath it. Each of these data elements or databases is known as child. Each child is further linked to databases or data element below it. This way the whole database is organised in a top-to-down manner, starting from the root (a single node at the top) to the leaves (lowest level of data organisation, which is not linked to any further data elements).

The following figure illustrates a hierarchical database model:

Features of a hierarchical database

- The top most data element (a record or a database) is known as the root of the hierarchical model.
- The records at the lowest level are known as the leaves. Leaves do not have child records.
- In case a parent record has more than one child record, then the child records follow the order from left to right.
- The three chief methods of traversing a tree or a hierarchical database model are preorder, postorder and inorder. In preorder, first the root is processed and subsequently the child nodes are processed. In postorder as the name suggests, the child record is processed prior to processing the root. In an inorder traversal technique, first the left child is processed followed by the root and then the right node.

Integrity constraints

A set of rules framed specifically to assist a database designer to efficiently design an error free database is referred to as *integrity constraints*.

Some of the integrity constraints to be enforced before designing a hierarchical model are:

- A child cannot exist independently on its own without a parent, in a sense that a child record cannot be inserted in the database without inserting the parent first. At the same time, a child may be deleted without deleting the parent record. Further, child records should get deleted when parent is deleted.
- No two child records in the same level can be linked.
- A root is always independent in a hierarchical model. Thus, a root can exist without being linked to any child record.

Merits of a hierarchical model

- Hierarchical database reduces data redundancy and provides an efficient scheme for handling data.
- It is simple in structure and needs minimum number of data manipulation or database traversal commands thereby making it easier to be modeled (or designed).
- Databases that have predefined and constant child-parent relationship can be managed in a better way with hierarchical modelling.

Limitations

- Data access is complicated. This is because, for retrieving a data element, the user has to traverse all the way in to the hierarchy (i.e. from root to child and again to the lower levels) thereby, making the process cumbersome as the user needs to know the complete structure of the database before he reaches the requisite record. Hence hierarchy model is not user friendly.
- There is little or no data independence. This makes further upgrades and restructuring of the database literally impossible.
- Since no two child records at the same level can be linked in a hierarchical model, data retrieval schemes become inflexible.
- It is difficult to represent many-to many relationship in a hierarchical model.

Answer: [d] Every root should have only one child

Module:4

Reference No:M5132

Question: Which of the following is evaluated to ensure the critical infrastructure protection in integration level of Security Maturity Levels?

- [a] Job description
- [b] Job rotation
- [c] Personnel screening process.
- [d] Effectiveness of critical operations

Module 4 – Integration – Security Maturity Levels – Part V

Continuing the discussion on the levels of Security Maturity this article dwells on the fifth level, the critical aspects to be considered while evaluating the criteria for the Integration level.

Level V: – Integration:

The following is the description of critical aspects, which are categorised topic-wise.

1. IT roles and responsibilities

Separation of duties, accountability controls, security roles and individual responsibilities must be in accordance with the business lines and should not defeat the main purpose. The business must follow a standard business practice for the separation of duties among personnel managing access control and those managing audit trail. Other responsibilities include support functions and recognising the related programs with which the high-risk program interfaces are according to the accepted business practices. IT security responsibilities need to be incorporated into the organisational structure as per business policies.

2. Security Controls review

Regular review of security controls for systems and programs, program reviews, independent reviews and operating systems must be conducted. The effectiveness of management's role in executing security actions and correcting deficiencies should be ensured. Authorising temporary access must be in accordance with the business policies. Security program must contain the audit trail review and automated tools used for audit record review must be a standard business practice. Appropriateness of the security controls has to be checked.

3. Behaviour and documentation rules

Check the appropriateness of the rules of behaviour in the present conditions. Business practice must prevent the illegal usage of protected software. Password usage, its security and prevention of unauthorised access should be in accordance with the standard business practices.

Documentation showing method of system usage must be as per the set standards. Check the effectiveness of IT backup, emergency, operational and security procedures. Ensure a controlled log-on sign is displayed on the screen if an unauthorised person tries to access. A privacy policy must be available on the web.

4. Performance evaluation and feedback

The accuracy and implementation of routine self-assessment tests and corrective actions must be checked. Ensure the security control tests are in line with accepted business mechanisms. The appropriateness of security alerts, timeliness of corrective actions and its implementation must be determined to ensure that they are in accordance with the standard business practices. Evaluate whether they minimise the weaknesses and improve the security of IT. Ensure the application of metrics developed for system security program in the capital planning, budgets, and lifecycle planning and investment controls.

5. Protection of critical infrastructure

Evaluate the effectiveness of critical operations, high-risk programs and resources supporting them. Critical assets need to be identified and their inter-dependencies recorded in standard business lines. The Critical Infrastructure Protection plan and contingency plan must be properly documented and updated. Identifying critical failure points and establishing recovery and communication plans must be in line with standard business practices. Alteration of plans in case of any changes in assets must be appropriate. The overall business policies must contain the development, review and audit of interconnection agreements with business partners.

6. Personal controls

The following must be evaluated to ensure that they conform to the standard business practices.

- Job descriptions reflecting individual responsibilities, job rotations and user responsibilities
- Appropriateness of the IT accounts management.
- Appropriateness of the personnel screening process
- Necessity for allowing access before the screening process
- Correctness of the approval and authorisation processes for allowing access
- Controls over maintenance and repair staff
- Examination of guest and anonymous account

7. Program specific controls

Ensure that the program specific controls are configured on the basis of standard rules and specific requirements is a standard business practice. .

Answer: [d] Effectiveness of critical operations

Module:5

Reference No:M5137

Question: Which of the following is not a part of risk management process in ensuring the security?

- [a] Identifying acceptable risk
- [b] Protecting the evidence of vulnerability
- [c] Mitigating risk

[d] Transferring the risk that cannot be mitigated

Module 4 – 4Ps of Security

Security is not just restricted to virus detection, preventing corruption of data system and recognising theft. It includes identifying acceptable risk, mitigating risks and transferring those risks that cannot be mitigated. Thus this approach minimises employee productivity loss, business loss, corporate asset damage, and enhances customer confidence. These benefits can be derived only when appropriate defensive mechanisms are adopted.

Meaning of security

Technology is not the only constituent of security rather a part of security. It is actually a combination of **People, Processes, Procedures** and **Policies** (4Ps). In short it is a risk management process in totality. Any risk management process should address the four aspects viz., identifying the risk, accepting the risk, mitigating the risk and transferring the risk to customers and insurance providers. However, 100% risk mitigation and security is not possible for companies. Companies can achieve the desired level of security by maintaining proper balance between 4Ps. The following is the relationship between 4Ps:

1. **Security policy:** The standards, procedures and guidelines mentioned in the security policies are the set of guidelines for operating and protecting corporate assets. Hence people in the organisation should follow these to ensure risk mitigation.
2. **Process and technology:** Business processes and technologies are closely related. The former determines the set of actions and latter performs it. Hence technology must be chosen by considering the existing processes.
3. **Procedures:** The implementation methodology for processes and technologies is mentioned in the procedures. Systems usage, user privilege and the reporting process are defined in the procedures. The expected risk mitigation level cannot be attained if the people in the organisation do not follow these procedures.
4. **Policies:** Policies serve as a basic security foundation and define the accepted behaviour and course of action for people. When these policies are followed properly, risk mitigation issues are managed efficiently.
5. **Life cycle process:** Identifying valuable data, defining policy, executing security procedures and monitoring activities are several steps involved in life cycle process of information security. They must be continuously reviewed and altered according to the emerging threats.
6. **Regular training:** Change in the security requirements is a common phenomenon. Regular training to the people about the changing processes, policies and procedures is essential to achieve the corporate requirements.

An organisation may face other challenges despite efficient management of policies, procedures, people and processes. The following are few such problems and measures to be taken to avoid them.

- **Interoperability and integration between layers:** Security may be affected due to the integration and interoperability matters between layers. This can be solved through layered defence mechanism.
- **Identifying future threats:** An organisation must continuously undertake research and analyse the possibility of future threats in order to prepare for the same.
- **Lack of expert security consultants:** Businesses may find it a costly affair to recruit expert professionals every time in the ever-changing security environment. Providing continuous training to the security staff and hiring expert professionals can solve this.
- **Lack of support from corporate officer:** Involvement of corporate officer in the security policy is

one of the requirements for success. A Chief Security Officer who is responsible for security management can be appointed to solve this risk.

- **Lack of layered defence:** Business liability may arise in event the partner's site is affected through a distributed attack from the company's site. Layered defence mechanism will help safeguard the customer and partner's data.

Answer: [b] Protecting the evidence of vulnerability

Module:5

Reference No:M5138

Question: Virus hoaxes must be communicated to which of the following parties?

- [a] Employees in the organisation
- [b] Personnel dealing with the security aspects
- [c] Top management
- [d] IT personnel

Module 4 – Malicious Code

The term malicious code or Malware refers to the malicious programmes like viruses, worms, Trojan horses etc. Apart from destroying the physical assets it causes great damage to the credibility of the organisation. Hence the organisation must employ risk mitigation strategies that include detection service to identify the Malware. The need for detection service assumes significance in the light of:

1. **Corporate assets:** Corporate assets like network connectivity, servers and other important applications are exposed to the risk of Malware attack. The protection of these assets can be assured if there are detection services.
2. **Customer assets:** If the malicious code is transferred to the customer network through the company's network it may affect the credibility of the company and attract legal liability. Therefore it is essential to protect the assets of the customer.
3. **IT personnel:** Time of IT staff is more precious. They can concentrate on more productive work if there are proper malicious code detection services.

Training

But despite the availability of many security and antivirus tools, the number of companies that are affected by malicious code is increasing. Hence deployment alone will not do. It must also be followed by training. Malware can affect the systems due to employee faults, no matter what amount of detection services exists. To achieve the true benefits of detection technology, training programme to employees on identifying threats and safeguarding the systems and organisation is essential.

Training programmes must be guided by the following considerations. These must be made a part of organisational policies too.

a. Personal e-mail access: Attachments like palm pilots, greeting cards, adobe files, cartoons accompanying personal mails and those transferred between computers can become the sources of viruses. In order to prevent the attacks from these sources, the access to personal mails must be prevented. Companies should enforce the firewall rules that block the email traffic to the unauthorised servers.

- b. Reporting about viruses:** Any virus hoaxes must be directly communicated to the personnel dealing with the security aspects.
- c. Communicating security policy:** The security policy, which contains details about employees roles and responsibilities, malicious codes and policy enforcement mechanisms, must be communicated to the employees' through appropriate training.
- d. Downloading files:** The antivirus detection software must scan all the attachment files before opened them. The antivirus technology must be made understood to the employees.
- e. Vulnerable applications:** In case of vulnerable applications that were attacked earlier, employees must be given clear instructions to be careful while dealing with them.
- f. Virus signature updation:** Virus signatures must be updated immediately after identifying the malicious code. The delay in updation leaves room for attacks. Automating the process will reduce such chances.
- g. Antivirus software:** The client based antivirus software must be reviewed regularly to ensure that the automatic virus signature updation and antivirus scanning features are not turned off. In addition the company should have other security features like firewalls, IDS, gateway level virus protection, application level security apart from client based antivirus software.

Answer: [b] Personnel dealing with the security aspects

Module:5

Reference No:M5139

Question: Which of the following is an example of multinational transborder data flow?

- [a] Transmitting organisational regulations by the head office to its subsidiary offices
- [b] Email systems
- [c] Scientific exchanges
- [d] Consolidation dataflow

Module 4 – Trans border dataflow (TBDF)

Introduction

In simple words transborder dataflow refers to the data transfer across national borders. Such a transfer of information includes data storage, data processing and usage outside national boundaries and also information retrieval from a site outside a country. If data is routed to its destination, across international borders without getting processed, used or stored by the nations in between, then such a transfer is not a transborder dataflow. TBDF is contractual and proprietary in nature.

Such an information exchange process started due to rapid advancements in technology giving rise to need for information transfer across natural borders. Due to existing economic interdependence between various nations worldwide, data transfer gained international importance thus ushering in transborder data flow.

Typically, information pertaining to international trade, scientific exchanges, corporate interactions, government relations etc. comes under transborder dataflow. Web pages, information concerning financial issues, audio and video exchanges are few examples of transborder dataflow

Volume of transborder dataflow

The volume of data that crosses international boundaries is huge and cannot be measured directly. To get an approximate estimate of cross border dataflow, commercial pipes crossing national borders are counted and the data flow is measured after taking the bandwidths of these pipes into account. In fact there are a number of satellites each with an enormous bandwidth to handle over 15 terabytes of data each day.

Types of data under transborder dataflow

The various kinds of data under transborder dataflow are discussed as follows.

- **Personal data:** Information concerning criminal records, plane reservations, credit card transaction, online purchases etc. are some examples of personal data that come under transborder dataflow.
- **Business data:** Information exchange due to corporate transactions, deals, partnership, automation of financial institutions etc. are a few examples of business data.
- **Technical data:** Information pertaining to weather forecasts, geological experimentations come under technical data. Such data also includes information regarding financial analysis or market research influencing the international market. In other words, technical data are of economic importance.
- **Organisational data:** Also known as 'operational data', it is the information concerning corporate exchanges like international deals, partnerships, subsidiaries etc. Such data also take into consideration government relations between various nations.

Types of dataflow in TBDF

Basically, transborder information exchange occurs in four major fields, viz. in company's intranet, within different companies (or inter company exchange), governmental exchange, and information tracking. Based on the technology involved in data transfer, TBDF is of two types.

- **Unidirectional data flow:** As the name suggests, unidirectional data flow is one-way. Such dataflows are implemented for distributing information among various nations. Unidirectional dataflow are again of two types:
 - **Consolidation flows:** In this type of dataflow, all the information is gathered from subordinate offices. Thus, collecting information regarding credit transactions, updating finances of a company come under this type of data in which all the subsidiary offices report to the head office.
 - **Distribution flows:** Distribution as the name suggests involves broadcasting information across all the centres. E.g. When an organisation requires to inform the subordinate offices regarding financial reports, official instructions etc., it is known as a distribution dataflow.
- **Bi-directional dataflow:** In bi-directional dataflow both the communicating parties are capable of sending and receiving messages. These are of two types:
 - **Transnational dataflow:** When communication takes place between the clients in one country and the server in another, it refers to transnational dataflow.
 - **Multinational dataflow:** It is similar to transnational dataflow except for the fact that the number of servers involved in the communication is more than one. This is to say that users of one nation access servers in other parts of the world. E-mail systems in which users access the mail servers set up in different countries across the world is an example of multinational dataflow.

Answer: [b] Email systems

Question: A security mechanism follows the principle of "Security through Obscurity." This is a vulnerability that can be classified as:

- [a] Logic Error
- [b] Weakness
- [c] Policy Error
- [d] Social Engineering

Module 5- Viruses

Computer security business entails use of security bulletins provided by reputed sources such as the CERT (Computer Emergency Response Team) to keep up with the latest flaws in computers.

Such bulletins discuss "vulnerabilities" in software - be it Operating Systems, Applications and even Security software. These vulnerabilities give unauthorised access to hackers or at least violate the principle of data integrity. Computer security vulnerabilities are so numerous that entire web sites are built around them, but the types of vulnerabilities can be restricted to just four.

- **Errors in Coding Logic:** These errors are caused by improper coding techniques and may give access to confidential data through a shortcut. Hackers first look for this kind of vulnerability in software, since it is the easiest to exploit. Examples are:
 - Protocol Design Flaws
 - Forced Trust Violations
 - Operating System bugs
 - Application coding errors
- **Weakness:** When a security mechanism in place, can be effectively bypassed, it is called as a "weakness." For instance, the familiar "security through obscurity" principle is actually a weakness. According to this principle, if vulnerability is hidden well, then the system can be assumed to be secure. Examples are:
 - Obscure Security
 - Improper passwords and password policies
 - Encryption
 - Eavesdropping
- **Social Engineering:** The vulnerability least known and understood, social engineering refers to the mechanism of using social skills to get the required information. Examples are:
 - Theft
 - Espionage by employees
 - Information fishing
 - Sabotage
- **Policy flaws:** Flaws in company policy form the last category of vulnerabilities. Examples of such flaws could be: non-removal of accounts of former employees, non-provision of adequate data backup policies. Another common policy flaw is to let hackers off the hook, which makes all other measures a waste. Areas of potential abuse are:
 - Physical security
 - Personnel security
 - Information sharing
 - Data Protection

Vulnerability is characterised by five elements, as detailed below.

- **Fault:** It provides the reason for the existence of the vulnerability and may even detail how it was created. For instance, the actual logic or other error causing it would be stated.
- **Severity:** This characteristic provides the intensity or level of security violation that has occurred due to the vulnerability.
- **Authentication:** It describes whether the hacker had to authenticate himself with the target computer before using the vulnerability.
- **Tactic:** This refers to how the vulnerability was exploited, since there might be different ways to exploit a flaw and hence a description of the actual method might be useful in tracking down a potential attacker.
- **Consequence:** It describes the effect of the vulnerability in terms of the increase in privilege an attacker gains by exploiting it.

Although logic errors and weaknesses seem similar, the basic difference between the two is that logic errors arise due to ignorance in secure coding techniques, whereas weaknesses are due to poor implementations. Further, social engineering differs from both of them in the sense that a human element is involved in it.

Note: Social Engineering is covered in detail in other articles.

Answer: [b] Weakness

Module:5

Reference No:M5141

Question: ----- occurs when a program has the opportunity of accessing and modifying another program's data or even its operations

- [a] Race condition
- [b] Synchronisation errors
- [c] Serialisation errors
- [d] Condition validation errors

Module 5- Vulnerability

As described in the earlier article, even one attribute of vulnerability amounts to a fault. In fact, vulnerabilities exist due to faults. Faults are of two kinds:

- Coding faults
- Eminent faults

Each of these categories can be broken down further. They are discussed in detail.

Coding faults

Coding faults are a result of logical errors while developing the programme. This is primarily due to improper specification of the objectives of the program. An important characteristic of this type of fault is that it would continue to occur, irrespective of external manipulations.

Coding faults can again be divided into two, *Synchronisation errors* and *Condition Validation errors*. The former is discussed below, while the latter is discussed in another article.

Synchronisation errors

These occur due to lack of precise coordination between objects operated upon by the program. In other words, if two events do not occur simultaneously, it gives rise to a small security hole. For instance, when a user types his password into a login dialog box, the keystrokes should appear as “#” or some other character immediately. If the actual characters are displayed even for a second before conversion, then any person looking at the screen can easily get to know the password.

- *Race conditions:* A race condition occurs when a program has the opportunity of accessing and modifying another program's data or even its operations. For instance, if a program creates a file, another program may be able to access it before the file can be “locked”. . Then a race condition is said to exist between the time of file creation and locking the file.
Temporary file race conditions are created when temporary files are created by applications. These temporary files are usually placed in directories that have full read/write permissions and hence it is easy for a malicious user or program to access these files. This access can open up vulnerability and lead to privilege enhancement for the attacker.
- *Serialisation errors:* It is possible for expert hackers to “hijack” existing network connections by using errors in serialisation (synchronisation). “Network Packet Attacks” is an example of misusing serialisation errors to gain control of a user's network connection. The network data is split into packets by the network protocol and is serialised, meaning that every packet contains information about the order of decoding the packet at the destination. Typically, packets reach the destination independent of one another, So, each packet contains a sequence number that states the order in which it has to be processed.

An example of such a sequence number would be the TCP sequence number, present in the TCP packet header. When a packet has to be sent, this sequence number is first initialised to a random value, but subsequent sequence numbers are just fixed increments of the first. So, it is possible to predict the next sequence number by carefully observing the packets. Once the sequence number has been guessed, then the attacker can create his own packet and fool the destination into believing that this packet belongs to the original set.

Answer: [a] Race condition

Module:5

Reference No:M5142

Question: A network attack does not involves which of the following step?

- [a] Network investigation
- [b] Network management
- [c] Access gaining

[d] Escaping

Module 5- Network Attack Tools

There are innumerable software tools that offer protection against hacking. I.e. to A thorough understanding of the functioning and usage of such tools can prevent outward incidents. In the same vein, it is also necessary to understand the hacking methodology and tools employed by the hackers.

An attack involves the following steps:

1. **Network investigation:** The first step in an attack is getting information on the features of network and obtaining its structure. Using various tools, attackers capture information such as domain names, firewalls, protocols and platforms in usage, IP blocks and network infrastructure.
2. **Access gaining:** Network access can be gained by cracking the password, sniffing, through physical access and default accounts, or using advance methods like TCP hijack. Invader can select a method depending upon the nature of the environment and type of the attack.
3. **Escaping:** With the information about the network and the means to gain access to it, an invader can easily attack. Thereafter the hacker makes an escape, which is the last step in the process.
 - The first thing in the escaping process is to eliminate the traces by using tools like rootkits.
 - An attacker tries to escape in the guise of a legitimate account on the server.
 - Setting up backdoors: It can be an attack through Trojan Virus or legitimate account creation.

Invaders categorise the tools in to 3 types, those used for investigation, access gaining and escaping. Security professionals on the other hand categorise them into defence in-depth tools and personal security assessment tools. The following is the list of some of the tools. The list not exhaustive though.

Argus: It is a network transaction-auditing tool that produces the status records of network traffic by studying the network datagram.

Asmodeous Port Scanner (WebTrends) for Windows NT

Asax: An Advanced Security audit trail Analysis on Unix.

COPS (Computer Oracle and Password System) version 1.04: scans and sometimes rectifies the weaknesses in the systems.

Fremont: It helps in identifying crucial network features like gateways, hosts, topology etc.

Internet Security Scanner (1.21 and 1.3 versions): It scans the UNIX system to identify the security holes.

NESSUS Alpha 2 -fix 4: It is a security audit tool for Linux

Nss: It examines both individual remote hosts and complete host subnets.

SAINT (Security Administrator's Integrated Network Tool): It provides the information on security flaws like wrongly configured services, bugs in the networks or system and report the data by analysing various network services.

SARA 2.0.5: It is a security audit tool.

SATAN (1.1.1. version): A tool used by system administrator to identify the well-known vulnerabilities in the systems by analysing networks and scanning systems.

Tiger (2.2.3 and 2.2.24 version): Scanning Unix system with a set of scripts provided by Tiger can identify security problems.

Web Trend Security Analyser: Security vulnerabilities, which give rise to exploitation of intranet, extranet and Internet, are identified by analysing the systems regularly and are fixed with the help of Web Trend Security Analyser.

Answer: [b] Network management

Module:5

Reference No:M5143

Question: Which of the following must be considered first while making security investment decision?

- [a] Aspects that provide low security and involve low cost
- [b] Aspects that provide high security and involve low investment
- [c] Aspects that involve high cost but provide least security
- [d] Security aspects that involve high cost and provide high security

Module 5- Security investment

Investment in digital security has been an undesired issue for many financial executives. Therefore, security department must properly communicate with them and draw the required budget for security investment.

Interpreting the terms

Authentication, white-box application and triple DES encryption are strange terms to finance professionals who often deal with revenues, profits, operating costs and cost of goods sold. Hence, it is essential to translate the security related terms into opportunity costs and benefits.

Method

A security policy first identifies the gaps in the existing infrastructure by running penetration tests with the help of consultants. It then finds a way to plug these loopholes. Thus, this reactive method of patching is a continual process, increasing the expenditure. Moreover, this approach does not ensure corporate security fully nor presents a precise view of security risks.

Therefore, instead of undergoing a regular penetration testing, companies must identify areas that need protection and those that do not. Some times avoiding security measures in certain areas may be beneficial for an organisation. This could simply be because their security costs are more than the cleaning up costs.

Identifying the needs

Protection of networks against undesired intruders is essential. The current design of networks makes this rather difficult. Also, transparency in operations and use of new technologies in electronic communication increases risk. Storage of applications on third party servers has further complicated the digital security.

Hence, security officers must be well aware of the developments in technology and emerging business priorities so as to align the security investment with business objectives. Investments made in different activities and shortcomings that still exist must be identified. This helps in planning a meaningful security investment.

Counting returns

An important responsibility of security officers is to measure the return on investments made in technology. This is possible only when economic return of investments is identified and security metrics are defined. Easier said than done. Security analytics, however, can help in measuring the return on investment (ROI) in these activities.

The returns on security investment are measured in terms of opportunity cost-the cost incurred on implementing the security measures versus those if not implemented. Companies are severely affected by the cost of not executing security measures. These include the cost of bringing the business to a normal condition, lost customers and their confidence and the cost of falling stock prices.

Investment decision

Investing decision must consider the following: -

- Primarily, companies must concentrate on aspects that provide high security with low investment. Such prioritisation ensures maximum benefits.
- Low cost aspects like application security, whose effect is low, must be considered for investment.
- Security aspects involving high investment like software development are generally in the nature of long-term and require the cooperation of other departments. This is more related to administration than security.
- The high cost security measures that provide least security must be the last priority for companies. Further, it is at the will and capability of the company.

Answer: [b] Aspects that provide high security and involve low investment

Module:5

Reference No:M5144

Question: Few independent systems can bring to a halt a large network through

- [a] Effect of the combined bandwidth
- [b] Trojan attacks
- [c] The combined scale of individual computers

[d] All of the above

Module 5- Distributed Denial of Service

Distributed denial of service or DDOS is an extended version of the denial of service attacks. The difference between the denial of service and the distributed denial of service attacks can be explained with a simple analogy.

If only a single line of telephone was available at an information desk, and some prankster continuously calls the single number, so as to not make it available for genuine users, it amounts to a denial of service attack.

Similarly, if there existed, say some 50 such lines and a co-ordinated gang of say 70 members call the number at a same time, this would render all the 50 lines unavailable to genuine users at that point of time. This is distributed denial of service attack.

Such an attack is carried out on large computer networks, rendering the entire network ineffective.

How is a distributed denial of service attack carried out?

Here the bandwidth capacity of a few numbers of independent computers can be used to disrupt the services provided by even large networks for instance the CNN. This has been explained in the following example:

Lets assume the attacker has around 500 machines each with a 256Kb/s of upstream bandwidth. So even if 500 machines together can generate $500 \times 256 \text{Kb/s} = 128000 \text{Kb/s}$, this is equal to the size of 42 TI lines a considerable bandwidth. This can be used to target even a large network like yahoo.com.

Mode of attack

The main idea of the attacker is to make people run the programs of the attackers choice. These programs will lie dormant, like zombies and once the attacker sends the signals, it will start generating traffic to a particular target.

The most commonly used method to send such Programmes is to package it as "Trojan horse". These are innocent looking but secretly malicious program that is sent to unsuspecting people. Since most of the time lay users do not think twice about downloading such executable programs from unknown users, these are sent to them.

Once the attacker activates the Trojan Programme, it registers itself somewhere. Sending TCP/IP packets to popular destinations does this. These registration messages give out some important information like IP address of the zombie machine, the bandwidth between the zombie and the selected target.

Once a machine is infected with such programs it always stays affected. And all that the attacker needs to do is to send a trigger command to the affected machine to attack the pre-selected target. The Trojan programme may also try to multiply itself. Many such Programmes may provide more command of the affected machine.

Means to protect from such attacks

Although it is difficult to prevent such attacks, it is not impossible. There are two issues that need to be considered here, one to prevent one's network from such attacks and the other to prevent from being used in such attacks

To prevent the network from being attacked is to use ingress filtering. This filters out the junk packets.

In case of home users and small network users, it is important to watch the network traffic. If the networks register a higher activity when actually the system has not been used much, then it might indicate such attacks.

Answer: [d] All of the above

Module:5

Reference No:M5145

Question: ----- is a component of identity management infrastructure

- [a] Identity directory
- [b] Identity authentication
- [c] Authorisation
- [d] All of the above

Module 5- Identity Management

What is identity management?

Identity management or managing the IDs of the employees in any organisation is one of the tasks of the security administrator or system administrator. This task forms a part of effectively management of access permissions. This task assumes more importance in complex integrated environments. Automated software packages are available in the market now to effectively manage the identities in an organisation. For instance the Microsoft Metadirectory services is one such product available in the market.

Why identity management?

Gone are those days when only a few selected people had access to the corporate network. Organisations now have a more distributed information network, which is open to almost everybody. The main idea now is provide employees secure access to information they require anywhere at anytime. This objective brings forth two issues - security and productivity. The issues that needs to be considered during identity management are threefold:

- **Security:** Only authorised users have access to the right information.
- **Complexity:** Organisations are run on a variety of platforms. And now the sizes of the employee users have also increased. This makes creating a common user policy a complex issue.
- **Cost:** Although security is an important concern, the cost factor will have to accounted for . A balance has to be achieved between the cost of maintaining such policies and

security issues.

Identity management infrastructure what is it?

Constructing an identity management infrastructure involves development of a user and resource management system as well as security administration. An identity management infrastructure contains the following components

- Identity directory
- Identity authentication
- Authorisation
- Rights management

Identity directory

Identity directory is a storehouse of information about users of computer resources and the details about the resources the users are authorised to use. The identity store might house the entire details about the users profile. It could be name, job profile, access rights to resources and data like passwords. It also has information about identity of computers, applications and other resources. This directory acts as a focal point for administration of user accounts, security policies etc.

Identity authentication

The identity source house is integrated with the security infrastructure of the operating system. The user will require only a single authentication means to access the client workstation and that in turn will grant access to various resources as stored in the identity directory. The authentication mechanism could be anything from simple passwords to biometric passwords or certificate based authentication.

Authorisation

Each object has an owner, who is capable of granting access permissions. Once a user has been authenticated, the access control lists determine what resources or objects this user can access. These access control lists are stored in the identity directory.

Rights management

This involves the administration of individual rights. This pertains to granting of rights to individual users, revocation of rights and review and upgradation of the rights.

Answer: [d] All of the above

Module:5

Reference No:M5147

Question: Duplicate payments is an example of ----- type of fraud profile

- [a] Static
- [b] Dynamic
- [c] Both static and dynamic
- [d] None of the above

Module 5- Data mining and fraud detection- part 2

This is the second of a two part series on data mining and fraud detection. In the first part we

explained the various concepts related to fraud and fraud detection to assist the fraud investigator. In this part we have described fraud-profiling, types of data and automated fraud detection tools.

Fraud profiling

Fraud profiling can be defined as the characteristics of the key elements for transactions. These key elements could be values, frequencies, volumes etc. Fraud profiling provides assistance in the creation of automated routines to verify these profiles.

Benford's law and breakpoint clustering are also type of fraud profiling. There are two kinds of fraud profiling - dynamic and static. The above mentioned are examples of dynamic fraud profiling. The other types of dynamic fraud profiling include:

- Round value invoices
- Round value expenses
- Consecutive invoice numbers for the same supplier over a period
- Pre-paid invoices
- Duplicate payments

The other type of fraud profile is the static fraud profile. This involves the analysis of information contained in the supplier's master file. An extreme case of static fraud profile is the one where an employee sets up a bogus supplier in the vendor's master file and a bogus invoice is received from the bogus supplier. One of the simplest ways to identify some dormant suppliers accounts is to inform the accounts department of change in details. The bogus supplier's reply may contain any or some of the characteristics:

- He might give an invalid VAT number
- He might give a telephone number of his residence mobile or a payphone
- Domestic resident addresses
- Addresses of accountants, company formation agents that may indicate that the company is newly formed

The above examples are ways of making use of internal databases to detect fraud. Similarly external databases like details of mobile telephone etc. can also be used for fraud detection

Automated fraud detection engines

It is now possible for companies to develop their own automated fraud detection engines at a reasonable cost. Even the spreadsheets and normal databases can also be utilised for such purposes. But there are some limitations such as

1. Excel can import only a limited number of records.
2. Data within spreadsheets and databases can be easily tampered without leaving any audit trail. This may defeat the whole purpose of the exercise.
3. An audit log should always be present within the fraud detection engines so that all results can be verified independently and authenticated.

A specifically designed audit package can be designed which contains all these features. The audit package should be able to perform the data analysis, statistical analysis, number crunching, static and dynamic fraud profiling. And also it should be able to depict visual representations of relationships between key components of the database. It should also depict a link analysis- for

instance the match between the addresses of vendors master file and external database of residential addresses.

Other tasks that the fraud detection system should do would be

1. Comparisons
2. Check for duplicates
3. Test Vat numbers for validity

Answer: [b] Dynamic

Module:5

Reference No:M5148

Question: In Benford's first digit law, the digit "1" will appear in ----- frequency than digit "9"

- [a] Lower
- [b] Higher
- [c] Similar
- [d] Higher or similar

Module 5- Data mining and fraud detection- part 1

The concept of data mining has been around for some time. Presently a lot of literature is available on the subject. This includes the technique of fraud detection with regard to data mining. Various areas with regard to fraud detection include fuzzy logic, neural networks, pattern recognition systems, genetic algorithms etc.

The background

Most of these systems were in the beginning developed by universities, research organisations and other such establishments. These were developed with an intention to identify patterns in the vast amount of apparently random data. This is somewhat similar to particle physics. Here the investigator will analyse the company data like invoice files, movements of shares in stock exchange to check for the involvement of a fraudster, if any. Looking for an apparent trail through some patterns in an otherwise random nature of data can do this.

However in practice, such statistical data-mining techniques cannot always easily be used in real life situations. And moreover the cost of implementing such systems is so high that only a few organisations are able to use it. These factors apart, many large organisations still rely on statistical analysis in environments such as credit card transactions monitoring, stock exchanges, telephone billing systems etc.

The objective of this article is to provide the readers the details of various fraud investigation techniques. Most of the tools are available in the market off the shelf. But such systems can also be developed internally in the organisations for a lower budget.

The fraud detection systems

Before embarking on the development of a system, it has to be reasonably established that a

fraud exists in the organisation. Most of the surveys conducted in this regard show the involvement of an insider. This is not surprising given the complete knowledge of the internal control systems and the day-to-day operations that he holds.

The main objective of the fraud detection is not just to prove the existence of the fraud but also provide tangible proof of the crime.

Development of a system

The first step for implementation of a fraud detection system is to consider the different types of fraud that could exist in the organisation and develop a fraud theory.

In most organisations, fraud is bound to be discovered by the purchases department. Purchasing officers are always susceptible to the abuse. In many cases it can be seen that certain patterns signify a problem. And often these patterns are obscured by inflated budgets, poor reporting mechanisms etc. Although the type of relationship may vary from organisation to organisation the overall trends remain the same. For instance it can always be seen that there will always be large number of low value invoices and few number of high value invoices.

One such instance is the Benford's Law. This law states that 1 will appear approximately 30% of the time as the first digit whereas 9 will be the leading digit (pl. check) only 4.6% of the time. Any other unusual behaviour will alter this natural pattern.

Another type of fraud is the abuse of financial level of authority. These authority levels can be easily overcome by having two or more low valued invoices. If this situation continues, a cluster of invoices will exist just below the authority limits. This can be uncovered by looking for invoices from the same supplier, same date invoices, invoices with consecutive numbers etc.

The rest of the fraud profiling has been covered in part two of this article. In part 2 we have covered the types of fraud profiles and the features of automated fraud detection engines.

Answer: [b] Higher

Module:5

Reference No:M5149

Question: Which of the following policy provides strategic direction to the organization?

- [a] Regulatory policy
- [b] Program policy
- [c] Advisory policy
- [d] Informative policy

Module 5- Non-Technical Aspects of System Security

Security is often viewed from the technical aspect. But there are several other aspects that must be taken into consideration for the success of a security - policies, organizational structure and the like.

Policies

Policies are the rules for security to ensure the desired protection level of information system. Security professionals must clearly understand the security policies. The following are the different types of policies:

- **Program policy:** It provides strategic direction for an organisation by allocating resources and designing the hierarchical structure.
- **Issue-specific policy:** Policies that address specific issues like contingency planning or password management.
- **System specific policy:** Policies framed specifically for a particular system.
- **Regulatory policy:** Policies that are required under legal obligations.
- **Advisory policies:** Unlike regulatory, these policies only advice the organisation on various aspects.
- **Informative policies:** Provides information to readers.
- **Management policy:** It states the support from senior management for enterprise-wise security.

The following are some of the guidelines in developing a security policy:

- Identify the assets including all operating systems
- Classify the information into different levels on the basis of standards
- Identify the security policy impact on employees and train them
- Monitor the policy continuously

Security policy implementation

The security policy implementation involves three stages:

- **Preparatory stage:** In this stage, the roles and responsibilities are identified, network vulnerabilities and the level of risk is determined. Further, a security team structure, which frames and implements the security policy, must be created.
- **Prevention stage:** Changes, if any, must be incorporated in an organised manner. Continuous monitoring must be ensured depending on the level of risk.
- **Response stage:** In this stage, proper reporting structure must exist for handling the security violations, if any. Policies should also contain the procedure for restoration. Finally the policies and practices must be reviewed.

Purpose: Readers must be informed about the purpose of the policy.

Background: Complete details about the problem inception and vulnerabilities must be described in the background section of the policy.

Roles and responsibilities: The roles and responsibilities of CIO, trainers and employees must be clearly stated.

Due dates: Effective data and expiry date of the policy must be clearly stated.

Standards and guidelines: Policies can be implemented by defining the standards, guidelines and procedures properly.

Components: Physical security, personal security, remote access, contingency planning, configuration management, virus protection, encryption and backup are some of the components of

a security policy.

The hierarchical structure of the security function

1. **CIO:** CIO is the ultimate decision maker and the person responsible for implementing security policies.
2. **Network plans and policy:** Network Infrastructure Section and Information Assurance Section manage the infrastructure aspects and security aspects respectively. These sections distribute the company wide policies to all.
3. **Network operations:** They are responsible for providing technical assistance in policy implementation.
4. **Managers at local branches:** Day-to-day operations, staffing, implementing further security measures are the responsibilities of these managers.

Answer: [b] Program policy

Module:5

Reference No:M5152

Question: Which of the following is not correct with regard to risks of client/server?

- [a] The successful implementation of the client/ server depends on its development
- [b] RAD does not provide for the flexibility of the system
- [c] Workstation without implementing security products and features provides the required security
- [d] The best security product will be one that authenticates the user and also encrypts the sensitive data

Module 5- Security of Client/ Server 1

Client server is the split of the application's processing capabilities over multiple processors unlike the mainframes where the processing is done at one central point. Each processor works independently but at the same time relies on other processors to complete a task. The main advantage of implementing the client server is

- Reduction in cost
- Empowerment of the users

Client sever is beneficial only when the network traffic between the machines is reduced and proper security features are implemented to ensure that access to the users is on need to know and need to do basis.

In this article we deal with the risks that exist in a client/ server and ways to mitigate the same.

Development of client/server

Risks

1. The success of client/server rests on the skills of its development team. The development

team may not have the required expertise to handle the new products, new operating environment, network and the like which may give rise to risk.

2. The second risks will arise due to the design method adopted by the development team. RAD (Rapid Application Development) is used for the development of client/server. With this method though the application can be developed quickly it will not allow for easy adoption to new hardware, software or change in organisation goals.
3. The next is the library controls over objects.

Mitigation of risks

1. The risks associated with lack of skills of the development team can be mitigated by having a peer review of the client/server application design by internal or external experts. This entails the development of a better design and cross-training of experience.
2. To mitigate the risks faced by deploying RAD it is necessary to define a data classification method for all the data that flows in the organisation. The data can be classified into corporate data, divisional data, departmental data and the local data. The hierarchy will be corporate, divisional, department and then local data. This will help the management to easily review the risks assessment of an application. This classification can also be implemented to save application objects in a repository.
3. The objects such as menus, programs, scripts and windows are stored in both source and object form. In the user environment only the object version should be present. To check this version, check-out/check-in controls should be used for updating the objects. This ensures integrity. The integrity of objects can also be verified by implementing checksum total feature of the system when the workstation communicates with the file server. The source code should be placed in an offsite library.

In the next article we will deal with other risks of client/server.

Answer: [c] Workstation without implementing security products and features provides the required security

Module:5

Reference No:M5153

Question: Which of the following is "TRUE" with regard to security of client/server?

- [a] The user id and password of the client should be communicated to all the users
- [b] Absence of segregation of duties can be compensated by audit of privileges of operating system
- [c] There exists no risk in a client/server environment
- [d] None of the above

Module 5- Security of Client/ Server 2

Client server splits the processing of an application over multiple processors. Each processor works independently but at the same time relies on other processors to complete a task. The client sever is advantageous only when the network traffic is minimised between the machines and appropriate security features are used to restrict the access of the users to the entire system.

Part 1 of the article dealt with risks of development of client/server. In this article we deal with risk of network wire and file server.

Network Wire

Risk

Multiple processors that are involved in the processing in the client/server must communicate with each other. This means that data such as user id and passwords, files and the other data for any activity are available in a clear text form in the equipment. A hacker can easily obtain this information. Encryption of the user id and password will not serve the purpose as the actual data still travels over the network, which can be captured by a hacker and decoded.

Mitigation of risk

The above risks of clear text messages can be reduced by implementing network diagnostic tools such as LANalyzer from Novell. This tool helps in identifying whether user id and password can be captured in clear text form when a user on a workstation signs on the file server of the mainframe computer.

Risks can also be reduced by implementing challenge and response system that authenticates the user or any product that is based on Kerberos features.

File Server

Risk

The main risk in a file server is that the system administrator has control over the entire system. He can easily alter any data, which may not even be captured in logs.

Mitigation of risk

1. To compensate for absence of segregation of duties audit of privileges of operating system is required. This can be performed by determining the administrator of file server. E.g., the ROOT authority for UNIX. The next step will be to review the application files and directories to determine who has similar authority to operate anything in the file server environment.
2. Risks can also be mitigated by reviewing whether all the users have authority corresponding to their job responsibilities.
3. Review of security controls for sign-on attempts, password creation, ageing of passwords, violation logs and the like should also be called for.
4. Implementation of vigorous audit checks on the file server for vital files to determine if they have changed since the previous audit. Examples of such files are program libraries, file of valid users. Check sum is an example of such audit check. It compares the hash total of the file's contents with the check sum taken earlier.
Even after implementing the measures administrator can still turn them off. For this surprise audit should be carried and security products should be implemented.

Answer: [b] Absence of segregation of duties can be compensated by audit of privileges of operating system

Module:5

Reference No:M5155

Question: Which of the following will help to mitigate the risk of network components with regard to the security of client/server?

- [a] An authentication mechanism attached to each device
- [b] Planning and testing contingency measures
- [c] Verification of application data tables
- [d] None of the above

Module 5- Security of Client/ Server 4

Client server splits the processing of an application over multiple processors. Each processor works independently but at the same time relies on other processors to complete a task. The Client sever is advantageous only when the network traffic is minimised between the machines and appropriate security features are used to restrict the access of the users to the entire system.

Part 1 of the article dealt with risks of development of client/server, Part 2 dealt with Network Wire and File Server, Part 3 dealt with risk of workstation, DBMS and mainframe connection. In this part we deal with other aspects of security.

Network Components

Risk

The client/server environment involves the use of bridges, routers, gateways and the like. All these interfaces are stored on SNMP (Simple Network Management Protocol). Each device is protected through the use of user id and password. The Administrator due to difficulty in remembering the password of so many devices would keep a default user id and password for all devices. A hacker who gains access to the user id and password has the entire network open to him.

Mitigation of risk

1. An authentication mechanism can be attached to each device and SNMP agent within the device can be used to log all failed login attempts.
2. A separate device can be used to encrypt all the data that passes through the network.
Example Network Encryption System from Motorola

Administration

Risk

Since the entire administration of client/server File Servers is in the hands of an individual, the management must decide on the risk that it is willing to accept. This decision will be based on the sensitivity of data.

Mitigation of risk

1. Audit trails should be established, logs should be maintained to check violations. Audit should be conducted to ensure that appropriate controls are built
2. The role and responsibilities of System Administrator should be clearly defined.

Dial up

Risk

The client/server environment has given the user the mobility to access the network even from remote places.

Mitigation of risk

No user should be allowed to access the network remotely without approval. The dial up connections should be user id and password protected. Security devices such as call back or smart cards should be used to ensure that only authorised users can remotely sign on. Devices such as communication gateways of Cisco can also be used to authenticate the users based on an access control list.

Contingency Plans

Mitigation of Risk

The effective functioning of the client/server environment will also depend on the effective and tested contingency plans.

Conclusion

Client/server has helped the management to save on the processing cost. But at the same time the risks have also increased. Management must try to mitigate these risks by defining the accepted level of risks and implementing appropriate security measures.

Answer: [a] An authentication mechanism attached to each device

Module:5

Reference No:M5156

Question: Which of the following is not related to application security?

- [a] Data integrity of application data
- [b] Data origin authentication of application data
- [c] Replay detection of application data
- [d] User identity confidentiality

Module 5- Third Generation (3G) Security Architecture

The 3G architecture defines five different sets of security features:

1. Network access security: It provides the user with secure access to 3G features. This could include authentication of users, confidentiality of data on the Network access link, Data integrity and mobile equipment identification.
 - User identity confidentiality: The user's confidentiality is assured through Temporary Mobile User Identities (TMUI), which is applicable in the local network only. The TMUI management takes place during the location (of the user) updates. The transmission of International Mobile User Identity (IMUI) over air-interface is done only in encrypted form.
 - Authentication of users: This is done by mutual authentication between the user and the network using a secret-key called K.
 - To preserve the confidentiality of user over the access network, ciphering algorithms are used between the mobile station and the serving network.
 - The data signalling in the network is very sensitive and demands preserving its integrity. For this purpose an integrity algorithm is used with an Integrity key, IK. The Integrity Key is established as a part of AKA process.
 - To identify the mobile, International Mobile Equipment Identifier (IMEI) is used. This uniquely identifies the mobile equipment.
2. Network domain security: This feature is especially important when sensitive signalling information is required to be exchanged between different network elements. It helps in imparting entity authentication, data confidentiality, data integrity, fraud information gathering system and the like. It has a 3-layered architecture:
 - Layer I: A secret key based on asymmetric cryptosystem is used to validate a symmetric session key for each direction between two networks X and Y. This

- layer is not required if the two networks belong to the same operator.
 - Layer II: The symmetric key obtained from the previous layer is distributed in each network to the appropriate elements. The distribution of key is done in a very secured way.
 - Layer III: In this layer a symmetric encryption algorithm is used along with the distributed symmetric key for securely exchanging the sensitive data between network elements of one operator or different operators.
3. User domain security: This feature provides secure access to mobile stations. This is done through the secret key stored in the USIM (Universal Subscriber Identity Module, it's a smart card used in 3G mobile phones)
 4. Application security: The 3G systems facilitate third party or the operators to create applications. So it becomes imperative to secure messages that are transferred over the 3G networks to applications on USIM. To ensure the security of messages following features are provided.
 - Entity authentication of applications
 - Data origin authentication of application data
 - Data integrity of application data
 - Replay detection of application data
 - Proof of receipt
 5. Security visibility and Configurability: Security features should essentially be apparent and visible to the user.. This could be done in many instances such as indication of level of security, indication of the network-wide encryption etc.

Answer: [d] User Identity confidentiality

Module:5

Reference No:M5157

Question: Which of the following is false with related to Spyware?

- [a] It is used to gather information related to users hobbies and interest
- [b] It is used to provide information to user
- [c] It is used to collect the user's system configuration
- [d] It is not obvious to User of its functionalities

Module 5- The Dangers of Spyware

The spyware is software with dual purpose and is defined as software applications, which sends user related information to the publisher through the Internet. The spyware doesn't function secretly but at the same time it's not obvious to the user . This is because although the information about its functions and features are already described in User License agreement, most users do not take care to read it.

The spyware can be of various types. They are generally available for free download on the Internet in the form of general use utilities and tools. Some examples are Download utilities, Games, Media players, Accounting software etc. The information collected depends on the type

of spyware used. The information collected could be system configuration of the user, user's browsing habits, users likes and dislikes etc. The spyware is certainly not a backdoor Trojan horse that secretly collects the information in the system and sends it back to hacker.

Operation of spyware

The information gathered by spyware differs from software to software. Suppose a person downloads software, which increases the speed of downloading from the Internet. The user may be asked to fill in some information, which could ask details like name, age, gender, education background and the like. The user is asked several questions as he browses and the questions gradually become more focused towards his tastes. After some time the software gathers information about various habits of the user. The user may certainly not be aware of all these happenings.

The nature of information gathered depends mostly on the information gathered. Gathered data could include type of data, statistical data and the like. At times the programs would give advertisement after correlating the data gathered. The data is given a unique identification at the spyware publisher in order to link it to specific installation. This unique identifier is stored in the users computer.

The unique identification can be done in two ways. One generating a GUID (Globally Unique Identifier) and the other by keeping a cookie on the hard disk. The cookie is installed during the installation of the spyware program. It contains data used by specific programs, the user name, computer specification and like. A GUID is generated with data, which is unique to computer.

Since the unique identifier is also sent along the information to spyware publisher, the publisher is able to know exactly what the user is looking for. Thereby sending the next set of advertisements depending on the analysis of user's taste.

Knowledge of declaration

The spyware programs have End User License Agreement (EULA) just like any other commercial software program. In this case the EULA also describes the actual functions and the purpose for, which the software was made. But in majority of cases the user is never able to know them. This is because the content is written in such a manner that it becomes difficult to derive the exact meaning and the data is confusing. This makes the user blindly agree to the terms and conditions without really knowing them.

Answer: [b] It is used to provide information to user

Module:5

Reference No:M5158

Question: Which of the following is a Polymorphic virus?

- [a] The virus changes the application of program when infected
- [b] The virus infects application in different ways
- [c] The virus encrypts the infected file and then stops functioning
- [d] The virus has a decryption routine, encrypted virus body and a decryption routine

Module 5- Polymorphic Viruses

A computer virus is a program that operates without the knowledge of the user and is primarily meant to damage the system on which it operates. A virus, which only replicates itself and then attaches to an application is a simple virus and can be destroyed by searching or scanning the signature (sequence of bytes). An encrypted virus is one, which has the ability to hide its signature and then mingle the virus in a form unrecognisable by the anti virus software. It has a virus decryption routine and an encrypted virus body. The virus first secures the computer and then decrypts the virus body. The decryption then transfers the control of computer to the decrypted virus. But as the decryption routines remain constant from each generation, the anti virus has to scan for virus signatures and the tell tale sequence of bytes to identify the decryption routine.

A polymorphic virus is similar to the encrypted virus. Only difference being, apart from decryption routine and encrypted virus body it has a mutation engine, which generates randomised decryption routine. This engine changes the decryption routine whenever it infects a new program. Since the mutation engine and the virus body are encrypted, the decryption routine first gains control of the computer. It then decrypts the virus body and the mutation engine. The virus then takes charge of computer from the decryption routine, which in turn locates a new program to infect.

The virus then duplicates itself and the mutation engine in Random Access Memory (RAM). The mutation engine is then invoked generating a new decryption routine, good enough to decrypt the virus at the same time bearing no resemblance to the earlier decryption routine. The virus then encrypts the virus body and mutation engine, appends a new decryption routine and attacks a new program. This limits the anti virus scanner search for tell tale sequence of bytes that recognises a decryption routine.

Polymorphic Detection

Generic Decryption

The generic decryption assumes the following about the nature of polymorphic virus.

1. The polymorphic virus encrypts its body to avoid detection.
2. The virus should decrypt to execute normally.
3. Once the virus infects a program, it has to gain control of the computer to decrypt the virus and then give the control of the computer to the virus.

To detect the polymorphic virus the generic decryption relies on this behaviour. While scanning every new program file, the scanner loads itself in to a self-contained virtual computer to the decrypted virus.

Inside the virtual computer the polymorphic virus does not cause any damage, as the real computer is inaccessible. So when a file is infected inside the virtual computer, the virus executes the decryption routine and decrypts the encrypted virus body. This helps the scanner to precisely identify the virus signatures. If the file loaded in the virtual computer is not infected then the scanner quickly stops scanning and removes it from the virtual machine.

Since it has to scan the file individually it is time consuming and greatly reduces the speed of the machine.

Answer: [d] The virus has a decryption routine, encrypted virus body and a decryption routine.

Question: Which of the following is not a data hiding method in open space method?

- [a] Message embedded after trailing space
- [b] Embedding the message between two lines
- [c] Justifying the text and then adjusting the data between each word
- [d] Embedding the data between spaces of each letter

Module 5- Data Hiding in Text

Hiding data in a text is difficult than doing the same in a picture. This because, it is very easy to identify an extra letter or character in a text. Hiding the text in soft copy is again said to be much more difficult when compared to hard copy. A reason being that hard copy text can be treated as a highly structured image and is easily susceptible to changes in letter forms, kerning, baseline and the like.

There are different ways of hiding data in text. Some of the methods most prominently used are:

- Open space Method
- Syntactic method
- Semantic method

In this article, we deal with one such method called open space method.

Open space methods

The open space method makes use of the white space present in sentence. The two main advantages using the white space method is one changing the number of trailing spaces does not change the meaning of sentence and the other it is highly unlikely that a normal reader would notice the extra space or the modification of white space.

Method 1

A binary message can be encoded in a text after each terminating character in the form of a single space or double space. A period is used as terminating character in English prose, in the programming language "C", semicolon is used as the terminating character. A single-space after the terminating character is treated as "0" and two spaces after them are treated as "1".

This method has problems related to space:

1. At the rate of one bit per sentence this is very inefficient. It requires a large quantity of text to incorporate even a few bits.
2. It depends on structure of the text. This means that when the text does not have consistency such as free verse poetry, and no well defined termination characters it becomes very difficult for encoding.
3. To maintain consistency in space, many word processors automatically set the number of spaces after each period to one or more period as required.
4. When white space is used inconsistently due to the carelessness or mistake on the part of encoder, it is not clearly identifiable and in contrast regarded as a part of message.

Method 2

The second method makes use of space between two lines. In this the data is encoded by inserting spaces at the end of the lines. Prearranged spaces are kept at the end of each line after encoding the data. Two spaces encode one bit per line, four spaces encode two spaces two bits per line, eight spaces encode three bits per line and so on. This method is therefore better than the previous one as it dramatically increases the amount of information that has been encoded. To start with, the text is justified. Additional spaces are then added to the end of each line to encode more data. One major benefit with this method is that, the spaces would go unnoticed by the readers, as it is very normal to have white space in the peripheral of any text.

Similar to method 1, programs such as "sendmail" would remove the extra white space in the peripheral of the text. Another problem is the data cannot be retrieved from a hard copy.

Method 3

In the third method text is justified. Data is then encoded in the extra spaces between each word.

Single space is understood as a "0" and a double space is understood as "1". Therefore, quite a lot of bits can be encoded in each line. Since justifications has its own constraints, every inter word cannot be encoded. To facilitate easy detection of hidden parts from the original text Manchester encoding is employed. In this method, bits are made into a group of two. Therefore "01" is treated as "1", "10" is treated as "0", "00" and "11" are treated as NULL. For example, the encoded message of "11010100" would be treated as "11".

Answer: [d] Embedding the data between spaces of each letter

Module:5

Reference No:M5075

Question: In network protection technique of e-commerce, which one of the following use Secure Socket Layer (SSL)

- [a] DMZ
- [b] Firewalls
- [c] Network segregation
- [d] Data encryption

Module 5 - E-Commerce Security 1

Introduction

While implementing an e-commerce application, the security aspect of the same should not be ignored. In e-commerce applications, logon ID method of authentication is not feasible because it is not possible to give every unidentified customer, their own Windows logon ID. There is thus a need for Security in e-commerce at the following three levels:

- Protecting front-end servers from unauthorised access.
- Protecting back-end applications for integrity and privacy of data.
- Protecting corporate network against intrusion.

There are four types of protections implemented at different levels:

1. Network protection
2. Application-level protection
3. Platform protection
4. Database protection

Note: This is the first part of the article on E-commerce security, which deals with network and application-level protection in detail.

1. Network protection

The requirements for implementing network protection are:

- **Demilitarised Zone (DMZ):** It is one of the crucial element for securing a website. It consists of front-end servers, back-end servers and firewalls. DMZ provides multi-layer protection between Internet and internal network of an organisation by:
 - o Firewalls that protects from end servers by filtering data traffic between back end servers and corporate networks.
 - o "Security harden" servers are installed so that malicious internal services like file sharing and telnet can be restricted.
- **Firewalls:** These are used to filter the network traffic coming in or going out of the corporate internal network. Firewalls can be configured according to the requirements of the company. They are implemented at network protocol layer and do not provide protection at higher level of protocols like HTTP. With the help of firewall one can block all ports except port 80 and port 443 for HTTP and HTTPS/SSL (HTTP is known as HTTPS when it is secured) respectively.
- **Network segregation:** It is done with the help of Network Interface Cards (NICs) and allow us to:
 - o Split various types of data traffic and route them to different web servers.
 - o Preventing IP forwarding between front-end servers. Virtual IP address is the only address, which is open to everyone.
 - o Prevent management traffic to pass through firewalls.
- **Data encryption:** Transferring confidential and secret information like credit card number over Internet is exposed to risk, if sent without any protection. Hence data should be encrypted before sending. It is done with the help of Secure Socket Layer (SSL). It also assists in establishing secure connection between source and destination and facilitates server authentication.
- **Intrusion detection:** Intrusion detection system (IDS) can:
 - o Recognise the attack signatures and alarms for vigilance of operating staff.
 - o Disconnects routers with hostile source.
 - o Prevent Denial of service attacks.

But IDS is not without disadvantages. For example it is very expensive and can affect the performance of the website. It sometimes gives alarm even for normal network traffic, misleading the operational staff.

2. Application level protection:

Windows DNA application is a multi-tier application, which is implemented using COM+.

Application service security depends upon the security features implemented in the middle-tier. It can be implemented by:

- **Administrative security:** It prevents the programmer from writing any authenticated code in the application. It also assists in detail auditing. Job configuration for COM+ application can be done by making use of component services administrative tool or administrative object model.
- **Authentication service:** Windows 2000 and COM+ allow us to authenticate the characteristics of client application. COM+ can have multiple level authentications. The lowest level is no authentication and the highest level is encryption of all data packets.
- **Impersonation:** A server application sometimes may be required to take the place of client for some applications. For example, a database can be accessed by server application on behalf of client. COM+ provides impersonation at different levels.

Answer: [d] Data encryption

Module:5

Reference No:M5082

Question: For which of the following options does the Demilitarised Zone (DMZ) Security in e-commerce work as a protection technique?

- [a] Network protection
- [b] Application-level protection
- [c] Platform protection
- [d] Database protection

Module 5 - E-Commerce Security-2

Introduction

In an e-commerce application, the security aspect is of great importance. Security is therefore necessary at three levels:

- Front-end server protection
- Back-end applications protection for integrity and privacy of data.
- Corporate network protection against intrusion.

There are four types of protections implemented at different levels:

1. Network protection
2. Application-level protection
3. Platform protection
4. Database protection

Note: This is the second part of our article and we will be dealing with Platform and database protection.

Platform protection

The network should be secured from internal as well as external attacks. At the same time, the components of the website should also be protected. Application platforms can be secured with the help of the following techniques:

- **Security of servers in a demilitarised zone (DMZ):** Individual security is mandatory for each server in a DMZ. Front end web servers can be protected by:
 - o Installing only necessary components.
 - o Using secure NTFS (NT File System- a file system for Windows NT) instead of File Allocation Table (FAT) or FAT32.
 - o Formulating policies for strong password protection for all user accounts.
 - o Disabling auto-logon.
 - o Implementing policies for low level filtering and putting a constraint on specific ports.
- **Monitoring:** Inspecting the server at regular intervals ensures that the security policies are generating the desired results. Any change in configuration of the server can also be determined through inspection. Access and service accounts can be regularly checked so that privileges can be granted properly.
- **Securing site data:** Data security policies can be defined by analysing the type of data being used by the site like HTML pages, database, catalogs, passwords, etc. The criteria for defining data security policies are:
 - o There should be fewer access points for sensitive information.
 - o Most critical data like credit card numbers should be stored after encryption. Only authorised users should be able to decrypt it.
 - o Password should be first converted by using one-way algorithm and then stored in a database. In case the user has forgotten his password, this technique will allow him to choose a password and mail it to company.
- **Client authentication:** For business sites like online universities, premium service sites and the like, it is necessary to identify the user. The following methods are used to authenticate the identity of the user:
 - o **Cookies:** These are small files (usually in encrypted format) stored on the client's hard disk. It helps the application in identifying the user for providing specific information.
 - o **Password:** Enables user identification through a unique user ID and password.
 - o **Client certificate:** A website owner can issue client certificates to the client. It helps the company in establishing and maintaining better customer relationships. It also verifies the identity of the user when accessing the site.

Database protection

The following techniques are used to implement security on a database (using Microsoft SQL) server:

- **Authentication:** Authenticating the client is a must for database protection. It is done by integrating Windows NT authentication and Windows NT Security system. It ensures a secure validation of passwords and their expiry, auditing and the like.
- **Application roles and security:** It will allow users to connect to the database only via applications that allow such access. The user cannot directly access the database. User authentication is carried out by the application and not by the SQL server.
- **Permission validation:** Once the user is authenticated for access, permissions are granted to the user for accessing database resources. SQL Server checks for user permissions and if there are no specific permissions for executing a command or statement, the request will be denied by the Server.
- **Encryption:** Confidential information is stored in an encrypted form and can be decrypted only by authorised users. Clients can send encrypted data to the database server by using

Answer: [c] Platform protection

Module:5

Reference No:M5085

Question: In an audit of Electronic Data Interchange which of the following tools and techniques are useful

- [a] Audit monitors
- [b] Expert systems
- [c] Computer Assisted Audit Techniques
- [d] All of the above

Module 5 - Audit consideration in an Electronic Data Interchange (EDI) environment

With the growth of EDI, there would be many changes in the functioning of the company. Many companies would actively think of implementing EDI due to its numerous advantages such as shortened business cycle, reduced inventory costs and the like.

Implementation of EDI is not without challenges to the auditors. Before preparing an audit plan the auditor must obtain an understanding of EDI process and its associated risks. There would also be a change in his method of obtaining evidences, as EDI is a paperless environment.

In this article we discuss the considerations for the auditor in an EDI environment. Such considerations are applicable to both internal as well as external auditors.

Obtaining an understanding of business: The auditor should obtain an understanding of the EDI environment in relation to the business as a whole and document the same. For this purpose he may use flow charts to obtain a clear understanding of the flow of information and transactions.

Value added network: In EDI, information passes through value added network both at the sender and receiver's end. The auditor should also audit and evaluate VAN to ensure that the controls and security provided are effective. The auditor may also seek an audit report from auditor of VAN service provider.

Assessment: Auditor should evaluate whether the objectives and expectations of the management in implementation of EDI have been met or not. A detailed analysis of deficiencies in meeting the objectives should be made. The assessment should not be limited to the assessment of the objectives. Even the human resources allocated to the process should be evaluated.

Disaster recovery plan: As in other systems audit, the audit of disaster recovery plan is important in EDI environment also. The auditor should evaluate the plan of the company as well as the Value Added Network.

Audit Evidence: With the introduction of EDI, and hence a paperless office, hardcopy or physical evidence for transactions will be less. Hence auditor has to ensure access to all transactions and certificate from management that the test data used for audit has not been modified. He would need to use computer assisted audit techniques to a great extent.

Audit tools and techniques:

- **Computer assisted audit techniques:** The auditor can buy commercially available software or he can develop the same. The software should be such that they can perform statistical sampling techniques, test of extraction of data based upon predetermined parameters and the like.
- **Transaction verification:** Value Added Networks may provide transaction verification. They usually store transactions for a short period. Any decision to make use of the VAN should be planned during the early stage of audit.
- **Test of EDI:** EDI should be tested for communication links, interfaces, translation software and the like.
- **Audit monitors:** Audit monitors capture transactions on receipt. These transactions can be stored separately for future use of the auditor.
- **Expert systems:** Based on predefined rules, the system can check the transactions so that exceptional transactions can be stored for auditor.

The above list of audit tools and techniques is not an exhaustive one. Many new tools are being developed and the auditor should stay current with these developments.

Answer: [d] All of the above

Module:5

Reference No:M5122

Question: The auditors need not ensure which of the following during the audit of E-commerce?

- [a] Authorised transactions are processed
- [b] Obsolete software is not used by the organisation
- [c] Privacy and confidentiality of information is maintained
- [d] Adequacy of audit trails

Module 5- Audit of E-commerce Part 1

E-commerce refers to the conduct of business online. It involves buying and selling of goods and services on the Internet. Audit of e-commerce is vital as it takes place across the international borders and involves international finance.

Objectives of E-commerce audit

- To ensure that evidence exists for all transactions
- Security techniques are implemented and are reliable
- Transfer of money is secure
- All the transactions are authenticated
- Digital signatures are used
- Common security standards are implemented
- Interface exists between e-commerce system and the financial system
- Business resumption plan takes into consideration the e-commerce system

Audit of e-commerce

There are three different phases to software audit

1. Pre-audit
2. Audit
3. Post audit

In part 1 we cover the pre-audit and few steps of audit phase.

Pre-audit

Pre-audit phase involves gathering information about the organisation and e-commerce activities.

This would include obtaining information on

- Personnel deployed for e-commerce activities
- Monetary value of transactions that are authorised in e-commerce transactions
- Policy on public key infrastructure and digital signatures
- Service level agreements with the certifying authority, buyers and the sellers
- Policy on quality assurance, standards, change management
- Business resumption plans in case of disasters and the like
- Stakeholders of the company

Audit

The detailed audit procedure would include verification and review of the following

- To ensure that only authorised transactions are processed the auditor should determine that there has been no unauthorised movement of money, no duplicate payments, no denial of orders and the like. For this, he should verify whether exceptional reports were generated and reviewed. He should also confirm that digital signatures are used for all the transactions and that, they are properly authorised.
- To ensure the implementation of proper security the auditor should go to the web page and enter a secured transaction. After changing the web page he should verify whether it is possible to go back to the secured page and view the transaction. If the secured information can be viewed then the security measures are not effective. The secured information should expire once the page is changed.
- To ensure that the privacy and confidentiality of information is maintained: This would include ensuring that
 - o Policy exists to separate confidential information from public information
 - o Only general information is available to casual visitors to the site
 - o The information is protected from virus and hacking by implementing proper security measures
 - o Access rights of the staff are reviewed when employee leaves
 - o Evaluating whether transactions were intercepted by unauthorised persons
- To ensure adequacy of audit trails: Audit trails should exist for all transactions. Auditor should ensure that the organisation maintains audit trails by analysing
 - o Allocation of resources for monitoring of activities. For example bandwidth, storage capacity and the like
 - o Monitoring of e-commerce transactions and the maintenance of logs
 - o Non-maintenance of logs to save resources
 - o Follow up actions taken in case of irregularities.

Answer: [b] Obsolete software is not used by the organisation

Module:5

Reference No:M5123

Question: Which of the following reflects the quality of a Website's design?

- [a] Complete disclosure of information
- [b] Appearance of the site, and ease of navigation
- [c] Correct and precise content
- [d] Connectivity to other sites

Module 5- Web Trust

Introduction

A while ago, smart salespeople and attractive television commercials used to attract customer. Now, with the advancement in the technology, the Web is considered as the most effective form of attracting the customer. However there is one essential requirement - Web trust.

Users must be convinced enough to trust the company's information provided on the site. This is possible only when accurate information and effective services are provided. But in reality, online customers are ignored or overlooked. Therefore, it is becoming difficult for companies to gain Web trust in a low-trust online society.

Web trust

Trust is developed through a long-term process in which customers use the site and derive benefits from the Web. However, this trust, developed over a period of time, can be lost in a single moment. Hence, organisations must develop contingency plans for avoiding mistakes which may erode the trust of the customers.

Honesty will win customer trust in the long run. It can be shown in many ways. For example, brand reputation, or seals of approval like TRUSTe can communicate trust to the users. Further, usage of right technology will also enhance trustworthiness.

Customer information: Users may not be willing to provide the correct e-mail address unless they find the company trustworthy. Hence, complete disclosure of a company's policy on usage of customer information will enable companies to elicit correct data.

Web design- Trustworthiness

Trust can be well communicated to the users through the Website's design. Following are some of the ways to perform the above function:

1. **Quality of design:** The quality of the Website design is reflected in its appearance and ease of navigation. A good design creates a feeling of trust. If navigation signals are complex or the appearance of the site is not professional, it is difficult to gain the trust of the customer.
2. **Disclosure:** Complete disclosure of information will enhance the customer relationship and thereby help in gaining users' trust. Concealing information may affect the customers' trust adversely.

For example, if the company does not reveal the transportation charges up-front along with other details, but adds it later, it may wreck the confidence a customer has in the website and he may not visit the site again.

3. **Quality of the content:** The content available on the site must be clear, correct and comprehensive. If it is placed in a haphazard manner, it is likely that the customers may lose faith. Further, content must include current aspects as well.
4. **Connectivity:** Other website links provided on the company's website would make the customers feel that the site is reliable. Moreover, third parties can also appreciate this initiative. On the other hand, an isolated site may be regarded as one that is trying to hide something from the users.

Answer: [b] Appearance of the site, and ease of navigation

Module:4

Reference No:M5133

Question: Who provides Web trust seal?

- [a] Web trust auditor
- [b] Business partners
- [c] Web site owner
- [d] Customers

Module 4 – Web trust services – I

The concept of web trust was conceived to deal with privacy and security aspects of business concerns as well as consumers. It confirms the authenticity of the company's policies in protecting the privacy and security of the information. Realising the need of their business partners and clients for privacy and security, Website owners engage independent web trust auditors to confirm their legitimacy. Web site owners follow highest business standards and also get their online procedures audited to ensure that they are according to the standards.

Web trust seal

The web trust auditor verifies the web site of the company and awards the web trust seal that guards the business privacy. Protection of private information is ensured with web trust seal and it develops trustworthiness for the business among the customers. Web trust seal can be obtained in the following six areas:

I. Privacy: - This area deals with the company's policy in information collection, usage and storage. It builds the trustworthiness of the company among customers. It ensures that the privacy of customer related information collected through electronic medium is maintained in line with the privacy policy stated by the web site owner.

An independent auditor verifies the compliance of the web site with the standard practices for the online privacy.

Requirement: The privacy practices maintained and followed by the company are to be disclosed. Company should assure the protection of information that is collected from the customers through electronic medium.

The web trust seal addresses the following important concerns of the customer:

- *Privacy*: The manner in which information is collected, used and protected.
- *Transaction*: The manner in which transactions are executed, business practices applicable to transaction processing and consistency maintained in such practices.

II. Security: - It is related to the technologies, measures and procedures pertaining to the information security maintenance. It ensures the security of the information by protecting it from unauthorised access. Further the compliance of the access controls for the electronic commerce system with the company's security policies is also confirmed. An independent auditor verifies the compliance of the web site with the standard practices for the online security.

Sharing of customer related and company related information between each other is apparent in a business that is transacted over the Internet. But the information that is communicated over Internet and that is stored on third party computers is subject to risk of unauthorised access. For example unencrypted personal information like credit card numbers is exposed to the risk of unauthorised access during its transmission. The risk is further compounded by the absence of firewall protection or accurate security for the systems.

Hence customers demand security of their information and restrict the access to authorised personnel. An independent audit, which considers the overall objective of the data security, ensures the protection of data in transmission and the data stored at third party's place.

Requirement: - The security practices maintained and followed by the company are to be disclosed. Company should also ensure that only authorised personnel are permitted to access the data and electronic systems. It should also confirm that the security controls are in line with the security practices stated by the company.

Answer: [a] Web trust auditor

Module:4

Reference No:M5134

Question: Which aspect of web trust seal provides confirmation of payment for online purchases?

- [a] Confidentiality
- [b] Non-repudiation
- [c] Security
- [d] Transaction integrity

Module 4 – Web trust services – II

Web trust confirms the authenticity of the company's policies in protecting the security of the information. The first part of the article Web trust services dealt with two areas where Web trust seal can be obtained. This is the second part that discusses the remaining four areas.

III. Transaction integrity: It deals with the concern of the customer towards information protection, as there are chances for information corruption and duplication in processing when the transactions are processed electronically. It minimises this fear of information loss among the customers. The correctness of the prices, quality and goods is assured when there exist transaction integrity controls and business practices.

An independent auditor verifies the conformity of the company's web site with the standard practices for transaction integrity and business processes.

Requirement: The business practices for online purchases maintained and followed by the company are to be disclosed. Further the company should also assure that the transactions processing is accurate and precise and they are in line with the business practices stated by the company.

The web trust seal addresses the following important concerns of the customer:

- *Privacy:* It shows the manner in which information is collected, used and protected.
- *Transaction:* It ensures that the transactions are executed properly, business practices applied for processing, and that consistency is maintained in such practices.

IV. Confidentiality: It deals with the confidentiality of the business-to-business information. It helps to gain customer confidence in exchanging data online.

An independent auditor checks the conformity of Website with the standard practices for confidentiality by considering the confidentiality standards provided by the web trust program.

Requirement: The confidentiality practices maintained and followed by the company are to be disclosed. Company should also assure that the access is allowed only to authorised personnel and the practices are in line with the confidentiality policies stated by the company.

V. Availability: It deals with the service levels as agreed by the companies. Business-to-business and business-to-customer transactions through web require the companies to keep their promise in providing the agreed service level. It helps companies to attract customers as a good Application Service Provider.

An independent auditor verifies the compliance of Website with the standard practices for data and e-commerce systems availability. This is done by considering the availability standards provided by the web trust program.

Requirement: The availability practices disclosed and followed by the company are to be stated. The company should also assure that the data and electronic commerce systems are in accordance with the disclosed availability practices.

VI. Non- Repudiation: It confirms the payment of online purchases by identifying the capability of the customers to pay. Web site owner is assured of his revenues. But what is essential in non-repudiation is proper integration and validation of these transactions. The third party verifies the compliance of web site with the standard non-repudiation practices by considering the non-repudiation standards provided by the web trust program.

Requirements: The non-repudiation practices disclosed and followed by the company are to be stated. Further the company should also assure that the integrity of transactions and its authenticity can be tested later through effective controls.

Answer: [b] Non-repudiation

Question: To ensure that the data is not corrupted during the processing of e-commerce transactions, the auditor should most likely determine

- [a] Incompatible duties are segregated
- [b] Business continuity plan exists
- [c] Review the minutes of board meeting
- [d] All of the above

Module 4 – Audit of E-commerce Part 2

E-commerce refers to the conduct of business online. It involves buying and selling of goods and services on the Internet. Audit of e-commerce is vital as it takes place across the international borders and involves international finance.

In article 1 we covered pre-audit and few steps of audit phase. In this article we deal with other audit steps and post audit phase.

Audit

- *To ensure that all transactions are authenticated:* To ensure that all transactions are authenticated the auditor should first review the policy that describes which transaction will be considered as authentic and which would be rejected. For maintaining the authentication of transactions the management can implement various control measures. Some of them are
 - o Control Self Assessment tools
 - o Review of evidences
 - o Segregation of duties
 - o Maintaining the list of suppliers and signatories currentThe tools should be implemented for security of firewalls, management of passwords and the like
The auditor should try creating fictitious suppliers or making changes to list of suppliers and the like. If he is able to alter the list the authentication process is not secure.
- *To ensure non-repudiation of transactions:* The auditor should ensure that the management defines policies when the transactions are repudiated and when not. Besides this, he should
 - o Determine whether audit trails are maintained of all transactions
 - o Verify whether duties were segregated
 - o Review the contracts recently entered into by the organisation
 - o Review history of transactions
- *To ensure that integrity of data is maintained:* For ensuring that data is not corrupted the auditor should determine
 - o Person responsible for amending catalogues
 - o Senior management from approval should be obtained
 - o Audit trails maintained
 - o Possibility of making changes to audit trails
 - o Segregation of duties
 - o Procedure for ordering and recording the orderThe management must ensure that effective tools and techniques are implemented for intrusion management and physical security.
- *To ensure smooth flow of business:* Smooth flow of business is vital for any organisation. For this it is vital for the organisation to implemented strategies for countering hacking of

- site, intrusions, viruses and the like. The auditor has to ensure that there are no disruptions in the functioning of the business by determining
 - o Business continuity plan exists
 - o Plan has been tested
 - o Alternate arrangements are made and they are adequate
 - o Tools implemented for volume attacks
 - o Improper interface between e-commerce system and financial system
 - o Adequate back up facilities
- *To ensure adequacy of funds:* Adequate funds are necessary for functioning of business. The auditor has to verify the following for ensuring that the organisation has adequate funds
 - o Analyse the funds required and available
 - o Review the minutes of board meeting
 - o Analyse the cost benefit analysis made
 - o Distribution of equity over the activities
- *To ensure legal and regulatory issues are taken care of:* The organisation may face many legal issues such as frauds, issues related to copyrights and the like while doing business on the web. The auditor should ensure that the procedures exist for minimising the legal risks.

Post-audit: The auditor should ensure that his findings and recommendations are considered by the management and implemented where appropriate.

Answer: [a] Incompatible duties are segregated

Module:5

Reference No:M5150

Question: In the audit of electronic banking, the auditor should ensure the existence of policies and procedures with regard to

- [a] Identification of customers who become members electronically
- [b] Corrective steps to be taken in case of any deficiencies in the system
- [c] Steps for complying with the laws, rules and regulations
- [d] All of the above

Module 5- Audit of Electronic Banking 1

Electronic banking is a form of banking in which electronic signals are exchanged between the financial institutions to transfer funds. This is unlike the traditional mode of banking where funds are transferred through exchange of cash, cheques and the like.

The objective of the audit is to

1. Assess the risks related to electronic banking services and to determine the adequacy of steps taken by the management
2. To assess the impact of the electronic banking services on the services of the bank as a whole
3. To ensure that the bank complies with the laws, rules and regulations that apply to the bank
4. To provide the recommended corrective steps where required

Audit of electronic banking can be categorised into three stages:

- Pre-audit
- Audit
- Post audit

Pre-audit

The audit steps to be performed before actually commencing the audit are

- To identify the activities of the bank which are provided electronically. Such activities generally pertain to retail Internet banking, telephone banking, electronic bill payments and the like. The services that are provided can even be identified by reviewing the bank's website.
- Analyse if any significant changes have occurred in the services or operations of the company since the last audit
- Determine the future plans of the company
- Examine the audit reports of previous year or reports of any other audit or of expert that may be available
- Examine the audit reports of service providers in case services are outsourced
- Examine the third party reviews of vendors
- Establish the number of customers that use electronic services, the deposits and loans generated, and the like

Audit

Documentation

- Determine if the policies and procedures exist for
 - Identification of customers who become members electronically
 - Method for accessing the electronic services eg. By way of PIN, password and the like
 - Controls that exist for wire transfers
 - Monetary limits on transactions
 - Security measures to be implemented
 - Analyse the business recovery procedures to ensure that all the events that can affect the services have been taken into consideration
 - Risk assessment
- Analyse the risk of electronic banking and the adequacy of the supervisory plans initiated by the management. The plans should commensurate with the size, activities and complexity of the organisation
- Determine the risk of electronic banking services on company's earning, assets, liquidity position and the like
- Evaluate if the procedures and steps taken by the management are adequate with regard to policies, internal controls, audit coverage, vendor and outsourcing management and the like
- Ensure that proper supervisory controls exist over areas which are highly prone to risk and vulnerabilities
- Perform detailed review of highly risky areas and where required the services of technical experts should be called for

In the next article we deal with other audit steps.

Answer: [a] Identification of customers who become members electronically

Question: Which of the following is not true with regard to audit of electronic banking?

- [a] Topology of the systems and network should be reviewed by the auditor
- [b] Auditor should ensure that the firewall is configured and monitored on a regular basis
- [c] Anti-virus software is being used
- [d] PINs of the customers should be issued to the relatives and friends of customers

Module 5- Audit of Electronic Banking 2

Electronic banking is a form of banking in which electronic signals are exchanged between the financial institutions to transfer funds. This is unlike the traditional mode of banking where funds are transferred through exchange of cash, cheques and the like.

In the earlier article we covered the pre-audit steps and audit of documents and risk management. In this article we will cover the audit steps related to website, physical and logical security and maintenance and services.

Website

- Determine who maintains the site. If the bank maintains the site, then ensure that the site is updated and changes made only by authorised staff and after dual verification. Where it is outsourced establish as to who performs the following operations and processes:
 - Maintenance of the home page
 - Maintenance of the server for the site as well as electronic banking services
 - Maintenance of the operations of the electronic banking system
 - Any other related operations and maintenance
- Review the topology of the systems and networks
- Review the flow of transactions being processed between the electronic banking services and bank's core processing activities
- Identify if the information is processed in real time mode, batch processing or hybrid mode
- Identify if any personnel is responsible for ensuring the accuracy and functioning of the information and links on the web site
- Consider whether the necessary disclaimers have been given on the site
- Consider whether the management has an incident response team for security breaches, tampering of the web site and other related situations

Physical and logical security

- Consider whether the bank has a firewall to protect the bank's web site
- Ensure that the firewall is configured and monitored on a regular basis
- Consider if intrusion detection system is in place
- Determine the procedure for issuing passwords and PINs, encryption of PINs and passwords while they are in transit or in storage
- Determine the number of logins allowed before the PIN gets deactivated
- Determine if the bank personnel are familiar with the security features of electronic banking software
- Determine if the systems that interface with the systems of service providers are secured and data is protected through implementing appropriate controls
- Consider if anti-virus software is used

Maintenance and services

- Determine if the management provides for reports to be generated regarding the usage of website, volume of transactions processed, maintenance of system logs, exception reports and the like and review of such reports by a responsible person
- Consider if the management provides procedures for addressing customer problems
- Verify if a procedure exists for escalation of exception reports to senior management

In the next article we will cover the audit steps relating to service providers and vendors and post audit stage.

Answer: [d] PINs of the customers should be issued to the relatives and friends of customers

Module:5

Reference No:M5160

Question: Audit of electronic banking requires

- [a] Review of contract with the vendors and service providers
- [b] Review of payments made to the vendors
- [c] Review of receipts from the customers
- [d] All of the above

Module 5- Audit of Electronic Banking 3

Electronic banking is a form of banking in which electronic signals are exchanged between the financial institutions to transfer funds. This is unlike the traditional mode of banking where funds are transferred through exchange of cash, cheques and the like.

In part one, we covered the pre-audit steps and audit of documents and risk management, part two covered the audit steps related to website, physical and logical security and maintenance and services. In this article we cover the audit steps relating to service providers and vendors and post audit stage.

Service providers and vendors

- In relation to service providers and vendors the auditor should ensure that the contract is written and includes the following:
 - Minimum service level agreements
 - Recovery time in case of disruptions
 - Penalties if any, in case of non-performance
 - Matters related to ownership of data, compliance with the defined procedures and the like
 - Liability in case of erroneous transactions
 - Adherence to the contingency plans
 - Maintenance of backups of data and programs
 - Review of the audit reports and security plans
- Ensure that the contract has been reviewed by the legal counsel
- Review the escrow agreement in case of purchased electronic banking software
- Review the access by the vendor's to the banking system and ensure that the monitoring of access by the vendors to the system is adequate

- Ensure in case of maintenance of the electronic banking services by the service providers, that measures have been taken to protect the site from unauthorised alteration and malicious attacks
- Consider whether the bank performs periodic reviews of the activities of the service providers which should include:
 - Review of policies and procedures relating to internal controls and security
 - Monitoring the performance of service providers and vendors
 - Review of exceptional reports, capacity reports and the like of the service providers and of vendors
 - Review of the backup arrangements

Management

The auditor should ensure that management approves for provision of electronic banking services. In this relation he must review

- Prospective customers for electronic banking
- Incentives that may be offered to new customers
- Impact of the electronic services on present customer's base
- Internal controls that may be implemented for new services
- Activities that should be outsourced
- Responsibilities of vendors and service providers
- Insurance coverage for operational risks and its adequacy

Post audit

After the report has been submitted, the auditor should ensure that the recommendations are implemented. If not, he should obtain an explanation regarding the same.

Answer: [a] Review of contract with the vendors and service providers

Module:5

Reference No:M5161

Question: Which of the following is not true with regard to audit of Internet banking?

- [a] Audit ensures that banking regulations are complied with
- [b] Audit need not be performed if an independent technical expert has evaluated the system
- [c] Policies and procedures with third parties relating to internet services should be reviewed
- [d] Audit should focus more on areas that are prone to vulnerabilities

Module 5- Internet Banking 1

Internet banking is the facility provided by the banks for customers to access account information and carry out transactions? via any computer connected to the Internet.

With many banks providing Internet banking services, the auditor is not left behind and his scope of audit also includes the audit of such services and the resources that are used to provide such services. The main rationale behind such audits is to ensure that

1. Policies and procedures are defined and are adequate
2. Internal controls exist and are appropriate to the risks and function as desired
3. Banking regulations are complied with

Before the auditor commences his audit, he needs to carry out certain preliminaries to plan his audit. The preliminary steps that the auditor should perform before he commences his audit of Internet banking are:

1. To obtain the list of personnel involved in Internet banking and description of their functions
2. Flow chart of the Internet banking function
3. List of services provided on the Internet
4. Policies and procedures
5. Independent assessments performed by experts, if any

Besides these, the auditor should also discuss with the management issues pertaining to the security, functions outsourced, changes made in the policies and procedures and any complaints specific to Internet banking.

He should review

1. Previous audit reports and any other independent expert reports and steps taken by the management to implement the recommendations.
2. Services that are outsourced to external vendors and their responsibility for development, operation and maintenance of these services.
3. Comparison between general ledger accounts and accounts related to Internet banking and obtain explanation in case of deviations.
4. Products and services specific to Internet banking viz.
 - Internet banking system and its capabilities, the link between the Internet banking system and other host systems and the network infrastructures
 - Flow of data related to transactions through the network
 - Areas which are more prone to vulnerabilities
5. Issues related to payment services viz.
 - Whether the banks' settlement responsibilities are clearly defined
 - Where it is outsourced, the policy of the vendor addresses issues related to funds that are not collected, customer service, issues relating to backup, contingency plans and the like
6. The web linking agreements with associated and non-associated third parties to ensure that third parties are sound and can provide services, have adequate resources to meet the contingencies, the policies and procedures are in place, rights and responsibilities are clearly defined.
7. Last but not the least he should ascertain the commitment of the management in providing such services and in implementing the security and control issues. Thus, he should ensure that a committee or a team is made responsible for Internet services and that they are trained in Internet related services.

In the next article we deal with the audit procedure for Internet banking.

Answer: [b] Audit need not be performed if an independent technical expert has evaluated the system

Module:5

Reference No:M5162

Question: When performing the review of policies and procedures in relation to audit of internet banking, auditor the auditor is least likely to verify

- [a] Information about the customer that can be disclosed to third parties
- [b] Classification of the data and category of data that should be encrypted
- [c] Duties of data entry personnel are clearly defined
- [d] Policies provide for firewall monitoring and its maintenance

Module 5- Internet Banking 2

Internet banking is the facility provided by the banks for customers to carry out their transactions online. This is made possible through any computer that is connected to the Internet.

In the first article, we dealt with the preliminary procedures that precede the task of audit. In this article we deal with the actual audit procedure.

Policies and Procedures

The auditor is required to examine the policies and procedures specific to the Internet banking to ensure that:

- Provisions exist therein for hypertext links and define financial products that are insured, products and services that are offered by the bank. This also includes the procedure to be followed by a consumer when he is leaving the bank's web site.
- It provides for non-disclosure of confidential information about a customer to a third party and other general information of a customer that can be shared.
- It also provides for information that should be reported to the top management such as number of customers to the site, number of Internet banking loan transactions, number of unauthorised attempts to the site, the hours for which the site was non-operative, the security threats and the like.
- Duties of security administrator are clearly defined. Also review whether their authority is appropriate to the responsibility.
- Firewall monitoring and maintenance exists and defines the access rules for allowing users access to the site.
- Encryption process is defined; designated person is made responsible for its functioning, data classification procedure and the type of data for which encryption procedure should be used.
- It addresses the security issues and provides for usage of anti virus software. Also whether it provides for the review of the security issues and its review by a responsible person

Processing and recording

With regard to processing and recording the auditor has to verify that

- Reconciliation is done at periodic intervals and extend to all general ledgers and subsidiary ledgers related to Internet banking
- Reconciliation and suspense items are reviewed by a responsible person

Contingency plans

Review of contingency plans by the auditor is also important and it should not be ignored. Adequate and appropriate contingency plans ensure that the bank can function even after a contingency or a

disaster arises, though the business may be disrupted for some time. The steps that would be involved in review of contingency plans are

- Whether the plans address all the services and the related resources that are used for providing services on the Internet
- Whether they are reviewed, updated and maintained by responsible personnel
- Backup arrangements exist with external vendors and suppliers and are adequate
- It provides for escalation of security breaches to the top management and external agencies
- Mentions the retention period for which the backups should be maintained
- Provides for storage of critical data at secured off-site location
- Plans are tested annually and the results are reviewed by the top management

In the next article we will deal with administration, operations and legal and regulatory matters related to audit of Internet banking.

Answer: [c] Duties of data entry personnel are clearly defined

Module:5

Reference No:M5163

Question: Which of the following is most likely to be performed by the auditor in the course of audit of Internet banking services?

- [a] To tour the server room
- [b] The user is not allowed to login after defined repeated failed attempts
- [c] Contract clearly states the services that will be provided by the vendor
- [d] None of the above

Module 5- Internet Banking 3

In the earlier articles, we dealt with the preliminary procedures and audit of policies and procedures, processing and recording and contingency planning during the audit phase. In this article we will deal with other related issues pertaining to audit of Internet banking.

Management and supervision

Management and supervision of Internet banking resources is vital as it ensures that the system is functioning effectively and as desired. The auditor should focus on the following:

- Determine if security officer has been made responsible for the functioning of the system
- Ascertain that the levels of access to the employees is determined by a senior management and is reviewed at regular intervals
- With regard to the servers, he should tour the server room once to determine if access to the area is restricted, the password to the server is changed regularly. Also ensure that the UPS is provided for unrestricted supply of power. The server should be physically and logically secured.
- Exceptional reports generated by the system are reviewed by the senior management
- With regard to passwords
 - Controls are established by the bank while issuing passwords to the customers
 - Alphanumeric characters are used for passwords
 - There is a forceful change of password after a defined period

- For the security of the systems
 - User should not be allowed to login after defined repeated failed attempts
 - Unauthorised attempts should be checked
 - Actual attacks against the bank system should be monitored
 - Incidents must be reviewed by the senior management
 - Resources must be physically secured
 - Unauthorised personnel should have no access to the computer resources
 - Virus detection software is implemented
 - Anti-virus software must be updated at regular intervals and current
 - Distribution of software must be through bank's server
- In relation to customers
 - Each user must be provided with a unique user id and password
 - Customer service levels must be defined
 - Level of access to the customers are defined
 - Confidential information of the customers must be protected
 - Policy defines the personal information of a customer that can be shared with the third parties
 - Legitimacy of each transaction with the customer must be verified before the transaction is processed further

Review the logs to ensure that the system is working effectively and all deficiencies are resolved.
- In relation to vendors with whom bank has entered into an agreement -
 - Contract must clearly state the services that will be provided by the vendor
 - Duties and responsibilities must be clearly defined
 - Frequency at which reports should be submitted must be stated
 - Basis of charging fees and its calculation must be specified
 - Provision of training where required
 - Provision must be made for the audit of the vendor resources
 - Specifies that a contingency plan should exist and which is current and provides for adequate backup arrangements
 - Services outsourced cannot be outsourced to any other party
 - Provides for provision penalty if the contract is to be cancelled before the expiry of the term

The management must ensure that the audit covers all the areas of audit are covered on rotational basis.

Answer: [d] None of the above

Module:6

Reference No: M6001

Question: Companies are exposed to various kinds of e-mail threats-mails containing racist, sexual content are typical of:

- [a] Spam
- [b] Information leakage
- [c] Interception and tampering
- [d] Offensive contents

Module 6 - E-mail Threats

Today, e-mail is one of the most widely used services on the Internet. Many businesses now use e-mail to send and receive important information. It is not only cheaper, but also a quicker. However, many companies have not realised the need for e-mail security. Businesses that rely heavily on e-mails for communication are at risk. The use of e-mail poses the following threats -

- **Spam** - One of the major threats faced by companies is spamming of their mail servers. A survey conducted by the Gartner group revealed that 90% of employees received spam or unsolicited mails, once a week. Spam mails not only block the bandwidth and slow down corporate servers, but also waste a considerable amount of employee time. Spamming also poses a security hazard; the 'spammer' can use a corporate mail server to send unsolicited mails, which may later land the company in trouble.
- **Information leakage** - Companies that don't keep a track mails expose themselves to the risk of information leakage. Employees may pass on sensitive corporate information to outsiders, which generally is the case with disgruntled ones. However, often many employees share sensitive information, unknowingly.
- **Interception and tampering** - Certain malicious software such as sniffers may intercept a mail, when it is sent. A person who installs a sniffer gets copies of mail passing through that computer; and can misuse the information. Usually sniffers look for information such as credit card numbers, passwords, competitor information and the like. There is also the threat of mail tampering.
- **Offensive contents** - Corporate e-mail users sometime indulge in sending racist, sexist or other offensive mail. This not only causes companies a lot of embarrassment and trouble, but in some cases also costs a lot of money. Chevron had to pay \$2.2 million to settle a case, when one of its employees sent a sexist e-mail message.
- **Viruses** - Viruses are a major threat to corporate servers and systems. As a result, many companies do not allow file attachments, because virus are embedded in them.
- **Delivery failure** - Now, many companies are using e-mails to send time sensitive information such as proposals, product information, orders and the like to their clients. In such a case, confirmation from the receiver is an issue that has to be dealt with. Sometimes mails do not reach the intended receiver; while at other times the receiver may deny receipt of mail. In such a scenario, the company may stand to lose, and ought to have a mechanism to ascertain the status of the email.

Companies should safeguard themselves against these threats, and formulate a security policy and guidelines regarding email usage by employees.

Answer: [d] Offensive contents

Module:6

Reference No: M6002

Question: BCP (Business Continuity Plan) should focus on:

- [a] Departments that are greatly affected by a disaster
- [b] Departments that are least affected
- [c] Departments that have at least 50% IS related assets
- [d] The entire enterprise.

Module 6 – Business Continuity Plan – 1

Today, people, systems, processes, services, and the like are so closely interlinked that even in the event of a disaster it is essential to resume business activities at the earliest. For instance, on September 11, 2001, many companies lost key managers; they lacked managerial expertise, at a time they needed it most. Thus, companies should plan and be prepared for such situations. Guidelines and policies need to be chalked out, so that normal operations are not disrupted even during a disaster. This is known as Business Continuity Plan (BCP).

BCP should involve the entire enterprise because of the interrelationship between functions. Since Information Technology is a critical part of any business, BCP focuses on protecting information systems, and retrieving the information during or after disaster.

First, the company should conduct a cost benefit analysis. This should assess the loss can could be incurred in the event of various kinds of disasters. It should then be compared to the cost involved in developing continuity plans.

The next step is to identify risks associated with different kinds of disasters. Costs would differ, depending on the risks and the type of disaster. While considering costs, intangible costs such as goodwill, market share and the like should also be considered. Before undertaking a BCP exercise, the company must –

- Undertake Business Impact and Risk Analysis (BIRA) after collecting detailed information
- Appoint a Plan Development Co-ordinator (PDC) who has a clear idea of business operations

The PDC should identify people from different units/departments, and conduct interviews to analyse the impact of disasters in their units/departments. This helps in brainstorming on action plans to be adopted, in accordance with the disaster. After such brainstorming, the PDC should develop a plan document that includes –

- Objectives
- Timeframe for business recovery of each unit
- Resources required

Thereafter, focus on effective implementation. Members of the recovery team should be well aware of their roles. The budget should also be fixed and recovery procedures should be checked.

Risks change as the business changes; thus the PDC should ensure that BCP is constantly reviewed. He should also assess the efficiency of the plan. Exercises should be conducted without prior notice to get accurate results. It would also provide good training for employees involved in recovery activities.

Answer: [d] The entire enterprise

Module:6

Reference No: M6003

Question: Which of the following statement is true with respect to Electronic Fund Transfer/Point of Sale transaction?

- [a] To verify the identity of the cardholder, using signature is more secure than using the PIN
- [b] All cards are not checked with hot card numbers

- [c] A central authority verifies the signature of the person holding the card
- [d] Before payment, the cardholder and the merchant agree upon the amount

Module 6: Electronic Funds Transfer

Billions of dollars are transferred between banks globally through Electronic Funds Transfer (EFT). EFT is a group of technologies, which enables financial transactions to be processed by electronic means. It enables information to be transmitted through various telecommunication channels, which results in the electronic transfer of funds from one financial account to another. EFT replaces the need for currency exchange and signed cheques improving speed and efficiency.

The focus of this article is to explain transactions that take place in shops, which is referred to as Electronic Funds Transfer at the Point of Sales EFT/PoS. EFT/PoS technology is usually employed in transactions that take place in supermarkets, departmental stores, discount chains and other merchandise outlets. Services that EFT offers are as follows -

1.Consumer oriented/decentralised EFT services

- Consumer oriented/decentralised EFT services (used in credit/debit card transactions)
- Check and credit authorisation
- Check verification
- Check guarantee
- Account status inquiry

2.EFT services that involve direct money transfer (through ATM services)

- Deposit
- Cash withdrawal
- Loan payment
- Inter-account transfer
- Debit of transaction balance with overdraft privileges
- Credit purchase
- Cash advance

3.EFT services that involve bill payments

- Telephone
- Utilities
- Petrocards

Institution oriented/centralised EFT services

- Direct deposit of payroll
- Pre-authorised debit services
- Corporate Cash Management (including inter-bank and intra-bank transfer)
- Inter-bank settlement and clearings

EFT cannot be considered an entirely new development. ATM and credit card transactions, which have been around for several years, are extended services of EFT technology. ATM is a kind of EFT service that dispenses cash; similarly, credit card enables the transfer of funds to the merchant's account, and simultaneously files an entry into the credit account of the cardholder. EFT/PoS transactions take place in following manner -

- A person who initiates a transaction and has to make a payment carries a plastic card (usually smart card). By swiping it, the cardholder can gain an entry into the system
- Before paying, the cardholder and merchant agree upon the amount to be paid. This amount is then entered into the system by the merchant.
- The system reads details from the card, identifies the cardholder and to a certain extent verifies whether the card is original or not.
- The next step is to ensure that the person carrying the card is the valid cardholder. This can be done either by verifying the signature or by using the Personal Identification Number (PIN). Verification of signature depends on the personnel, the merchant establishment, and usual practice reveals that this step is omitted. Therefore, from the security point of view PIN is preferred to signatures.

After confirming ownership, the next step is to authorise payment. If it is a small amount, authorisation is almost instantaneous, without referring to the central register. However, if the amount of payment is high, then the transaction information has to be transferred to a central register, where many checks are performed before authorising the payment.

Verification of PIN is the first check; the second check involves matching of card with the list of hot card numbers issued by the issuing authority. Thereafter, the cardholder's account is checked whether he has got sufficient funds or not. After the entire verification is completed, the merchant receives the printed authorisation receipt from the issuing authority.

Answer: [d] Before payment, the cardholder and the merchant agree upon the amount

Module:6

Reference No: M6004

Question: Which of the following is not true of a Disaster Management Team -

- [a] To decide on locations from where remote access is possible, in the event of disaster
- [b] To make a list of employees, who should be called to remote sites for work
- [c] To provide remote access to the network to all employees
- [d] To continuously check whether security and intrusion systems are functioning effectively

Module 6 - Disaster Recovery - Remote Access

Disasters often affect the functioning of local sites. If a company's operations are spread over different regions and locations, then a disruption in one location is likely to affect others also. In either case, companies should plan ahead to minimise the damage caused.

Action Plan for managing remote sites

To begin with, companies should establish Disaster Management Teams (DMTs) for each region. Responsibilities should include communicating with employees in the region, and restarting operations in the event of disaster.

Other responsibilities of DMTs -

- To decide whether it is safe for employees to report to work
- To make a list of employees who should report
- To decide on alternate locations where employees should report to work

- To create virtual business teams. A disaster could result in scarcity of resources, and employees whose functioning is indispensable to the company only should be called. Others can be directed to tele-communicate or work from hotel rooms or net centres
- To monitor networks that are functioning, and redirect employees to them

Post disaster, if the physical site is not made operational for some reason, then DMTs should check whether temporary offices can be set up in employee homes or in a hotel room. Employees having broad bandwidth and network connection could volunteer to do so. Otherwise, teams should arrange for network connections, and provide basic facilities to work groups.

They should also create a site that provides information and instruction for employees. It should contain host names, addresses and other contact information. Employees who have restricted access to networks should be redirected to this site.

DMTs should also ensure that intruders do not consider this as an opportunity to hack into their systems, and constantly monitor the functioning of security features. In case there are problems, it should instruct employees and clients not to send sensitive information over public mail systems.

Conclusion

Remote access capabilities ensure that companies become operational, within a short span of time, and employees are not restricted to physical locations. Business survival hinges on remote access in times of disaster.

Answer: [c] To provide remote access to the network to all employees

Module:6

Reference No: M6005

Question: A Data Replication Architecture that updates the secondary site by capturing changes using the asynchronous process is,

[a] Shadowing

[b] Mirroring

many businesses. Companies involved in e-commerce transactions and other real time customer service businesses are highly dependent on information systems. Businesses cannot afford to have these services disrupted even for a short period. They have to be prepared to recover as quickly as possible to avoid loss of data during such events.

Businesses that incorporate data replication architecture into their disaster recovery plan can considerably reduce their recovery period. The function of this architecture is to replicate data and transactions from the primary processing site to an alternative site. This ensures that the enterprise continues to function even when the primary site fails.

Before designing the replication architecture, it is essential to determine the recovery objectives. If a business can afford to lose transactions (say for 5 -60 minutes), then an asynchronous solution can be used as it is more cost-effective, and does not block the bandwidth. In cases, where the enterprise cannot afford to lose data, then synchronous mirroring can be used. Other factors to be considered include the frequency of the process, the site/location where the replication will be done, as well as, personnel who will be responsible for it. Following types of replication modes can be used -

Transaction Aware Replication

This involves replication at the transaction level, i.e. it transfers the database or file changes to a secondary site. The secondary site identifies each transaction as the file is transferred using logs. The main feature of this method is that it identifies the unit of work i.e. transaction, thus maintaining data integrity (i.e. rollback/roll forward), to a large extent.

Shadowing

First, it replicates databases at the alternate site. It then updates the database by continuously capturing changes on the alternative site. Shadowing replicates using the asynchronous process, and requires considerably less bandwidth. **Recovery Time Objectives (RTOs)**[1] are significantly reduced (ranging from one to eight hours) and **Recovery Point Objectives (RPOs)** [2] are updated till the last receipt and application of logs from the actual site.

Mirroring

It also replicates databases and/or file systems by applying changes at the secondary site, synchronous to changes in the primary site. In this case, RTOs range from 20 minutes to few hours, while RPOs are reduced and include only the loss of uncommitted data. Since it adopts the synchronous process, it requires far more bandwidth than Shadowing.

[1] **Recovery Time Objective (RTO)**: The duration in which a department must be re-established to provide critical function(s) of business. All department-planning activities should be directed to meet this objective.

[2] **Recovery Point Objective (RPO)**: The duration in which data must be restored in order to resume processing of transactions. RPO is the basis on which the data protection strategy is developed.

Answer: [a] Shadowing

Module:6

Reference No: M6006

Question: In the event of a disaster, the crisis management team should first -

- [a] Inform the stakeholders
- [b] Assess the impact of disaster on the company
- [c] Take care of personnel and their dear ones
- [d] Form an emergency response team

Module 6 – Disaster Recovery

After the 11 September 2001 terrorists attack, many organisations have realised the need for an elaborate Disaster Recovery Plan (DRP). Disaster Recovery Plan refers to the steps an enterprise should take when the organisation's normalcy is disrupted during a natural and man made disaster. DRP becomes important because at times it takes months or years to recover from the disaster, and in worst cases organisations do not recover at all. A research by Gartner reveals that two out of every five organisations that face a disaster close their shops within five years. Primary reasons for these are high cost of recovery and loss of customer's confidence.

- Disaster could result due to reasons such as: Extreme Weather Conditions
- Power or Communication failure
- Robbery or any other criminal activity
- Civil unrest
- Terrorist attacks

Disaster Recovery is a component of Business Continuity Plan (BCP). Companies should not stop at just DRP; they should extend their scope to BCP as well. . Many companies are opting for BCP because chances of survival are higher than those companies who do not opt for it. BCP includes Disaster Recovery, Business Recovery, Business Resumption, and Contingency Planning. Another important component, which forms a part of BCP, is Crisis management.

Crisis follows disaster, hence companies should prepare for Crisis Management. Crisis Management refers to actions an enterprise takes in case the normal operations are disrupted due to some event. Proper Crisis Management builds confidence in the employees, customers, partners, investor and the society that the company can sustain disaster.

It is important that each and every aspect of the business process is analysed and their risk factors identified. A detailed analysis of information flow should also be done in order to consider the recovery options in cases of a crisis.

Crisis Management Team

A proper crisis management team should be ready to take charge of the situation. This team should be drawn from senior management, risk management, human resource, facilities/building, legal and public relations, and should include Chief Information Officer and Chief Technology officer. The team should -

- Take care of personnel and their relatives
- Assess the impact of the disaster on the company and issue a disaster declaration
- Inform the stakeholders (employees, customers, partners, investor and the society) of the disaster and the steps that are being taken

An emergency response team should also be formed which should work closely with "crisis management team". This team should comprise of employees who work closely with -

- Local government agencies, such as fire, police, etc.
- Utilities - (Gas, electricity and telephone)
- Facilitation services such as transport, hospitals recovery units

Actions in case of Disaster

1. In case the disaster takes place during the daytime, the entire office premises should be evacuated and head count of employees done in order to check for any missing personnel. Injured personnel should be attended to and a rescue team for missing personnel should be sent.
2. In case the event takes place after office hours, it is important to document the contact information of all employees so that they could be reached for confirmation. Contact information should include home, office, mobile and pager numbers, e-mail ids, addresses etc.
A call tree should be established specifying the contacts with the contact information in case of crises.

3. Emergency Information Card provides instructions on dos and don'ts of actions to be performed during/after crises. The information usually includes -
 - Immediate evacuation location - a place where employees will assemble for the head count
 - Recovery location - Alternative place from where the business can be continued
 - Emergency hot line - This will help the employees to communicate
 - Business Continuity co-ordinator - Name, telephone number and other contact information of the co-ordinator

Answer: [c] Take care of personnel and their dear ones

Module:6

Reference No: M6007

Question: Software change management -

- [a] Is all about managing alterations, irrespective of the stage of lifecycle of a product
- [b] Is done only in the development stage
- [c] Is done only in the maintenance stage
- [d] Activities decrease after the product release.

Module 6- Software Change Management

In 1995, the Australian Stock Exchange (ASX) sought to implement a major software change, over a weekend. The Exchange closed its operations on a Friday hoping to continue operations with a new share trading system. Analysts predicted a turnover of A\$1bn on Monday, however trading took place merely for 2 hours, and total transactions amounted to just A\$550mn. As a result, several brokerage firms lost a large amount of commission. The cause of the failure was the new software.

On Monday, when the Exchange opened, the new application failed yet again, and the matter worsened when ASX was not able to roll back to the earlier version. Corruptions in the database forced the Exchange to close down. It tried to implement a disaster recovery mechanism; yet trading had to be stopped for 2 hours. Although ASX used highly reliable hardware and software, and spent millions of dollars on a 'hot' remote backup site, systems failed. The kind of disaster recovery that ASX had adhered to, did not guarantee business continuity.

The lesson here is that care should be taken while making software change management decisions. Enterprises should develop policies and procedures for effective change management of software that include:

- Planning and tracking of problem/Change Request (CR) initiation
- Impact analysis of software change
- Version control
- Security aspects of new software assets
- Methods to train users
- Quality reviews

Software distribution

There is a need to understand software 'configuration management' and 'change management'. Configuration management includes version control, efficient usage of reusable components and advance assembly systems etc.

Software maintenance deals with simple localised changes, short-term activity, and is a response to one software requirement at a time. Software evolution deals with structured changes, and complies with a broad range of requirements. Stepwise incremental changes occur throughout the life of the software, which means evolution, takes place both during development and maintenance. Managing these changes is a part of change management.

Every software cycle is divided into two phases -

- Software Development - It includes all activities prior to the release of a product.
- Maintenance - It includes all activities after the release of a product.

The development phase involves change management to some extent. It includes changes that have to be made in the code in accordance with changing requirements of the product. The amount of development reduces when the software is nearing its completion, but this ensures that maintenance begins. Any work during the maintenance phase also involves change management.

Software change management can be of three types -

- Active change management - It refers to planned changes. Environmental changes are normally planned.
- Reactive change management - It refers to changes that are made due to an unexpected change in the environment.
- Pro-active change management - It anticipates changes that are likely to take place in the environment. So, it becomes easy to make reactive changes.

Conclusion

Enterprises should adopt appropriate software change management to avoid disasters that may otherwise result. The methodology used should take care of different types of CR workflow.

Answer: [a] Is all about managing alterations, irrespective of the stage of lifecycle of a product

Module:6

Reference No: M6009

Question: If outsourcing a hot site is a feasible solution, then which of the following should be considered while interacting with the vendor?

- [a] Hardware, software and networking requirements
- [b] Location and testing requirements
- [c] Staff expertise
- [d] All the above

Module 6 – Requirements of hot site

A 'hot site' ensures quick recovery of operations in case of a disaster. In business, depending on the requirements, companies have to decide whether to opt for an internal hot site or to outsource

from hot site solution providers. Many companies prefer to outsource the task, as it saves the company expenditure involving space and manpower. By paying a monthly fee for space and equipment, it can avail of hassle free services offered by the hot site solution provider.

These independent service providers offer a hot site configured to the specifications of the corporate client, that can be up and running, at just a moment's notice. It is equipped with the required hardware, software, networks and expertise that enables the company to run an alternate site, in case the primary site becomes inoperable.

Requirements to be specified to the hot site vendor

Before deciding on the hot site provider, it is essential to list out recovery requirements. These include anticipated recovery time frame, precise hardware/software requirements, network specifications, and level of expertise required. If confidential information is provided to the hot site vendor, the company should clearly mention protection and handling details. Companies should also specify-

- *Compatibility* - The company should check whether the alternative site can support operating systems, applications and networks. It should also ensure that connectivity is maintained in case of LAN and WAN.
- *Hardware Requirements* - Vendors should be provided with details of existing hardware, specifying the brand name, model number and other requirements. Details of different sites and inventory being used thereof should also be supplied. All this information helps the vendor to work out a cost effective solution.
- *Software Requirements* - Vendors should also be provided with a list of software that is currently in use, and that may be required in the hot site. The company should also provide details that include the name of the software application, name of and vendor, version and other details so that it is easy for the vendor to understand its software requirements.
- *Network Requirements* - Vendors also need to have a detailed list of network components such as ports, connectors, cables, interfaces and other devices necessary to set up the network environment.
- *Testing Requirements* - Testing is very important while setting up an alternative site. Since, activating the alternative site has to be done quickly testing reveals the flaws (if any), and improves effectiveness of the recovery plan. Good vendors provide assistance in developing and in testing.
- *Location* - The choice of location of alternative sites is very important. The alternative site should at a reasonable distance from the primary site, so that the disaster does not affect both sites. Companies should ensure that both locations are not within the same power grid. Generally, vendors suggest locations after considering flood-prone areas, earthquake fault lines, neighbourhood crime statistics and the like.
- *Staff expertise* - Hot sites are generally equipped with hardware and software. However, during a crisis hot sites require competent staff to respond and take relevant action. Thus, the vendor should train personnel in hardware/software and networking, so that the client can resume business with little delay, in case of disaster.

Answer: [d] All the above.

Question: Electronic Data Interchange

- [a] Is another name for e-mail
- [b] Is not of much use in data transfer between two computers
- [c] Provides strategic, operational and opportunity benefits
- [d] Is a tool that can even transmit information in an unstructured format

Module 6: Electronic Data Interchange

Electronic Data Interchange (EDI) helps to conduct transactions and carry out business electronically with trading partners. In general parlance, EDI refers to paperless trading, because it seeks to eliminate paper-based communication. For instance, placing orders with suppliers, carrying out financial transactions and the like.

Technically, EDI refers to electronic interchange of structured data in accordance with the message standards of computers systems, between which data has to be interchanged. Structured data is presented in fixed formats such as invoice, order form and the like. Message standards ensure that information exchanged between computers are interpreted correctly. Information is interchanged without any human intervention.

To some extent, EDI is similar to e-mail, as both help to receive and send messages between computers. However, the differences between the two are -

- e-mails have no structured format, whereas EDI has
- e-mails are not intended to be processed, whereas EDI has to be processed further
- e-mails are received by the recipient as it is, whereas EDI is received only after processing

EDI helps in automating tedious paper work. Apart from this, many other benefits make it a very efficient and effective tool for managing business processes. Initially, companies used EDI to avoid data errors and improve data flow. Since it removes the need of re-entering data from paper to the computer system, clerical errors are minimised. Research suggests that 70% of output from one computer system can be used as input in another computer system.

Therefore, with the help of EDI, the output can be automatically used, without having to enter the same data into the system again. This also results in lot of cost savings, and reduces the number of personnel required to do the same job.

It also speeds up data processing; in cases where receivables are concerned, company's cash flows improve substantially. Similarly, in cases where order is placed through EDI, it is processed almost instantaneously. This helps the company to plan production much more accurately, and consequently decreases inventory costs considerably.

Benefits of EDI can be grouped into three different categories -

1. Strategic benefits

- Decreases trading cycle, resulting in faster business processes that provide a competitive edge to the business

- Improves business processes by implementing techniques such as Just in Time manufacturing
- Enhances customer relationship management. Since data exchanged through EDI is automated, it can be used as a powerful marketing research tool to yield operational benefits
- Enhance ability to compete with other market players

2. Operational Benefits

- Reduces operations costs (such as paper, manpower, inventory)
- Improves cash flow
- Makes data more secure, as error handling and detection becomes easier

3. Opportunity benefits

- Provides competitive edge
- Increases scope for corporate relationships and strategic partnerships

Answer: [c] Provides strategic, operational and opportunity benefits.

Module:6

Reference No: M6011

Question: Which of the following is not a component of Electronic Data Interchange?

- [a] Standards
- [b] Management Involvement
- [c] Software
- [d] Communication

Module 6 – Process of Electronic Data Interchange (EDI)

Companies should not merely consider EDI as a tool that eliminates paper based operation; rather they should consider it as a tool to enhance operational efficiency, improve business processes and provide strategic benefits. Thus, the support and involvement of the management is essential to implement EDI. The management should move in a planned manner –

1. The first step in the process is to appoint an EDI project leader who will drive and co-ordinate the entire process. The primary responsibility of the project leader is to form a cross functional team of committed people.
2. The next step is to identify and analyse internal as well as external information flow, and to segregate them into manual/automated generated information.
3. Once the information flow is analysed, the next step is to identify processes that should be automated.
4. Interact with different EDI information centres and parties to gather information. Different parties that can provide EDI based information are –

- a. Trade associations
- b. EDI software vendors and network operation
- c. EDI consultants
- d. EDI users

5. Conduct cost-benefit analyses and kick start the pilot process by involving some partners in the process

6. Run pilot project. If it succeeds, expand to other business processes and partners

From the technical perspective, the three major components of EDI are -

1. Standards - Standards are the basis for structuring data into electronic form from their paper-based equivalent. They comprise syntax, the message design rule and directories. Message design rules refer to technical design rules to compose a message in a set format. Directories are building blocks of messages, which comprise codes, data elements and segments. Three EDI standards widely used world over are ANSI X.121, UNTD12 and EDIFACT3. A business is required to select a specific EDI standard for Information Interchange. The selection of standard is usually based on the kind of industry in which the business operates, and the standards being used.

2. Software - Software enables data entry, and consequently to code it into the standard EDI format. Similarly, the software also decodes incoming information from the EDI standard format to the in-house format.

3. Communications - Information is transferred among partners through various media. Communication media enables the transfer of electronic business documents, between a large number of companies within and outside the country. It can be done through disks, tapes, private networks and others. Now, many companies have started using communication services of third party, by using Value Added Network Services (VANS).

After the three components are identified and set, the five main processes involved in EDI are -

- 1. Retrieving data from a computer system
- 2. Translating the data into a format that can be transmitted
- 3. Transmitting the message
- 4. Translating and interpreting the message at the receiving end
- 5. Downloading the data in the receiving compute applications

Answer: [b] Management Involvement.

Explanation: The components of EDI are standards, software and communication. However, the involvement of the management is essential for the successful implementation of EDI. The management has to co-ordinate activities so that the three components of EDI work effectively and efficiently.

Module:6

Reference No: M6012

Question: Access to the Electronic Funds Transfer (EFT) terminal should be restricted to authorised persons. The auditor need not-

- [a] Check the security of the place in which the terminal is located
- [b] Check whether or not the terminal is kept locked when not in use
- [c] Check the level of management supervision over the terminal
- [d] Check if there is a proper segregation of duties

Module 6 – Audit of Electronic Funds Transfer – Part 1

EFT is initiated through an electronic terminal, telephone, computer or magnetic tape. The term includes, but is not limited to Automated Clearing House (ACH) transfers, transfers made at Automated Teller Machines (ATM) and Point-of-Sale terminals (POS). This is first in the two part series on EFT audit.

The auditor must focus on the following:

To ensure that the EFT terminal is used by to authorised persons and functions: The audit of EFT involves identifying and satisfying the physical and logical access controls of various terminals and systems including the maintenance of such systems. In addition the focus should be on proper authorisation, authentication, integrity and confidentiality of messages. Finally the backup and recovery of procedures must be adequate enough to work in the event of a system failure.

1. Physical access:

- Check the security of the premises in which the terminal is located
- Check whether or not the terminal is kept locked when not in use
- Check if there is adequate supervision by the management for the terminal
- Identify security breaches that taken place previously and the controls put in place to prevent such occurrences in future.

2. Logical Access:

Find out how logical access is granted to users of EFT. Check if -

- It is through tokens, smart cards, pin card combinations or two or more control mechanisms.
- Control over the receipt, storage and issue of physical tokens, PIN or other access cards exists
- All persons having access to passwords and PINs given to users are identified. Also check the procedures available to keep such information confidential
- The system allows only authorised customers or all customers
- Passwords/ PINs are changed at regular and frequent intervals
- The system compels users to change passwords/PINs
- The system authorises only specific functions
- A session path is restricted to authorised persons or is open to all users
- A record of all attempts to work outside the authorised functions are available
- Scrutiny of the above record is done by a responsible person
- All violations of login either using wrong passwords or attempted unauthorised functions are logged, reported and proper actions is taken
- The Staff keeps the passwords confidential and secure

3. System maintenance procedure: Determine whether -

- A suitable and independent officer is put in charge of the EFT function and system

- There is a dual control over setting up of new users or changing authority levels
- A proper authorisation procedure is in place for making changes to user/functions
- A log of all the resources accessed is maintained by the system manager
- Access by the system manager is supported by properly authorised requests
- The management scrutinises all the resources accessed by the system manager
- A list of authorised users/ functions is available
- The list is approved by the management
- Controls exist to ensure that access rights are revoked when a person leaves the EFT section

To ensure satisfactory division of responsibilities surrounding the system: Determine whether

- There is a list of authorised users and their corresponding functions
- The functions are allocated in a way in which responsibilities are distributed
- There is segregation of duties between
 - Input and verification
 - Input/verification and authorisation
 - Input/verification and collection of output (Logs etc.)

To ensure that all messages are properly authorised: Determine whether

- The system has validated the terminal ID when a session is established
- Access to the system requires an authorised user to use a secure key
- The system ensures that all messages are authorised before transmission
- Transmission of unauthorised messages is prevented by the system
- Procedures exist for reporting unauthorised messages at transmission time
- Procedure exists for proper authorisation for input documents
- Controls are in place for reaching the daily/individual value limit for messages and if they are properly authorised

Answer: [d] Check if there is proper segregation of duties.

Module:6

Reference No: M6013

Question: Checks should exist in an Electronic Funds Transfer (EFT), to ensure that messages transmitted are delivered completely and are fully accounted for. The auditor should ensure that -

- [a] A permanent record of all transmitted messages is maintained
- [b] Messages are encrypted
- [c] All changes to a user function are properly authenticated
- [d] The system prevents unauthorised transmission

Module 6 – Audit of Electronic Funds Transfer – Part 2

EFT implies the transfer of funds initiated through an electronic terminal, telephone, computer or magnetic tape. The term includes, but is not limited to Automated Clearing House (ACH) transfers, transfers made at Automated Teller Machines (ATM) and Point-of-Sale terminals (POS).

This article is second in the two part series on EFT audit.

During the course of the audit of EFT, the auditor must focus on the following:

For ensuring that all messages sent are validated: Determine whether The messages are sent is a standard form

- If the standard form can be altered then there should be a proper control over the authorisation process for such an alteration
- Entry of validated fields is ensured by the system
- The system ensures that entries in the validated fields are in the required format
- Controls exist to ensure that the total value of a message is within the limit
- Amounts entered outside the expected range are reported by the system
- Controls exist to ensure that values outside the limits are not accepted

For ensuring that all messages are entered accurately and are transmitted without alteration: Determine whether

- Messages that need to be entered are re-typed/checked
- The messages are checked by the authorised officer to the original documents
- Original documents are appropriately endorsed at the time of input and authorisation
- Re-input and proving differences is enforced by the system
- Procedures exist for handling errors
- An input register is maintained
- Control totals for the number and value of the messages input are generated by the system
- Control totals are checked against input records
- Procedures exist for dealing with rejects
- Check sums and other similar checks are generated by the system
- Error detection and correction techniques are used by the communication protocol

For ensuring that messages are delivered and accounted for completely: Determine whether

- Each message is assigned a sequential serial number
- Messages are recorded in input documents/ registers
- The register/input document is scrutinised by the management
- A permanent record is kept of all transmitted messages
- Accepted/ rejected messages are checked against the permanent record
- Data in individual messages can be retrieved
- An audit trail is produced for all input messages which contain the following information
 - Unique message reference number
 - Date and time of input
 - The person who has verified or authorised the input
 - The person who has established the session path
 - Date and time of the transmission
 - Details of the message content
- The audit log is scrutinised by someone who is not involved in the input function
- There is accessibility to logs
- Transmitted and bank statements are regularly reconciled
- Originators are notified about the acceptance of the message

For ensuring that the system offers adequate provision for controlled recovery in the event of system failure: Determine whether

- The system provides for a record of accepted messages
- Procedures exist for the re-transmission of messages that are not accepted
- A log is kept of all interruptions of the normal processing

- Alternative terminals exist which can be switched on in case of hardware failure
- Written procedures exist for the above
- A process can revert to an alternative or manual system and if a procedure exists for it
- Controls exist to prevent duplication of messages
- Availability of other communication media that can be used in case of line failure

To ensure the confidentiality of message details held on local computer media and the security of messages in transit: Determine whether

- Messages are encrypted when they are received or sent
- Details of log files are encrypted
- Other history files are encrypted
- A local terminal allows dial in

To ensure that the EFT service is covered by an appropriate written legal agreement: Determine whether

- A written and signed legal document is in force for the EFT service
- The document is approved by the legal department
- The Agreement defines what constitutes an authorised message
- The agreement specifies accounts to which/ from which transfers can be made

Answer: [a] A permanent record of all transmitted messages is maintained.

Explanation:

- Ensures confidentiality and security of messages
- Ensures that there exist proper system maintenance procedures
- Ensures that all messages are properly authorized

Module:6

Reference No: M6014

Question: Generation of PIN in EFT/PoS involves -

1.Acquirer validates information 2. Acquirer sends response to the acceptor 3.Authorization request message is sent to the acquirer 4.PIN entered is encrypted

Which option indicates the correct order of events?

- [a] 1, 2, 3, 4
- [b] 1, 3, 4, 2
- [c] 4, 3, 1, 2
- [d] 4, 3, 2, 1

Module 6 - EFT - Parties involved and Security issues

In any Electronic Fund Transfer (EFT) the parties involved are -

- Cardholder - The person who makes the payment using the card
- Card Issuer - The organisation that holds the account of the cardholder, usually the provider of EFT/PoS (Electronic Fund Transfer at the Point of Sale) services
- Acceptor - The person/organisation that accepts payment through the card
- Acquirer - The link between various EFT/PoS terminals and card issuers

The transaction data is entered into the terminal by a cardholder. Then the authorisation request message is sent to the card issuer for various checks. After the card issuer validates the cardholder and the card, the acceptance response is sent back to the terminal.

Since there are a large number of terminals and card issuers, there is a need for an acquirer, to link these two groups.

Terminals may be grouped on criteria, such as geographical locations or communication patterns. Intermediation of the acquirer helps to simplify the communication flow. Direct communication between numerous terminals and card issuers helps to increase the number of transactions. The acquirer plays a central role in transaction processing, and in communicating with card issuers.

Security issues

Cards that are used in EFT/PoS, and ATMs are exposed to security issues. If an authorised person deciphers the PIN of the card, it can be misused. For instance, in case of ATMs, money can be withdrawn without the knowledge of the cardholder. Thus it is essential to protect the PIN. Therefore, a field, that stores cryptographic data related to the PIN, is included in the card.

When the PIN is entered, it is compared with the value of the secret key stored in the system that accepts the card. Terminals such as ATMs have secured and strong physical environment, where such keys are stored. It is very important to safeguard this key, as it is a global key, which is common to the whole system. The problem with the EFT/PoS terminals is that this global key cannot be stored there, as they are not physically safe.

In consequence, every time the PIN is entered, verification has to be done through a central system. The PIN is carried in an authorisation request message that is sent to card issuer through an acquirer. Since the PIN is carried in a message, the message has to be encrypted and the key has to be kept in insecure EFT terminals. Clever key management is required so that acquirer is not able to decipher the block of message that is received from the EFT/POS terminal.

In addition to the authorisation request message, there is a need to protect the response that is received from the acquirer. For instance, amount specified in an authorisation request message can be altered. Similarly, amount specified in the response message can be also altered. Thus it is important to maintain "message integrity" during both the authorisation request and response.

After validation by the acquirer, all transaction details are forwarded to the acceptor's account and, the transaction is settled between the card issuer and the acceptor.

Answer: [c] 4, 3, 1, 2

Module:6

Reference No: M6016

Question: Audit of LAN disaster backup and recovery plan ensures that business is restored after a system failure or disaster. Which of the following is FALSE with respect to such plans?

- [a] Plan identifies the critical hardware and equipments
- [b] Confidential information is not disclosed in the plan
- [c] Plan is reviewed and accepted by the management
- [d] Plan is communicated to the employees

Module 6 – Audit of LAN Disaster Backup and Recovery Plan

The audit of LAN disaster backup and recovery plan ensures the management that the LAN servers are properly backed up and they can recover and restore the business after a system failure or disaster. The auditor should perform the following tasks to ensure that the disaster backup and recovery exist, it is current and it is effective.

Evaluation of plans: Ensure that the plan documents

- Incorporate the names of key personals, their responsibilities and the respective telephone numbers
- Identify the level of disruption viz. part or total failure that effects the database, program files, application files etc.
- Describe the procedure and documents for levels of disruption.
- Identify the critical application software and data files.
- Identify the critical hardware and equipments.
- Identify the security requirements for alternative processing location.
- Identify the risk for each area – impact analysis, acceptable downtime and disaster definition.
- Provide for the service level agreements with hardware and software vendors.
- Provide for service level agreements with business users.
- Analyse the above agreement and note exceptions
- Identify if procedures exist for server and system shutdown and system restart and takes into consideration the following tasks.
 - Scheduling consideration
 - Backup journalising
 - Disk/ Tape archiving
 - Program sequence and dependencies
 - Retention of source documents
 - Re-input of data
 - Internal/ external reliance

Review of plan

- Ascertain if the plan has been reviewed and accepted by the management.
- Assure that the plan has been communicated to employees.
- Identify the person responsible for the plan.
- Ensure that the plan is current.

Testing of plans: For ascertaining that all the backup and recovery plans are tested on a periodic basis

- Ensure that all the data and program files, which are critical to the business, are available off site.
- Make a note of location of such files and the regular updates.
- Ensure whether the system can be reconstructed with the help of backups.
- Make a note of the last update.
- Ensure whether the system can be set up at an alternate site.

Identification of critical assets

- Ensure whether the management has identified critical systems and application data, file names, communication equipment, configuration settings, programs, documents, manuals and supplies. This includes the update and the last time a file or data identified as critical was added.
- Ensure that the management has prioritised applications on the basis of business need and risk analysis.
- Verify whether the provision for hardware recovery exists.
- Verify whether provision for hot site or cold site has been made.
- Verify whether the management has entered into vendor replacement agreements and reciprocal agreements.
- Identify interdependencies between business units, functions and/or application systems.
- Determine if the backups are properly labelled.
- Ensure that the stand alone PC applications are regularly backed and labelled.
- Ensure that the back up media like tapes, disc et al are is stored in a physically secure location.
- Determine whether the procedure has been specified for reinstallation of data and programs.
- Verify whether the employees have been familiarised on the necessity of backups and also that the management is following the guidelines with respect to the frequency of back up.
- Verify the frequency at which the users update the back ups in their local PC and whether the same is in agreement with the policy.
- Ensure that the backups are kept in a fire proof safe.

Failure of back ups

- Determine if proper procedures exist that should be followed when the backup fails.
- Determine if the logs are maintained for system failures.
- Identify the person responsible for reviewing the logs.
- Verify if any previous failures of back up had taken place.
- Ensure that the management has taken preventive measure to keep the problem from recurring.

Facilities and mirroring

- Ensure that the servers and special systems have a continuous power supply through use of Uninterrupted Power Supply (UPS) or any other means.
- Ensure that the UPS' are tested on a regular basis.
- Ensure that the power supply and other facilities are in accordance with the manufacturer's recommendation.
- Determine if critical servers and special systems are mirrored.
- Determine the consequences of unattended backup process.

Answer: [b] Confidential information is not disclosed in the plan

Module:6

Reference No: M6017

Question: It is widely accepted that every company should have a disaster recovery plan.

Importing of data (a component of LAN disaster recovery plan) does not help in keeping track of -

- [a] Equipment inventories
- [b] Policy inventory
- [c] Software inventories
- [d] Data that is necessary for the recovery process

Module 6 – Components of Successful LAN Disaster Recovery Plan

It is widely accepted that every company should have a disaster recovery plan. Without a plan even a BOND 007 cannot rescue the company from a disaster. But when management voices its need for a disaster recovery plan the general feeling is that management doubts the competency of the technical staff. Far from being so, the efforts of the technocrats is always laudable since it is they who frame and design the entire network of the company. The management should make it clear that at times other technical personnel could be called upon to handle the job in the absence of key personnel. The emergency can be handled smoothly if procedures and requirements are well documented. Hence it is necessary that equipments that are critical to the business operation should have a disaster recovery plan. It is cost-effective to negotiate the disaster recovery services with a vendor.

Components:

1. Equipment inventory:

The people concerned with the recovery and response should have an idea of what has been installed. For this purpose the equipment inventory constitutes an important components of a plan. The equipment inventory may include List of all equipments by type and model number

- Date of purchase
- Original cost of the equipment
- Name, address and telephone number of the manufacturer
- Local distributor of the equipment
- Location of third party equipment suppliers

The above details will help in taking quick decisions during a disaster.

2. Software inventory:

The plan should include all the software that will be required for operation of missing critical equipment. The inventory may include:

- The purpose which the software serves
- Acquisition date of the software
- License number
- Version number
- Original cost

3. Importing data:

Importing is a means of finding databases and repositories of information within the organisation that can be expected to stay up to date and then acquiring them for the plans. The information may be imported manually or over a LAN. Importing data is the best method to keep track of equipment inventories, software inventories or such data necessary for the recovery process. A link to the

accounting software, which ultimately records all purchases, would automatically update the equipment and software list in disaster recovery plan.

4. Contact Information:

The plan should maintain telephone numbers of personal and critical equipment vendors. It should also contain the names of the concerned persons connected with the disaster activity to be contacted with the home telephone numbers. All the telephone numbers should be current. The plan should be regularly updated when there is a change in the address or the telephone numbers of key persons and vendors. The best way to do is to import such information through object linking files in a LAN environment.

5. Other information:

The plan should have the diagrams and detailed information about the functioning of the company. The information may include -

- Inventory and report forms
- Carrier call out and escalation lists
- Maintenance forms
- Network schematic diagrams
- Contract and maintenance diagrams
- Special operating instructions for sensitive equipment
- Individual members duties and responsibilities

Disaster recovery plans are complex and can take more than a year to complete. The management must take this into consideration and decide whether the plans should be framed in house or should be outsourced. The important thing that should always be considered while framing this plan is that plan should not be in conflict with the overall plans of the organisation.

Answer: [b] Policy inventory

Module:6

Reference No: M6018

Question: Which image processing display technique is also known as point operations?

- [a] Pre-processing
- [b] Image coding
- [c] Local operations
- [d] Contrast enhancement

Module 6 – Image Processing

Images are two-dimensional data structures made up of picture elements or pixels. When any operation is carried out on an image, it is termed as image processing. Images displayed by computers are digital in nature. Hence, image processing is mostly concerned with digital data. To gain an insight into the features of image processing, a thorough understanding of image characteristics, operations and the like is essential.

Characteristics

Images contain large amounts of data, most of which is redundant in nature. Each pixel in an image is related to its neighbouring pixels.

Operation

The diagram below explains the operational flow for image processing.

Image coding: This removes redundant information and thereby reduces storage space. Digital cameras, videophones, video-conferencing and video on demand use image coding.

Image enhancement: Processing an image to make it viewable is termed as image enhancement. Application areas include medical imaging, astronomy, microscopy and publishing.

Image restoration: Restoring an image to its original form by learning about what actually caused its degradation is termed as image restoration.

Image segmentation: Categorises images according to a specific application.

Feature detection: Most of the time, only part of an image is useful for application. By using feature detection, one can create an image that contains information about the presence of certain types of features. Typical applications of feature detection include remote sensing, data analysis, feature location, character recognition and gesture recognition.

Pattern Recognition: It identifies complex arrangements of sensory stimuli as an instance of a particular type of pattern. It involves comparing sensory stimuli to representations in the memory. It often involves applying a label (or code) to the arrangement of stimuli. For example, classifying the visual pattern Z as the letter "Z", or recognising a visual pattern as a face.

What is digital image processing?

Customising digital images into data for specific applications, which involves manipulation and interpretation is called as image processing. In simplistic terms, it is nothing but analysing and manipulating images using a computer. Accordingly, three steps are involved:

- Importing an image either through an optical scanner or through digital photography.
- Analysing the image, which includes image enhancement and data compression.
- Obtaining the desired output.

Some widely used image display techniques include pre-processing, geometric correction, contrast enhancement, and spatial enhancement.

Pre-processing

This removes distortion, degradation and noise introduced during the imaging process. Pre-processing is done to produce a corrected image that is as close to the original as possible both geometrically and radiometrically. To improve the fidelity of the brightness value magnitudes, radiometric correction of remotely sensed data is performed. Geometric correction is related to improving the fidelity of relative spatial or absolute locational aspects of image brightness values.

Contrast enhancement

The aim of contrast enhancement is to improve the visual interpretation of an image. The techniques used are also known as point operations since they modify the brightness values of individual pixels in a data set separately.

Local operations

This is an enhancement technique that uses the values of an individual pixel and its surrounding pixels to improve spatial features. A local operation also modifies the value of each pixel based on the brightness values of neighbouring pixels.

Geometric correction

Digital images contain numerous geometric distortions. Geometric correction is used to make the data usable in tandem with other spatial data, like maps, GIS data.

Answer: [d] Contrast enhancement.

Module:6

Reference No: M6019

Question: Every organisation should have a contingency plan regardless of its size. Contingency plan should be detailed for the management and staff to actually act in event of a disaster. The contingency plan need not address -

- [a] Event declaration and escalation
- [b] Audit of the plan
- [c] Employee responsibility
- [d] Recovery operation

Module 6 - Guidelines on Framing a Contingency Plan

Every organisation should have a contingency plan regardless of its size. Contingency plan relates to anticipating any disastrous event and measures to tackle it. The disasters that should be taken into consideration may range from total loss of the computer center to fire or explosion, from loss of communication lines to disasters outside the control of the computer center.

Contingency plan should be detailed for the management and staff to actually act in case a disaster strikes. The contingency plan should address -

- Emergency response and evacuation procedures
- Damage assessment and emergency declaration procedures
- Management and employee notification procedures
- Recovery resources and logistics for mobilisation
- Event declaration and escalation
- Employee responsibilities
- Recovery operation
- Restoration procedures to return to back to normal business operation.

The following are some of the guidelines that must be considered while developing a contingency plan.

- Before formulating the plan the management must consider the business, technology or project risk to which it is exposed, and the the probability of its occurrence. The management should rank the it on the basis of the impact the risk will have on the organisation.
- The management should conduct a detailed analysis of all its assets and identify the assets that need protection and which are likely to be affected by the disasters.

- The management should document for each key business unit, the organisation structure, major functions, key computerised applications, critical internal and external data exchanges and geographical region and location of key business units and key third party supply chain and service providers.
- Plans framed should satisfy short, medium and long-term recovery. The short term should include all important systems and services, medium plans should include recovering of all systems and services on a temporary basis, and long term plans should include the total recovery of the processing environment.
- The plan should provide for recovery from the loss of the physical computing environment, which can be in the form of hot, warm or cold site. The disasters to which the organisation is exposed must be taken into consideration while considering the construction of the site.
- The plan should chart out the responsibilities for all the recovery processes. It should also contain the procedures for reproducing computer media, location of back-up media, priorities of recovery, sources of replacement hardware and software and alternative data communication facilities.
- The plan should also provide for the additional controls to be affected during recovery, the priorities for the recovery of each business function and should outline the procedures for keeping the plan current.
- The organisation should include a detailed restart procedure in its plans to be implemented when a disaster occurs.
- The authorised person who should implement all the procedures when a disaster occurs and coordinate all the people to function for the recovery of the business should be specified.
- The vendors of consumables must be identified and documented. They should be an assurance from the vendors that they can supply quickly the consumables when a disaster occurs.
- The manual procedures to be followed should be properly documented and the employees must be educated and trained about them.
- Lastly, the plan should be tested.

Answer: [b] Audit of the plan.

Module:6

Reference No: M6020

Question: A primary objective of BCP is : -

- [a] To provide a sense of security
- [b] To make systems reliable by providing back ups
- [c] To ensure continuity and survival
- [d] To minimise decisions to be made during times of disaster

Module 6 - Components of a Business Continuity Plan - 1

Many businesses are dependent on technology and automated systems, and any disruption to these systems may cause severe losses, and may even threaten the survival of the organisation. Thus, it is important to have a disaster recovery plan to cope with disruptions in the system.

The Disaster Recovery Plan is a comprehensive statement of actions that must be taken before, during and after a disaster.

Objectives

The primary objective of BCP is to reduce loss due to the failure of systems and operations, and to maintain organisational stability, while ensuring speedy recovery. Primary objectives may be divided into -

- Ensuring continuity and survival
- Ensuring protection of corporate assets
- Controlling risks and exposures
- Taking preventive actions and adopting a proactive approach to control business interruptions

Other objectives include -

- Providing a sense of security
- Making systems reliable by providing back ups
- Minimising decisions to be made during times of disaster

Components

- Involve the top management
- Set up a planning committee
- Perform risk assessment
- Establish priorities for processes and operations
- Develop recovery strategies
- Collect data
- Organise and document a written plan
- Develop a testing schedule
- Test the plan
- Approve the plan

In this article, we will focus on activities such as:

Involve the top management

The commitment of the top management is essential for developing an effective BCP. Besides, the initiative and monitoring of the plan, they should allocate adequate resources (financial and personnel) to the planning team.

Set up of a planning committee

A planning committee has to be set up for effective development, testing and implementation of the plan. The committee should comprise representatives from all functional areas. It should include an Operations manager and a Data Processing manager. The team should try to answer the following questions -

- What is a disaster?
- What are the ways to re-establish business operations?
- What is its impact?
- How much loss can the business sustain?
- What are the options available for re-establishment?
- What is the cost of implementation of the plan?
- How much should be spent on BCP?

Answer: [c] Ensuring continuity and survival.

Module:6

Reference No: M6021

Question: With respect to BCP, critical activities can be segregated into -

- [a] Essential activities, recommended activities, non-essential activities
- [b] Essential activities and non-essential activities
- [c] Recommended activities and non-essential activities
- [d] There is no segregation

Module 2 - Components of a Business Continuity Plan - 2

Perform risk assessment -

The planning committee should identify different risks that the organisation may face, and assess their impact on business. It should consider different types of disasters including natural, technical and human threats. The Business Impact Analysis should estimate losses that may be incurred; and costs involved in minimising losses and risk exposures.

Establish priorities for processes and operations

The next step is to focus on critical areas in each department, such as -

- Functional operations
- Key personnel
- Information
- Processing systems
- Documents and vital records
- Policies and procedures

Critical needs could include information, procedures and equipment that are required to continue operations in case a department, computer centre, building or all these entities are destroyed or cannot be accessed.

To identify the critical needs, each department should document the functions they perform. The functioning of each department should be observed for a period ranging from two weeks to one month, and the following points should be identified-

- The amount of time, the department can operate without existing equipment and resources
- List different tasks that are performed and their frequency (daily, weekly or yearly and rank them in order of priorities like Essential, Recommended or Non-essential.
 - o *Essential activities* are those activities, which when disrupted for more than one day would seriously affect operations
 - o *Recommended activities* are those activities, which when disrupted for more than one week would seriously hamper operations
 - o *Nonessential activities* are those activities, which have to be documented, but do not seriously affect operations, if not performed
- Identify personnel and equipment required for priority tasks
- Note lead times and measures necessary to make the equipment and personnel available in disaster situations

- List manuals and procedures used by each department, and steps to make them available during a crisis
- Specify temporary operating procedures to be followed in times of crises
- Mention the effect that the disruption of activities in one department has on others
- Identify persons in departments who would be responsible to implement the contingency plan

The above findings should be documented, with a special mention of critical activities in each department, and the minimum requirements of staff and resources to run operations.

Develop recovery strategies

An alternative plan to continue operations should be developed and evaluated on the basis of facilities, hardware, software, communications, data files, customer services, user operations, MIS, end-user systems and the like.

Depending on the processes that are involved in an organisation, the alternatives may be -

- Establishing a hot site, warm site or cold site
- Entering into reciprocal agreements
- Maintaining two data centres
- Maintaining multiple computers
- Arranging for service centres
- Entering into a consortium arrangement
- Entering into an agreement with a vendor for supplying equipment
- All the above

The alternatives selected should be documented and must cover the following points -

- Duration of the contract and the termination of conditions
- Testing of alternative arrangements
- Costs involved for each alternative
- Compatibility and inoperability issues
- Clauses on extension of services

Answer: [a] Essential activities, recommended activities, non-essential activities.

Module:6

Reference No: M6022

Question: Which step comes just before the final approval of the BCP?

- [a] Collecting data
- [b] Organising and documenting the plan
- [c] Testing the plan
- [d] Writing policies and procedures

Module 6 - Components of a Business Continuity Plan - 3

Collect data

The following is a list of information that has to be documented -

- Back up positions
- Important telephone numbers
- Inventory of communication equipment, documents and forms - equipment inventory should record all critical equipment. In cases, where the lead-time for replacement is long, then a back up for such equipment has to be in place.
- All requirements to facilitate replacement.
- List of vendors
- Inventory of computer hardware and software
- Inventory at offsite storage location
- Backup schedules

Organise and document a written plan

First, an outline of the plan should be chalked out, and the management should approve it. The outline should -

- Organise detailed procedures that are required
- Develop procedures
- Eliminate duplication of procedures
- Identify steps to be followed, before the complete plan is written

A standard format for writing procedures should be developed. This is essential, if many persons are involved in writing procedures.

The plan should mention job responsibilities of different personnel. It should also specify teams responsible for different functions, such as -

- Administration
- Facilities
- Logistics
- User support
- Computer backup
- Restoration
- Other important issues

Develop a testing schedule

Once the plan is created, a testing schedule should be chalked out. The plan should be tested at periodic levels, reviewed and modified. Procedures for the entire test should be documented.

Testing -

- Ensures reliability of back up plans
- Identifies areas that need to be modified
- Trains team managers and members
- Reveals the ability of the organisation to recover
- Motivates the team to maintain and update the plan

Test the plan

Once testing procedures are established, structured walk through tests should be done. Initially, testing of the plan should be done after office hours, so that normal business operations are not disrupted. Types of tests that can be carried out are -

- Checklist tests
- Simulation tests
- Parallel tests
- Full interruption tests

Approve the plan

After the plan is written, it has to be approved by the top management. The management should ensure that the plan is well written, and covers all aspects.

Answer: [c] Test a plan.

Module:6

Reference No: M6024

Question: Which of the following project scheduling techniques does not provide information about predecessor and successor relationships -

- [a] Gantt Charts
- [b] Critical Path Method
- [c] Program Evaluation and Review Technique
- [d] Critical Chain Path Method

Module 6 - Project Scheduling

Project scheduling is an important part of project management. It refers to the agenda that lists the time of execution of various activities. It acts as a controlling and monitoring tool and reflects deviations, if any, in the predefined schedule. Some of the scheduling techniques include -

- Program Evaluation and Review Technique (PERT)
- Critical Path Method (CPM)
- Gantt Charts

In the late fifties, the US Navy developed PERT to manage projects. Around the same time, Du Pont developed the Critical Path Method. Both these techniques involve drawing-up a network highlighting the relationships between different, critical and non-critical activities and their slack times (spare time available).

PERT involves graphical representation of different activities in the project and their interrelationships. It depicts the duration of a task and its dependent activities by forming a network of nodes and connecting them through lines.

CPM determines the minimum amount of time needed to complete the project. It is based on the methodology that certain tasks are dependent on predecessor tasks, and these tasks should be completed in a sequence in order to complete the successor task. There may be other non-sequential tasks, which may be accomplished along with these tasks.

The chain of events in a project is called a "path". The time taken for the completion of the activities on a particular path is called a duration. Thus "Critical path" is the path that takes the longest time to complete. Activities on the critical path are referred to as "critical activities". In short, it can be said that the critical path is the shortest duration during which the project can be completed. A delay in any activity on the critical path delays the completion of the project unless other activities on that path are speeded-up to compensate for the delay. CPM helps in scheduling many large and complex projects.

Gantt Charts - are also a type of graphical representation of different activities in a project and their time schedules. These charts show the starting and the concluding time of different activities and their progress. However, unlike CPM and PERT, it does not show the precedence relationship. In Gantt Charts, the X-axis represents the time and the Y-axis represents different activities. "[" represents the scheduled beginning of any activity at a particular time and "]" represent the scheduled ending of the activity. These two symbols are joined by the solid line (See figure below), which represents the schedule during which the activity has to be completed. Once the activity begins, another line is drawn below the schedule line to indicate the time at which that particular activity began and the time elapsed since. See figure below -

For instance, though activity 1-2 was started on time, it took longer than the scheduled time to finish it. While activity 1-3 took longer to initiate, it was completed on time. On the other hand, though activity 2-3 also had a late start, it was completed before the scheduled time.

Answer: [a] Gantt Charts

Module:6

Reference No:M6025

Question: The auditor should ensure that the policy has been formulated and communicated by

- [a] Asset profile
- [b] Liabilities profile
- [c] Technology environment profile
- [d] Relationship profile

Module 6- Prioritising Security - Part 1

Securing a company's data and network system is an uphill task. Finding the right balance between security and cost can be quite difficult. Despite several offerings on hand from vendors and several more suggestions from consultants, companies are often at a loss to decide how much to invest, and in what. The management has to channel security investment into critical security areas to obtain good returns.

Gartner G2, from Gartner Inc. has come out with a report, which details important elements to prioritise and structure security management in companies. It tells what to prioritise, how to structure and how much to spend.

To prioritise security management, a company should thoroughly understand, its own operations and the business environment. It can do this using the Security Profile Model, which consists of 6 types of profiles:

1. Enterprise profile
2. Asset profile

3. Cultural profile
4. Technology environment profile
5. Relationships profile
6. Existing security profile

The next step is to break down the security structure into six broad 'security responses'. They are as follows -

1. **Policies and plans:** They are security procedures and guidelines that are put down on paper, and guide the organisation in its security management process.
2. **People and management:** This deals with issues such as who to hire, how to educate personnel, and how to manage them.
3. **Technology:** This focuses on the technology (hardware and software) to be used in providing adequate security.
4. **Risk management:** This refers to plans, procedures to actively identify, control and mitigate risks.
5. **Physical security:** This aspect dwells on security procedures for physical assets and facilities
6. **Auditing, testing and monitoring:** These procedures help to assess the effectiveness of security measures periodically.

Now, that the security responses are clear, let's go back to analyse different profiles in detail. In this article, we will be dealing with only the Enterprise profile.

Enterprise profile

This profile focuses on corporate information with regard to its operations, competitors, level of regulation, size and geographical reach, and the risk tolerance levels of its stakeholders. Given below is an example of an enterprise, which tries to prioritise the security procedures on the basis of two factors - Regulation and Revenue.

Priorities

For instance, small companies with low revenues, operating in a highly regulated environment need to have policies and regular audits. Moreover, they may have low risk tolerance. Thus, risk management and business continuity should be prioritised over policies. On the other hand, large companies in highly regulated industries need to focus first on policies and plans, and then on auditing to minimise internal fraud and ensure fulfilment of legal compliance.

Small companies in less regulated environments have fewer resources, and consequently, their spending on security is low. Their priority should be human resource and corporate culture management. At the other end, large companies in less regulated environments may face high levels of competition and high employee turnover. Their priorities should thus be greater investment in technology, followed by people management.

The prioritisation process involved in the other profiles is explained in the subsequent articles.

Answer: [b] Liabilities Profile

Module:6

Reference No:M6026

Question: The responsibility of business continuity does not rest with

- [a] Management
- [b] IT operation
- [c] Auditor
- [d] None of the above

Module 6- Control Objective - To Ensure Continuous Service - Part 1

Continuous service implies that the users both internal as well as the outsiders should be provided with the required information under all circumstances so that the impact of operational disruptions is minimal. Continuous service does not relate only to providing services when a disaster occurs. E.g. An online booking system should be equipped to provide service throughout, irrespective of whether it is day or night, holiday or working day and whether the infrastructure is operational or not. The business continuity plan spans across the entire IT resources viz. people, applications, technology and data. The primary objective is the effectiveness and availability of resources and the secondary being efficiency. The responsibility of business continuity rests with the management and IT operations.

Management control

1. **IT continuity framework:** The management in consultation with IT users and IT operation should provide IT continuity framework. It should define the roles and responsibilities of people involved, the methodology to be adopted in ensuring business continuity and the procedure to be adopted in case of disaster management.
2. **Continuity plan, strategy and philosophy:** The management should ensure that the IT continuity plan forms a part of the short range and long-range strategic plan of the overall business. There should be incorporation of plans and procedures for IT continuity, maintenance and management of plan, testing and training and for appropriate backup procedures.
3. **Identification of critical IT resources:** The plan should identify critical IT resources. Critical IT resources are minimum information, procedure and equipments that are required to continue operations in case the department, computer centre, or the building is destroyed or cannot be accessed. This process should include all IT assets namely people, application, technology, facilities and data. They should be identified based on the amount of time for which the operation could be disturbed, the dependence of the assets on the business objective and an analysis of different types of disturbances. The disturbance can range from a power failure for a short duration to a disaster spanning a number of days. The users play a major role in identifying critical assets and assessing their criticality. The users in association with IT management should identify, document, prioritise and get the approval of management.
4. **Continuity plan contents:** Though the common objective in the plan document is continuity of operation and recovery process during disaster, the actual procedure would slightly vary depending on the circumstances. The management must ensure that the plan document contains the following:
 - Guidelines on how to use the plan for different circumstances.
 - Information about continuity teams, customers, suppliers, public authorities and media.
 - Response and recovery procedures for known and identified incidents.
 - Emergency procedures in case of identified disasters. E.g. If the plan is for an area that is prone to earthquakes, flood, hurricane and the like, then it should accommodate foresight.

In addition, guidelines should be available to cope with unforeseen contingencies like terrorist attack.

- Coordination and communication procedure.
- 5. **Back up plan:** As an integral part of continuity plan, it is important that sensitive data, information, programs and other software have back ups to ensure quick recovery from incidents or disasters. A reference can be made in the continuity plan with regard to policies on back up procedures.
- 6. **IT organisation and relationship:** The management should ensure that when the organisation structure is being defined, it includes the people who are responsible for handling the emergency situation. The ownership and custodianship of the plan documents, special equipments, hot/ warm sites, additional hardware and software purchased to cope with emergency should be identified and responsibility allocated.

Answer: [c] Auditor

Module:6

Reference No:M6027

Question: Responsibility of business continuity rests with the management and IT operations. To ensure this the management need not ensure which of the following:

- [a] The plan is tested
- [b] Plan is maintained
- [c] Plan is distributed to authorised people
- [d] Plan is static

Module 6- Control Objective - To Ensure Continuous Service - Part 2

Continuous service implies that the users both internal as well as the outsiders should be provided with the required information under all circumstances so that the impact of operational disruptions is minimised. Thus the service has to be continuous and not just restricted to the time of disaster. The responsibility of business continuity rests with the management and IT operations. The first part of the article covered management control. This is the second part that covers the IT operations and other related matters for ensuring continuity of service.

IT operations: With the management providing the guidelines for such service, it is the responsibility of IT operations to implement them.

Testing: A business continuity plan document is not a static document. The management should be satisfied that the procedures are such that they help in disaster recovery. The management should also ensure that the:

- Plans are current, relevant and usable
- Changes in circumstances would prompt changes in plan document.

Therefore the plan should be tested. This requires careful preparation by people, testing of equipments and the documentation of test results.

- **Training:** The concerned employees should be trained regarding the procedures to be followed in case of an incident or disaster.

- **Maintenance:** IT industry is one of the fast changing segments. It is one of the important functions of IT management to update the IT environment in line with the change in the IT and business scenario Business continuity plan if prepared with one set of IT environment and business environment, without updating loses its relevance. Hence there is a need for updating the plan document itself so that it reflects the current business and IT requirements.
- **Distribution:** A business continuity plan is a sensitive document of the company as it shows their preparedness vis-à-vis their competitors. It is important that individuals are well aware of their roles during emergencies, at the same time ensuring that only authorised people know the complete plan.
- **Minimising the IT continuity requirement:** An analysis of disturbances in the IT operations caused due to personnel, facilities, hardware, software and the like would give an idea of the causes of the disturbance to the IT operations. It is the responsibility of IT operations to identify such causes and to find out an alternate permanent solution rather than treat it as emergency or disaster event and following the disaster plan. In this way the IT continuity requirements should be minimised and kept for meeting most unexpected, non-repetitive and sudden incidents and disaster.

Others

- **Human Resource:** IT critical company should also provide for cross training, staff back up, to ensure continuity of service. Thus if the staff critical to IT operations have been effected by the disaster, they can be replaced by other trained personnel.
- **Insurance:** When planning for the overall insurance requirement of the company the insurance cover for disaster recovery and back up should be considered.
- **Third party services:** If the contingency maintenance is done through a third party service then before its deployment, an assessment should be made of their capabilities, experience, infrastructure, manpower and the utilities to be used by them.
- **Managing facilities:** All matters related to managing facilities by installation of suitable environment and physical controls, matters related to personal safety and the like should include a reference to business continuity planning and crisis management.
- **Independent assurance:** An independent assurance, of the effectiveness of activities critical to the continuity of the business including activities that are outsourced, should be obtained.

Answer: [d] Plan is static

Module:6

Reference No:M6029

Question: Factors such as Distribution channel and Target Segment are considered in which of the following profiles:

- [a] Cultural Profile
- [b] Relationships Profile
- [c] Technology environment profile
- [d] Existing security profile

Module 6- Prioritising Security - Part 3

A thorough understanding of its own operations and the business environment would help a company to prioritise issues and manage security effectively. The Security Profile Model, which consists of 6 types of profiles, is a very useful tool in this regard:

- Enterprise profile
- Asset profile
- Cultural profile
- Technology environment profile
- Relationships profile
- Existing security profile

In this article, we will be discussing the prioritisation process in the last three profiles.

Relationship profile

Relationships are critical to any business, but they also have a flip side – they necessitate greater security measures. Points to consider here are:

- Dependence on B2B and B2C relationships
- Dependence of such relationships on electronic data exchange across networks
- Dependence on real-time interaction through electronic systems
- Level of physical interaction on the shop floor level, through mail, exchange of paper and so on
- Sensitivity of such information

Two important factors that need to be considered are channels that will be used and the target segment. The following diagram suggests the security responses to be prioritised.

Companies that depend heavily on physical interaction to maintain B2B relationships should prioritise auditing to ensure continuity of channels. This is required, for instance, to prevent breakdown in delivery of goods or services, or fraud by employees of either side. Thus physical security is important. Those that maintain B2B relationships through digital channels need technology-based solutions to prevent attacks and errors.

B2C companies using digital interaction channels should set up auditing for fraud, and improve overall risk management. Employees of B2C companies using physical channels of interaction should be trained and made aware of the need for security, so that they can limit losses and simultaneously maintain good relations with customers.

Technology environment and existing security

It is essential to assess the technology environment of a company. This is something more than merely taking inventory of software and hardware; it's about considering the security of each software and hardware that is used in the organisation. For instance, if the employees are connected to the network through an intranet, then care should be taken to ensure that employees do not gain access to files that are confidential.

Existing security: It refers to evaluation of security measures that are currently being used. It checks whether the proper policies, organisation structure, training procedures are in place. Two factors that should be assessed while prioritising the security, using this profile are: degree of technology solutions used by the organisation, and the management structure required to support the security.

Conclusion

The company should thus evaluate its security management in accordance with the above criteria,

raise accountability levels, educate employees and ensure that major security gaps are bridged.

Answer: [b] Relationships Profile

Module:6

Reference No:M6032

Question: Which one of the following forms a part of transmission control in EDI control layers?

- [a] Interchange
- [b] Functional group
- [c] Transaction set
- [d] None of the above

Module 6- EDI- Overview

Definition

EDI (Electronic Data Interchange) refers to the exchange of information between two computers as per the Industry standards. Here, trading partners (parties sending and receiving information) exchange information through computer systems (electronic media).

One of the variants of the information systems through computers is Direct Exchange (DEX). Here the exchange of information takes place directly from a hand-held computer to a business application system.

Attributes

1. .It is unconnected to the normal application systems of the trading partners.
2. .It links and connects to the trading partner's internal application.
3. .It can be operated on any platform and is independent of the application systems used by the trading partners.

Process

The process involves assembling of data by the sender, translation into EDI standard format by a translator, transmission of the translated data either directly or through VAN (Value added network) and de-translation of the EDI transaction set into usable files by the receivers business application systems.

Benefits

- Convenience: The paperwork to a large extent is reduced. It also reduces the need for large number of clerical staff and hence the operation costs involved in the process.
- Error-Free: Due to minimum human intervention, inbuilt computer control mechanisms and the process of automatic reconciliation, exchange of information is relatively error-free.
- Timely operations: This method provides for a faster communication.

EDI Standards

Specific Industry standards are available for exchange of information electronically. Standards are specific rules for formats of business document for its electronic exchange. These standards help in uniformity of formats and ensure that a common language is used by the industry to exchange

information.

EDI Control layers

There are three control layers that surround the business document. They are

The interchange: This is the transmission control layer. This serves as an overnight express mail. All data to be transferred from one location to another location is contained in this. Each envelope (interchange) is identified and given a unique number.

The functional group: This is a like internal envelope wherein documents of a similar kind are grouped together. This the second of the control layers enveloping a business document.

The transaction set: This is like a unique communication document. This acts as a uniform format for the transmission of a business document.

Different message standards are available for different types of business communication. These include Purchase orders, invoice, electronic funds transfers, payment advice, statements, promotion announcement, functional acknowledgement and the like.

Transmission

There are three kinds of transmission routes available for data transmission

1. Value added network
2. Interconnect transmission
3. Direct Transmission

Value Added Network: Here the exchange is conducted through a Value added network or a service provider. The service provider acts a clearinghouse for transfer of data. VANs also act as a storehouse and an archive wherein data can be retrieved or sent a second time if necessary. They also send messages for the purpose of tracking transmission success.

Interconnect Transmission: In this type of transmission the message is first sent to the sending partner's VAN, then transferred to receivers VAN and finally to the receivers application. This situation arises wherein different VANs are hired by both the sending and the receiving trading partner.

Direct transmission: When data is directly transferred from sender to a recipient's application system it is called a direct transmission. Unlike in a VAN transmission, the management of traffic, security trails and the like is to taken care of by the individual trading partners. This is the most economical way of exchanging data when large volumes have to be transferred.

Answer: [a] Interchange

Module:6

Reference No:M6034

Question: Which of the following is not an EDI risk?

- [a] Segregation of duties is not possible
- [b] Audit trail may not be available for transactions which are in electronic format
- [c] Data that is transmitted is always error free
- [d] Dependency of trading partners on each other increases

Module 6- Risks in Electronic Data Interchange

The advent of Electronic Data Interchange (EDI) has facilitated buying, selling and trading of information. EDI is the transfer of data between different companies. Usually companies use the Internet for transfer of data. However, the Internet is an unregulated media and poses security risks.

Though EDI has brought about tremendous changes in the way business is done, there are certain risks associated with it. The company should take into consideration the following risks before it implements EDI:

Functionality: When EDI is implemented it should be ensured that it is functioning properly. Any lacuna in the system would adversely affect the company's relationship with its customers and vendors, and even business.

Dependence: With EDI, mutual dependence of trading partners increases. For example, a manufacturing unit will have to depend on its trading partner to supply the just-in-time inventories. If the trading partner is not able to deliver on time then his work will be held up.

Proprietary information: When business is done through EDI, information is exchanged between the two parties. Some of this information may fall into the competitor's hands. For example, price lists, manufacturing schedules, R&D information and the like.

Segregation of duties: There is not much scope for segregation of duties in an EDI environment. It involves less number of people and emphasis on internal control increases. If there is a lack of control then this may have serious repercussions on the business. For example, it may lead to payment to fictitious customers or excessive payments to vendors.

Inaccurate data: If the communication channel is not error-free or if there is some disturbance, there are chances of either loss of transaction, receipt of inaccurate or corrupt data.

Audit trail: EDI means a paperless environment. For the purpose of audit, audit trails need to be developed. It should be seen that the same is incorporated in the EDI environment.

Internal controls: In an EDI environment, any error will affect numerous transactions causing huge losses. With no control mechanism present, the business will receive a setback as the customers and vendors will no longer rely on the system and the company. Therefore, internal controls should be put in place to reduce the losses.

Software failure: For EDI it is necessary that each party meet its commitment on the due date. If the software fails then the management would have no information about the dates on which it has to meet its commitments. This refers to payments that would attract penalty if not made in time, renewal of insurance, warranties, AMC and the like.

Legal liability: The trading partners should define the terms and condition specific to business in order to avoid any legal liability in future. It should also specify the laws to which it is subject to and the jurisdiction.

The company should implement EDI after taking into consideration all the business risks.

Answer: [c] Data that is transmitted is always error free

Module:6

Reference No:M6035

Question: Which of the following is TRUE in relation to the input controls of EDI ?

- [a] The data that is entered into the system should have sequence numbers
- [b] Data that is entered into the system need not be translated to EDI standard
- [c] Parity and redundancy checks should be used
- [d] Any changes to EDI should be tested before implementation

Module 6- Internal controls - EDI Part 2

Electronic Data Interchange is the application of computer and communication technology to the traditional business environment. It is the transmission of business transactions from one company to another in a standard form using an electronic communication network. Though the benefits of EDI outdo the costs, it can be reverse if proper controls and security measures are not implemented. In this article we focus our attention on controls. The controls can be classified into two - internal and external. While internal controls deal with application system and communication interface, external controls deal with proprietary networks connected with trading partners and the VANs.

The controls help the management in achieving its organisational goals and objectives. But this is possible only when controls are properly designed and implemented. Proper controls ensure that

- Any error in the EDI process does not affect other applications and programs.
- Applications are protected from errors and unauthorised access.
- Accurate and secured information is transmitted.

We would now discuss in detail the internal controls for the EDI process.

General controls: These controls are for general application and not related to any specific EDI process.

- The transmission of data should be at scheduled times. The trading partners should decide the time.
- The period for which data and other information should be retained should be decided.
- A back up, recovery and contingency plan should be formulated. The test should be conducted for testing the plan. The plan should not be static and must be updated when changes are made to the EDI functioning.
- Data centres should be physically secured. The physical controls should be the same, as it exists for other systems.
- Access control mechanism should be built in the system, which restricts the access to data and files based on access authorisation table.
- Where required, the transmission of data should be in encrypted form. This should be decided between the trading partners as to whether all the transactions would be sent in encrypted form or otherwise.
- EDI standard should be decided and the same should be followed. Changes if any, should be decided with the trading partner before they are incorporated.
- The trading partner agreement should spell out clearly the terms and conditions especially the dispute sensitive areas.

- Similarly written agreement should be drafted for the services of VAN provider.
- Changes if any, to EDI should be tested and properly documented for all the changes.

Input controls: Input requires an establishment of an interface for translating the transaction from the application system being using by the company to the format used for EDI system. Input controls should ensure that

- The data that is entered into the system has sequence numbers. Batch totals are computed and assigned for transactions.
- Data that is entered into the system is properly translated into EDI standard.
- All inputs that are not accepted are transferred to a separate file say a suspense file.

Processing controls: Processing stage should ensure that parity and redundancy checks are being used.

Output controls: Output controls ensure that the output is as desired by the system. An interface should exist at the receiving end for translating the transaction from the EDI system to the application.

- Edit checks test for accurate, complete and valid input. Edit checks should check for accuracy and completeness of data before they are transferred to the application at the other end.

Answer: [a] The data that is entered into the system should have sequence numbers.

Module:6

Reference No:M6036

Question: Internal controls of EDI should address which of the following risks?

- [a] Storage errors
- [b] Transmission errors
- [c] File errors
- [d] Accounting errors

Module 6- Internal controls - EDI Part 1

Electronic Data Interchange is the exchange of the business documents between companies. It is computer-to-computer exchange using a standard public format. EDI has bridged the information gap that had existed previously between companies with different computer systems, as different platforms or communication equipments among trading partners no longer limit its use.

The emphasis on internal controls is not lost in EDI environment. The implementation of internal control is the responsibility of the management. When internal controls are planned, it would be better if the internal and external auditors are present. This helps in including all the required controls initially as once the system starts functioning it will be difficult to bring about changes.

The changes due to implementation of EDI when compared to the non- EDI environment are as given below. They should be kept in mind while internal controls are planned for.

- Most of the controls would be automatic. This leads to reduced manual intervention as all the controls would be designed in the programs.

- Unchecked errors would affect many transactions before it is realised that an error has occurred.
- The accounting procedure would be substantially changed as EDI means paperless environment.
- No physical audit trails would exist for the electronic portion of the transaction. The system should be designed such that audit trails are maintained electronically. If audit trails are not maintained then there would be no way to know how the transaction had commenced, the stages of its process and how it had ended.
- The security of data and information are very important, as lot of sensitive and critical data would be shared between the EDI parties.
- Segregation of duties would not be possible and an individual will be performing many tasks.

The authorisation process would be changed and the system should provide a field for authorisation within the system the access to which should be restricted.

Controls should address the following risks:

- Transmission errors: A standard format should be decided between the parties as to the format in which the information would be transmitted. If the format is not the same then the parties can know that there has been some error in transmission.
- Translation errors: The widely used EDI standards are in ANSI. There should be control to ensure that these ANSI transmissions are properly converted by the translator application for the application software.
- Reasonableness checks: The company receiving the information has to ensure that the information received is correct. For this purpose, reasonable checks should be in place. This reasonable test checks the data against a predetermined reasonable limit.
- Manipulation of data: There are high chances of manipulation of data during its transmission. Data can be manipulated even in old archives and the active transaction files. There should be a mechanism whereby all changes made to the records should be recorded by the system so that they can be later reviewed and exception reports prepared.
- Authorised messages are sent and received: Control should exist for ensuring that all the messages and information that is transmitted is received only by the trading partner and vice versa.

The controls should be applied to both inbound and outbound transactions.

Answer: [b] Transmission errors

Module:6

Reference No:M6037

Question: Many organisations do not stress on security measures because

- [a] They don't think that the investment on security will provide any returns
- [b] They think that their systems are secure enough
- [c] They think that losses due to security breach will be less than the investment on security
- [d] They think that they can tackle the situation when the crises will occur

Module 6- Return on Security Investment

In March 1998, an organisation in Boston, England caught fire. Although the fire was extinguished by 32 automatic sprinklers the incident should serve as a valuable lesson in security.

Many organisations are reluctant to invest in security products, unless they are guaranteed a return on their investment.

Absence of benchmarks

The plight of data security vendors and consultants is no better since they are unsure of the benefits the security measures would accrue to the organisation. Companies on the other hand are reluctant to invest until they are assured of a Return On Investment (ROI). This, despite being aware of the vulnerabilities like loss or damage of data and security breach. The problem has been compounded by the absence of a Return On Security Investment (ROSI).

The only return companies can be certain of is that the expenditure on security measures would prevent losses from security breaches!

Research is on, to develop methods by which the return on security investment can be calculated. However, various research groups have now developed a few basic ROSI models. These are explained below:

Tangible Benefits

Researchers at the *University of Idaho* have developed a formula for calculating the ROI by using intrusion detection, as a protection. The research team installed an intrusion detection box on the periphery of a network. Incoming data that followed a specific pattern was to be investigated. The team also assigned values to the cost of:

- Tangible assets in terms of dollars, and also accounted for depreciation.
- Intangible assets by assigning relative values. For example, software B is thrice as valuable as software A.
- Different types of hacks, based on an existing and widely accepted taxonomy by the US Department of Defence

The team came up with the following formula:

$$ALE = (R-E) + T$$

where,

ALE is the Annual Loss Expectancy

T is the cost of the intrusion detection box

R is the cost per annum to be recovered from any number of intrusions

E is the savings arising from preventing intrusions Thus,

$$ROSI = R - ALE$$

The team simulated common types of network hacks to determine if the simulated costs matched the theoretical ones. Both costs matched.

They now had figures to prove that investment in security yielded tangible benefits. The intrusion detection system cost \$40,000. It proved to be 85% effective on a network, which was expected to lose \$100,000 per annum due to security breaches. The detection system thus yielded an ROI of \$45,000.

Need for further research

The above research provides important insights into the benefits of investing in security at an early

stage. However, if companies were to adopt the techniques outlined, further research would be required. Moreover, not all companies would be willing to disclose information on the flaws in their security.

Conclusion

Nevertheless, the results of these studies seems convincing enough for the top management to invest in security. This would help new technology to develop faster. More research would also help insurance companies to provide hacking insurance, the rates of which would vary depending on the kind of security measures in the company's network.

Answer: [a] They don't think that the investment on security will provide any returns

Module:6

Reference No:M6038

Question: In a credit card transaction, the equipment that is used to verify the cardholder's authenticity is called

- [a] Point of sale device
- [b] ATM
- [c] Hand held device
- [d] All of the above

Module 6- Credit card processing-basics

Introduction

Payments through credit cards are one of the convenient modes of payments now available to the customers. There are 2 kinds of credit card processing - a normal credit card processing and an online credit card processing. Online credit card processing has been described separately.

The parties involved in both the types of transactions are:

Merchant Bank: The bank that contains the account of the merchant or the provider of service

Acquiring Bank: This is a specialised bank, which manages the credit card transactions for the merchants or the service providers.

Credit card network: This connects the acquiring bank and the issuing bank

Issuing Bank: The bank, which issues the credit card

Equipment required for credit card transactions

The equipments that are required may vary depending on the types of customers; the number of customer a merchant caters to.

However the most common types of equipment utilised now are

Point of sale terminals

This terminal is used to verify the available credit limit of the prospective customer. The terminal is normally connected to the merchant account provider via a leased line or dial up network. Or it may be connected to a computer system. The customer swipes the credit card and verification is done real-time.

Card Present Service (Terminals)

The point of sale devices is connected into these terminals.

Card Not-present service (Mail/phone)

This terminal is useful when there are mail orders, and low volume phone orders. The transactions are fed into either the computer system or a point of sale terminal. This data can be automatically integrated into the existing database of the merchant. This is a software, which can be loaded onto the existing computer system of the merchant. This is connected to the merchant bank's network through a leased line or the dial up method.

Card Not-Present Internet Application Service (Phone)

This service is required if the volume of phone transactions are high. Here too, verification is in real time. This requires a dedicated Internet access.

Merchant Account

A merchant account is like any other normal bank account held by a merchant. But these accounts are specifically set up for the purpose of credit card transactions. It acts as an intermediary for collection of funds from credit card purchasers and disbursement to the merchant account.

Services provided by merchant account

Some of the services provided by the merchant account banker or a third party service provider (on behalf of the merchant bank) include credit card authentication, settlement of funds from credit card companies or associations, deposit of funds into checking account, activity reporting of the merchant account and merchant billing.

Answer: [a] Point of sale device

Module:6

Reference No:M6039

Question: Which of the following statements is not true with regard to payment gateway based online credit card processing?

- [a] Payment gateway helps in protecting the credit card data during transmission.
- [b] Payment gateways generally use encryption methodology to provide security to credit card info
- [c] Payment gateway authenticates the payment card.
- [d] All of the above

Module 6- Gateway based Online Credit Card Processing

Introduction

This is the first of a two part series on "gateway based online credit card processing". In this article, we have discussed the basics of the online processing through payment gateways. In the

subsequent articles, we have discussed the actual processing of the payment gateways, different facilities available and the types of payment gateways.

Online credit processing

It involves the following main activities

1. Customer sends the credit card information like card number, name, billing address and the like through the Internet.
2. This information is forwarded to the acquiring bank
3. The acquiring bank forwards the transaction data to the card-issuing bank
4. The issuing bank performs the security checks for correct name, funds available, number authentication, address verification and the like.
5. The issuing bank notifies the acquiring bank through the credit card network whether the transaction is approved.
6. The merchant sends the request to the acquiring bank for funds.
7. The acquiring bank forwards the requests through the network to the issuing bank
8. Transactions are settled, when the issuing bank transfers the funds to the acquiring bank, which in turn transfers the funds to the merchant bank.

Payment Gateways

Payment gateway acts as an intermediary between the merchant (seller) and online buyer with their respective banks/financial institutions. Merchants utilise their gateways to process their credit card transactions. It is a third party network, which links the online e-commerce portal to the banking/credit card network. It provides a safe route to the merchants to process their transactions over a secure Internet connection.

Activities

Information of credit card transactions is extremely sensitive. So all efforts must be made to prevent any exploitation of this vital information. Payment of gateway facilitates in the provision of the security features to the transmission. Most of the gateways use the encryption method of securing the data to prevent the unauthorised use of the credit data. Secure socket Layer (SSL- This is explained in a separate article.) is the current industry standard to prevent data tampering. Specifically the activities performed by a payment gateway are as follows

- Collection of data from the web portal.
- Certification of the data
- Encryption of the data
- Routing of the data
- Translations and decryption of the data

Technology

The payment gateways use the "Secure Electronic Transaction" encryption technology to protect the on-line transactions. This technology secures payment information in the following manner:

- Authentication that the merchant is authorised to accept online card payments
- Authentication of the payment card
- Advanced encryption system to secure personal payment system during transmission of data
- By ensuring that data is received only by the intended recipient

Benefits

Quick authorisation: Credit cards are authorised in real-time.

Security: It provides a secured link buyer, seller and the banking network.

Efficiency: It provides for an efficient transfer mechanism.

Customer friendly: Refunds are easily granted to the eligible customers.

Reports: Reports can be easily generated in real-time

Settlements: It provides for multi currency settlement.

Answer: [d] All of the above

Module:6

Reference No:M6040

Question: ----- is the most advantageous payment gateway access when orders are mostly received through phone or mail

[a] Real time processing solutions

[b] Weblink

[c] API

[d] Virtual Terminal Solution

Module 6- Gateway based online credit card processing -2

This is the second and concluding part of the series on gateway based online credit card processing. In this article, we have discussed how a payment gateway works.

The working

The functions of a payment gateway can be broadly classified into 3 categories

1. **Authorisation:** Verifies if credit can be extended to the prospective customer.
2. **Clearing:** This is similar to any normal clearing performed by a bank. It transfers the credit card transaction data to the banks to facilitate the receipt of funds
3. **Reporting:** The payment gateway facilitates obtaining comprehensive reports of the transactions. The transactions can be viewed using the payment gateway facilities.

Authorisation

Every prospective credit card transaction must be authorised by the issuing bank (the bank which issued the credit card). An authorisation request is sent to the issuing bank by the payment gateway. The request could be answered in any one of the three ways.

- **Accepted:** The issuing bank authorises that the transaction can go ahead for a sale.
- **Rejected:** The bank rejects the card for any further processing
- **Invalid Data:** This indicates a problem with the card details, invalid numbers etc.

Clearing

The payment gateway uses batch processing for funds settlement of transactions. At the end of each day, all transactions of a particular merchant are grouped and transferred to the merchant's bank. This process is called the clearing. It may take 3-5 days before the merchant account

receives the final funds. In the process of settlement, two scenarios can emerge. Either the batches are accepted or rejected. In case of rejection, it is the responsibility of the gateway to rectify the batch and resubmit it.

Reporting

Payment gateways also provide the service of recording all the transactions and providing transaction reports to the merchants. These reports can be viewed from the website, transferred to the applications of the merchant for further processing and the like. Some of the common types of reports given by the gateway are

- All transaction report, which indicates all the transaction conducted through the website
- Transactions settled, which refers to those transactions that have been sent to the issuing bank.
- Not yet settled - refers to the transactions yet to be sent to the issuing bank (similar to current transactions).

Access to payment Gateways.

Payment gateways can be accessed by the merchants in one of the three ways: Web link, API, and virtual terminal

Web link: This is one of the real-time online credit cards processing system. Web link use the HTML for linking the merchant website to customisable payment pages on the payment gateway's servers.

API: Here the payment pages are located on the servers of the merchant. Using the application programme interface, the data on the payment pages is transmitted to the gateway.

Virtual Terminal: This is an Internet based application and the transactions are entered by the merchant one-by-one through a browser. This is useful for merchants who have more mail or phone orders.

Virtual terminals are much more faster than the standard dial-up authorisation systems.

Answer: [d] Virtual Terminal Solution

Module:6

Reference No:M6041

Question: The overall objective of designing application controls in framing long term and short term IT plans to ensure

- [a] Accuracy
- [b] Consistency and validity
- [c] Completeness, accuracy and validity
- [d] Consistency, validity, completeness and accuracy

Module 6 – Control objectives for implementation block

Data management

Introduction

Application and general controls are essential features that are to be incorporated into the design of the application system. This article has been dealt in a two part series. This is the first part..

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To ensure that data remains unchanged, complete, accurate and valid during input processing, output and storage.	To ensure integrity of the information generated by the system.	1. Data preparation controls 2. Input, processing and output controls 3. Back up and recovery 4. Library management 5. Data ownership 6. Data administration 7. Data integration and consistency 8. Legal requirements	• Data

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

Not applicable for this activity

II. Operational Controls

- **Source document controls:** The application controls designed should take into consideration the following control objectives:
 1. An established data preparation procedure. The data origination forms should be designed to prevent errors and omissions. The procedure established should consist of error handling mechanism.

2. Authorisation of source document by an appropriate authority with due consideration to principles of segregation of duties.
 3. All authorised documents are accounted for and transmitted for input in a timely manner.
 4. Source document should be retained for a considerable period to facilitate recovery and to comply with legal requirements.
- **Data input controls:** The application controls designed should take into consideration the following control objectives:
 1. Authorised personnel only must carry out data input.
 2. Controls exist to ensure completeness, accuracy and validity of the data that is being input.
 3. Error handling and management.
 - **Data processing controls:** The application controls designed should take into consideration the following control objectives:
 1. Principles of separation of duties.
 2. Update controls like run-to run controls, batch controls, and master file update.
 3. Validation controls.
 4. Authentication and editing controls.
 5. Error handling and management.
 - **Data out put controls:** The application controls designed should take into consideration the following control objectives:
 1. Procedures for retention of output.
 2. Procedures for distribution of output.
 3. Procedures for balancing of output with control totals.
 4. Audit trails to facilitate reconciliation.
 5. Review of output.
 6. Error handling and management.
 7. Security considerations.
 - **Security measures during transmission:** The process adopted should ensure that data is not modified, used by unauthorised sources during transmission and transportation. Additional security measures should be taken to ensure that data is protected during transmission over Internet or other public network.

Answer: [d] Consistency, validity, completeness and accuracy

Module:6

Reference No:M6042

Question: E-transaction security measures should be adopted to ensure the following attribute of information

- [a] Durability
- [b] Consistency
- [c] Completeness
- [d] All of the above

Module 6 – Control objectives for implementation block

Data management-2

Introduction

Application and general controls are essential features that are to be incorporated into the design of the application system. This article has been dealt in a two part series. This is the second part.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To ensure that data remains unchanged, complete, accurate and valid during input processing, output and storage.	To ensure integrity of the information generated by the system.	1. Data preparation controls 2. Input, processing and output controls 3. Back up and recovery 4. Library management 5. Data ownership 6. Data administration 7. Data integration and consistency 8. Legal requirements	• Data • Technology

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

Not applicable for this activity

II. Operational Controls-contd

- **Protection of disposed information:** Procedures should exist to ensure that unauthorised internal parties or external sources do not have access to data deleted or disposed.
- **Storage management:** Procedures should be adopted to manage the storage of data and its retrieval taking into consideration cost effectiveness and security. Policies should be

established for retention periods and terms of storage for data, programmes, messages as well as data like keys and certificates used in encryption and authentication.

- **Media Library Management:** A media library management procedure should be adopted. The contents of the media library should be inventoried as per established policies. Regular verification should be conducted and discrepancies verified and rectified. The integrity of the data contained in the library should be maintained. House keeping procedures should be adopted to protect the contents. Procedures should be established for identification, movement of the media contents, responsibility for media content and accountability.
- **Backup and recovery:** A well-defined backup strategy, which satisfies the business requirements as well as the recovery plan of the organisation should be adopted. It should also be ensured that backups are taken as per the defined policies Adequate procedures also must be designed to ensure the storage of back ups in the right media and for adequate time. Back-ups should be stored both off-site and on-site with adequate security conditions. It should be ensured that archiving policies of the organisation meets the legal and regulatory requirements.
- **Authentication:** Adequate security precautions should be taken to ensure that data originating from outside the organisations is checked for its authenticity and integrity. Such messages could be received through voice data, fax, network-public or other private networks and the like.
- **Electronic value security:** Due to the uniqueness of the nature of transactions involved, a separate security measure needs to be adopted for electronic transactions. The procedures adopted should ensure integrity for the following attributes of e-transactions.
 1. Completeness
 2. Consistency
 3. Durability
 4. Non-affectability by other transactions.
- **Integrity of stored information:** Procedures should be adopted whereby integrity of data stored is reviewed periodically.

Answer: [d] All of the above

Module:6

Reference No:M6043

Question: Which one of the following documents is **MOST LIKELY** to help the auditor in understanding the provisions made by the management for ensuring the continuity of business?

- [a] Insurance policies
- [b] Operational risk assessment
- [c] Job descriptions
- [d] Minutes of the IT steering committee

Module 6 – Audit working guideline

To ensure continuous service Part 1

Table of applicability

For IT task	Control objectives	
To ensure continuous service	Management controls	Operational controls

	1. IT continuity framework 2. Continuity plan, strategy and philosophy 3. Identification of critical IT resources 4. Continuity plan contents 5. Back up plan 6. IT organisation and relationship 7. Human Resource 8. Insurance 9. Third party services 10. Managing facilities	1. Testing 2. Training 3. Maintenance 4. Distribution 5. Minimising the IT continuity requirement

Audit Process

The audit process has been covered in two parts. This article is the first part, and deals with a preliminary understanding and analysis of the process.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. IT management 2. Operations team 3. Continuity evaluation and maintenance team 4. HR team 5. Users 6. Site management team 7. Off-site maintenance team 8. Insurance evaluation personnel	1. Policies and procedures with respect to • Continuity plans and strategies • Priorities • Testing • Backup • Training 2. Organisational policies and procedures relating to business continuity 3. List of users of business continuity plans 4. Recent outcome of the continuity plans 5. Criteria for prioritising applications 6. Contracts with vendors for services based on continuity plans 7. Insurance policies

Preliminary analysis

The next step is to analyse the effectiveness of the control measures adopted, and their reliability- This can be done by ensuring that the following are in place:

- The organisation's policies require the framing of business continuity plans covering all IT functions
- The following are provided in the IT policies and procedures
 - o Need for developing continuity plans
 - o Prioritising applications on the basis of time and returns, to take appropriate actions in

- case of catastrophe
 - o Risk assessment and appropriate insurance for the loss of business in continuity conditions
 - o Roles and responsibilities of different personnel
 - o Agreements to be entered in with the vendor for providing of services in case of recovery or business resumption
- Continuity plan is in place and provides for the
 - o Recovery procedure based on long range plans
 - o Procedure for emergency situations
 - o Roles and responsibilities of IT personnel, users, vendors and any other personnel involved in business continuity
 - o Addresses of key personnel
 - o List of various alternative resources that should be provided for. Image system, fax system, paper documents, telephones and the like are also included in the list of resources besides other IT resources
 - o List of applications, and their priority, recovery time and the performance desired
 - o Provision for communication and support services
 - o Recovery strategies for different situations including a detail step by step recovery procedure
 - o Training of personnel in the organisation
 - o Testing and evaluation of the results of the test
 - o Modification of the plan based on the above evaluation
 - o Location of the back up resources including the operating system, applications, data, manuals and the like
 - o Business resumption plans for users when resources are provided
- Requirements of external agencies and government regulations

The next article focuses on the second part - the test of controls and substantive testing.

Answer: [a] Insurance policies

Module:6

Reference No:M6044

Question: Which one of the following statements is "FALSE" with respect to the audit guideline on ensuring continuity of service?

- [a] The auditor should review contracts with vendors to obtain information on lead times
- [b] Relevant training is provided to users
- [c] Continuity plans are tested
- [d] The performance appraisal is done at the time of implementation of emergency procedures

Module 6 - Audit working guideline

To ensure continuous service Part 2

Table of applicability

For IT task	Control objectives	
To ensure continuous service	Management controls	Operational controls

	1. IT continuity framework 2. Continuity plan, strategy and philosophy 3. Identification of critical IT resources 4. Continuity plan contents 5. Back up plan 6. IT organisation and relationship 7. Human Resource 8. Insurance 9. Third party services 10. Managing facilities	1. Testing 2. Training 3. Maintenance 4. Distribution 5. Minimising the IT continuity requirement

Audit Process

The audit process has been covered in two parts. The first part covered a preliminary understanding and analysis of the process. This article is the second part, and focuses on the test of controls and substantive testing.

Test of controls

A clear picture of the functioning of controls can be gained by:

- Obtaining evidence
- Reviewing the deliverables

Tests: Before the auditor takes a stand on the functioning of IT tasks in the organisation, he should check whether

1. Continuity plans are in place and reflect the existing situation
2. Training is provided to all the users
3. The defined continuity plans, policies and procedures are followed and objectives met
4. Roles and responsibilities of appropriate personnel are defined
5. Plans have been tested and approved by the management, and appropriate corrective actions have been taken and documented
6. Agreements with the vendors are as per the plans
7. Provision for backups is made
8. The management has identified and prioritised vital data and operations

Tests should be performed to ensure that control measures identified in the preliminary analysis are functioning as desired.

Substantive testing

This step is undertaken to substantiate the auditor's viewpoint that control objectives are either not being met, or do not exist. The shortcomings in controls and their consequences also should be documented. He can also:

1. Identify comparative benchmarks from similar organisations and industries
2. Review continuity plans for their consistency with the organisational plans
3. Interview personnel to ensure that they understand their responsibilities

4. Ensure that the users and the senior management have reviewed the plans to make sure that all the required business needs have been provided for
5. Review the manual documents related to recovery procedure to be followed by the users in case of loss in the continuity of business
6. Review alternative resources to ensure that they are adequate in number
7. Review agreements with the vendor to obtain information on lead time and costs

Identifying shortcomings

The auditor should identify:

- Management plans to purchase any telecommunication and network components
- If written contracts exist for offsite facilities and if they are adequate
- Arrangements at the alternative site, if they are as per the requirements of the users
- If vendors and service providers have continuity plans
- Business resumption teams for migrating the processing from the alternative site to original site

Answer: [d] The performance appraisal is done at the time of implementation of emergency procedures

Module:6

Reference No:M6045

Question: Which of the following team needs to be interviewed with regard to auditing the procedures of data management?

- [a] Data base administration
- [b] Support team
- [c] Operations team
- [d] All of the above

Module 6- Audit working guideline

Data Management -1

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Data management	Not applicable for this activity	1. Source document controls 2. Data input controls 3. Data processing controls 4. Data output controls 5. Security measures during transmission 6. Protection of disposed information 7. Storage management 8. Media library management 9. Backup and recovery 10. Authentication

		11. Electronic value security 12. Integrity of stored inform

Audit Process

The audit process has been covered in a six part series. The first part covers preliminary understanding.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. Data base administration team 2. HR and training 3. Operations team 4. Application development team 5. Support team 6. Back-up and security administration 7. Critical Users	Policies and procedures of the entire organisation regarding the data management which includes - The data flow within the organisation and the IT function - Data originating points, editing points, processing points, output points, review points and correction and resubmission to users points - Source document authorisation - Data collection processes - Data tracking and transmission process - Error identification and rectification processes during data origination - Procedures adopted to ensure data integrity at the data origination point - Procedures to ensure data integrity during transmission over network/internet - Storage and archiving procures for source documents - Special considerations with regard to legal requirements or other regulatory requirements. - Interface between system provision and data usage - Outsourcing contracts for data management - anagement reports if any with regard to the review and monitoring of data management tasks The auditor should also obtain a list of applications and

	related operational manuals and user documents for • Application models undertaking input accuracy, completeness and validation checks • Data entry functions for all applications • Data entry error rectification procedures • Prevention and detection control mechanisms used for data entry errors • Control measures used to ensure integrity of processed data • Application models undertaking accuracy, completeness and validation checks that ensure the process data is close to the original data • Output handling and retention of the same • Distribution of output and interfacing outputs • Methods used to ensure integrity of data during the output process including balancing of output to control totals • Accuracy review of output reports • Generation of output distribution reports • Security of data during transmission between applications • Controls used in disposal of sensitive input, process and output results • Control measures over outsourced operations for the above tasks Policies and procedures of the entire organisation regarding central data base repository maintained by the organisation including • Organisation and data dictionary • Maintenance and security • Determination of ownership • Control procedures about changes in content and design • Maintenance of reporting and audit trails Policies and procedures of the entire organisation regarding library and off site storage maintained by the organisation including • Administration • External identification of all media • Inventory process • Housekeeping • Reconciliation • Recycling and rotation of data media • Recovery tests. • Role of personnel in media and off-site storage

Answer:[d] All of the above

Module:6

Reference No:M6046

Question: With regard to auditing the procedures of data management, which of the following statements is "TRUE" regarding principles of separation of duties

- [a] Separation needs to be maintained between origination and approval of source documents
- [b] Separation needs to be maintained between origination and conversion of source documents
- [c] Separation needs to be maintained between approval and conversion of source documents
- [d] Separation needs to be maintained between origination, approval and conversion of source documents

Module 6- Audit working guideline

Data Management -2

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Data management	Not applicable for this activity	1. Source document controls 2. Data input controls 3. Data processing controls 4. Data output controls 5. Security measures during transmission 6. Protection of disposed information 7. Storage management 8. Media library management 9. Backup and recovery 10. Authentication 11. Electronic value security 12. Integrity of stored information

Audit Process

The audit process has been covered in a six part series. In the first part the preliminary understanding has been covered. This is the second part and focuses on a part of preliminary analysis of the control measures identified. The preliminary analysis has been concluded in the third part.

Preliminary analysis part 1

The next step is analysing the effectiveness of the control measures adopted and the degree of reliability that can be placed on the control measures. This can be done through ensuring that data management plan/procedure adopted by the organisation consists of /provides for the following Control activities

Source of data

1. Authorisation procedures should exist for all source documents
2. Segregation of duties should be maintained between origination, approval and conversion
3. Integrity of authorised data should be maintained through source document origination
4. Timely transmission of data
5. Review of source documents for completion and approval
6. Identification and handling of erroneous documents
7. Separate control measures should exist for sensitive documents to prevent compromise
8. Procedures should exist to ensure integrity of source documents and timely and proper accounting
9. Retention of source documents for adequate period taking into consideration any legal requirements

Entry of data

10. Procedures to ensure that all data to be input are authorised
11. Segregation of duties should be maintained between submission, authorised and entry functions
12. Unique codes to identify individual work stations and data operators
13. Maintenance and control of Workstation codes and Operator Ids
14. Audit trails to indicate the source of input
15. Data edit and verifications checks to be incorporated
16. Erroneous report handling
17. Assignment of responsibility for data authorisation

Processing of data

18. Programmes must be developed to identify errors in input
19. Validation of transactions against a master list
20. Disallowance of error override
21. Error handling procedures including approval for rectification and resubmission, identification of ownership for each suspense file creation, generation of report for non-resolved errors
22. Logs should be maintained for execution of transactions
23. A separate group should be maintained for monitoring and reconciliation and balancing of records and control totals
24. All erroneous data fields should be edited
25. All tables utilised should be periodically reviewed
26. Written procedures should exist for data error handling and resubmission
27. Responsibility for errors should be mapped to original submitting function
28. If Artificial intelligence is used, it should be ensured that vital decisions are approved by human operators

Contd.

Answer:[d] Separation needs to be maintained between origination, approval and conversion of source documents

Module:6

Reference No:M6047

Question: The audit trails with regard to auditing the procedures of data management should ideally provide the following details,

- [a] Only transactions processed
- [b] Only the reconciliation details of disrupted data
- [c] Both transaction details and reconciliation of disrupted data
- [d] None of the above

Module 6- Audit working guideline

Data Management -3

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Data management	Not applicable for this activity	1. Source document controls 2. Data input controls 3. Data processing controls 4. Data output controls 5. Security measures during transmission 6. Protection of disposed information 7. Storage management 8. Media library management 9. Backup and recovery 10. Authentication 11. Electronic value security 12. Integrity of stored information

Audit Process

The audit process has been covered in six parts. The first two parts dealt with the preliminary understanding and a part of preliminary analysis. This part focuses on the rest of the preliminary analysis

Preliminary analysis part 1

The next step is analysing the effectiveness of the control measures adopted and the degree of reliability that can be placed on the control measures. This can be done through ensuring that data management plan/procedure adopted by the organisation consists of /provides for the following Control activities

Data output and interfaces

- 29. Only authorised personnel are allowed physical and logical access to output
- 30. A periodical review of the output requirements should be conducted

31. Outputs should be balanced to control totals
32. Audit trails should provide details of transactions processed and the reconciliation details of any disrupted data
33. A control group should monitor the accuracy of the output and error handling
34. Security issues defined for output processing/interfacing and distribution of output need to be followed
35. Security breaches should be reported to management and acted upon promptly
36. The output processing and the responsibility of the personnel should be clearly defined
37. Unrequited material should be disposed with adequate security
38. All data should be stored in an offsite location
39. Information marked for deletion should not be in a retrievable form

Media library management

An inventory of all media library contents should be documented

40. All differences between the actual and records should be resolved promptly
41. Procedures adopted should maintain the integrity of the stored media
42. Media library management procedures should adequately define the housekeeping procedures
43. The roles and responsibilities of the library management personnel must be clearly defined
44. A back-up and restoration strategy should be defined
45. The backup procedures should be followed diligently and verified to ensure that the backups are usable
46. Retention periods should be defined in compliance with any legal requirements.
47. Apart from storage of other conventional forms of information like paper, even significant telephonic conversations can be stored and retained

Information authentication

49. Procedures should exist to verify any requests received through phone or voicemail like callback facility etc.
50. Procedures for independent verification of requests received through fax should exist
51. Documents received electronically should be verified using digital signatures

Answer:[c] Both transaction details and reconciliation of disrupted data

Module:6

Reference No:M6048

Question: One of the control measures adopted for media library management with regard to auditing the procedures of Data managementis that

- [a] The contents of library should be inventoried
- [b] Adequate house keeping procedures are defined
- [c] Independence is maintained between Input, processing and output functions
- [d] All of the above

Module 6- Audit working guideline

Data Management -3

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Data management	Not applicable for this activity	1. Source document controls 2. Data input controls 3. Data processing controls 4. Data output controls 5. Security measures during transmission 6. Protection of disposed information 7. Storage management 8. Media library management 9. Backup and recovery 10. Authentication 11. Electronic value security 12. Integrity of stored information

Audit Process

The audit process has been detailed in six parts. The first three parts covered the preliminary understanding and the preliminary analysis. This part focuses on the test of controls.

Tests of controls

A clear picture of the functioning of controls can be gained by:

- Obtaining evidence
- Reviewing the deliverables

Tests: Before the auditor takes a stand on the functioning of IT tasks in the organisation, he should perform the following tests.

Source of data

For a selected sample of documents ensure that all control measures stated in the previous section exist and ensure the completeness, accuracy and authorisation of the source documents. Ensure evidence is available for timely transfer of data.

Also all source, conversion, and data entry staff should be aware of and understand the procedures of the organisation.

Entry of data

- A sample test data (both good and erroneous) has to be verified if the normal data edit and validation checks are being conducted by the application.
- Master files of selected transactions before and after input must be compared
- Appropriate procedures should be in place for error handling and review integrity.
- Evidence that actual error handling is in compliance with the procedures must be available.

Processing of data

- Evidence that run-to-run controls and master file update control procedures are being used should be available.
- A sample test data (both good and erroneous) that verifies if the normal data edit and validation checks are being conducted by the application has to be submitted.
- For a sample, Master files of selected transactions before and after input have to be compared
- Appropriate procedures should exist for error handling and review integrity.
- Evidence that actual error handling are in compliance with the procedures must be available.

Data output and interfaces

- Evidence exists that output is regularly balanced to control totals
- Audit trails are available
- Outputs are being reviewed for accuracy
- Appropriate procedures exist for error handling and review integrity.
- Evidence that actual error handling is in compliance with the procedures exists
- Outputs to be distributed/ under distribution are adequately secured
- Sensitive information under transmission are adequately secured
- Disposal of irrelevant information is done as per established policies and procedures

Media library management

- An inventory is taken of the media library, regularly reviewed and discrepancies adequately resolved.
- House keeping functions are performed appropriately
- Assignment of media responsibilities is clear and adequate
- Principles of segregation of duties are followed while assigning media library responsibilities
- Adequate media backup and restoration plans exist and are followed.
- Media storage sites are physically secured
- Retention periods are appropriate

Information authentication

Evidence that control measures are followed for transactions through phone, voice mail or fax or through Internet or public network is necessary. These controls are applied to support facilities that are used for transmission such as fax software etc.

Answer:[d] All of the above

Module:6

Reference No:M6049

Question: Suspense files concerning the procedures of data management, should have the following control details:

- [a] Identification of operator making the error
- [b] Error code
- [c] Date and time of error
- [d] All of the above

Module 6- Audit working guideline
Data Management -5

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Data management	Not applicable for this activity	1. Source document controls 2. Data input controls 3. Data processing controls 4. Data output controls 5. Security measures during transmission 6. Protection of disposed information 7. Storage management 8. Media library management 9. Backup and recovery 10. Authentication 11. Electronic value security 12. Integrity of stored information

Audit Process

The audit process has been covered in six parts. Preliminary understanding; preliminary analysis and test of controls were covered in the first four parts. This article focuses on the substantive testing.

Substantive testing

This step is undertaken to substantiate the auditor's viewpoint that control objectives are either not being met, or do not exist. The shortcomings in controls and its consequences also should be documented. He should also:

1. Identify comparative benchmarks from similar organisations, industries.
2. Utilise industries best practices or international standards to review the adequacy of the risk assessment approach.
3. Test a few sample transactions. The auditor needs to confirm the accuracy of transactions for each of the following stages:
 - Data sourcing
 - Entry of data
 - Processing of data
 - Output generation and distribution
 - Interfacing

- Data retention and disposal
 - Error and incident management for all the above stages
 - Integrity of data through all the above stages of processing
4. The following mandatory tests to be done
- Tests for completeness and accuracy
 - Adequate authorisations and approvals
 - Existence of control measures for both operational and mangemental- either within the process or through a control group.
 - Retention of the source documents for subsequent requirements. The retention period should match the organisational policies and procedures.
 - Recover a few documents to verify their availability and accuracy
 - Review the audit trails and verify if they identify the source document and operator for each transaction and the level of controls by the operating systems over each transaction.
5. Verify if the input programming has incorporated the following edit checks for selected input transactions. (The list given below is only an indicative list and not a comprehensive one.)
- Mandatory blank fields for certain transactions
 - Negative Amounts
 - Code validation
 - Other required checks and conditions
6. Conduct tests to verify if the data validation routines are adequate
7. Conduct tests to validate if the following control measures are incorporated for creation of suspense files.
- Identification of the operator committing the error
 - All error transactions must be moved to suspense files
 - Suspense files must be maintained till the resolution of the errors
 - Suspense files should indicate the date/time and machine from which the errors originated.
 - Management reports should be created for their trend analysis.

Answer:[d] All of the above

Module:6

Reference No:M6050

Question: Which of following activities with regard to auditing the procedures of data management, control the integrity of production files when accessed by operators?

- [a] Creation of a 'before' image
- [b] Creation of an 'after' image
- [c] Creation of a 'before' and 'after' image
- [d] None of the above

Module 6- Audit working guideline

Data Management -6

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Data management	Not applicable for this activity	1. Source document controls 2. Data input controls 3. Data processing controls 4. Data output controls 5. Security measures during transmission 6. Protection of disposed information 7. Storage management 8. Media library management 9. Backup and recovery 10. Authentication 11. Electronic value security 12. Integrity of stored information

Audit Process

The audit process has been covered in six parts. The first five parts highlighted the preliminary understanding, preliminary analysis, test of controls and part of substantive testing. This article focuses on the rest of the substantive testing.

Substantive testing_contd

This step is undertaken to substantiate the auditor's viewpoint that control objectives are either not being met, or do not exist. The shortcomings in controls and its consequences also should be documented. And also:

The following tests should be conducted for selected output transactions:

- Verify accuracy and completeness for selected output reports and listings
- Review output retention schedules for compliance with procedures
- Confirm if actual distribution of reports was done as per standard procedures.
- Compare the output of one process to the input of another to validate integrated processing
- Review if files and other medias are being relocated/destroyed as per retention policies
- Ensure that only authorised personnel have access to sensitive data
- Validate actual retention periods with the policies.
- Witness actual transmission or delivery of sensitive information for security compliance or other processing requirements.
- Validate if the backup process is as per policies of the organisation.

9. Tests for the media library should

- Validate the access controls to media library
- Test a sample of media to be destroyed and verify if the process is in compliance with procedures
- Verify if records maintained adequately assist in accessing the records of media.
- Verify if controls exist for preventing overriding labelling conventions
- Test if control measures are being complied with
- Review if back up creations are adequate for emergencies

- Review the reports of latest media inventory
- Confirm if the media inspections have been carried out as scheduled.

Identifying shortcomings

Auditors should identify instances wherein:

1. A before and after image was not created when production files were accessed by the operators
2. Sensitive documents like input and output forms are not protected.
3. Logs are not maintained for control totals for all processing
4. Inadequate, irrelevant output reports are generated. The reports generated are not distributed appropriately. Designing of the output forms is inadequate
5. Data transmission is not adequately protected which includes
 - Unlimited access
 - Improper authorisation and identification
 - Unsecured means of transmission
 - Non -utilisation of encryption for security data under transmission
 - Tests for completeness
6. Security and control clauses are missing in third party servicing agreements
7. Deficiencies exist in offsite storage management.

Answer:[c] Creation of a 'before' and 'after' image

Module:6

Reference No:M6051

Question: Digital cash actually refers to

- [a] A credit card number
- [b] An identity number issued for a person by a bank
- [c] A unique number issued by the bank that represents a real sum of money
- [d] Money spent in online transactions

Module 6- Digital Cash or E-Money

Introduction:

Digital cash or E-money refers to an arrangement that permits transaction of money for buying and selling of goods online. This is done by transferring a unique number from one workstation to the other. These numbers are analogous to the serial numbers printed on currency notes and represent a specific sum of money. A bank issues these numbers. Digital cash, like real money is anonymous and can be reused, i.e. the sender cannot be traced after a transaction (this way digital cash transaction differs from a credit card transaction).

In general, banks that issue digital money, issue digital certificates for account holders of the bank. On purchasing a digital cash certificate, money is withdrawn from the owner of the digital certificate. During a transaction, this certificate is transferred to the trader for buying a product or service. In case of large transactions, the vendor ensures authenticity of the cash number (in the digital cash certificate), by verifying it with the issuing bank.

Implementation of digital cash:

E-money or digital cash are viable and workable due to the presence of digital signatures and public-key encryptions that can ensure safe and foolproof transaction through digital cash. Both banks and the owner of the digital cash obtain public-key encryptions. Typically, public-key encryptions are in pairs - a private key known to the owner and a public key that can decrypt the information transferred by the owner. A public-key decrypts whatever a private key encrypts. The owners and the banks use encryption for securing the transaction and digital signatures for identification and authentication (in deposits and withdrawals). Public-key encryptions are used for signing money orders (by the banks), and the customers sign deposits and withdrawals using their private keys. The banks verify these transactions (deposits / withdrawals) using the customer's public key.

Types of digital money:

E-money is of two types:

1. Identified e-money
2. Anonymous e-money

Identified e-money gives information about the owner (i.e. who withdrew the money from the bank) while, anonymous digital money does not keep any track of the owner. *Anonymous* digital cash is issued using blind signatures instead of non-blind signatures. The two types of money are further classified as *online money* and *offline money*.

In order to transact using online e-money, one needs to get connected to the bank. Offline digital cash (the most complicated form of digital money) can be used in transactions without interacting with the bank directly.

The problem of double spending:

Double spending refers to duplication of digital cash. Digital cash is nothing but a number (stored in the memory in form of bits), issued by a bank representing a real sum of money. Thus, these numbers can be easily copied if the network is not secure.

Solution: The double spending problem can be solved in the following ways:

- If the transaction is online, the transaction is made secure by keeping track of the spent cash (by maintaining a database stored in the bank's computer) and crosschecking the validity (i.e. whether it can be spent or not) during every transaction. If the digital cash is marked 'spent' in the bank's database, the transaction is not carried out. This method is quite similar to the way credit card transactions are validated.
- There are two ways of avoiding double spending in case of an offline transaction
 - *By implementing Observer:* An observer is a tamper-proof chip that maintains mini databases for keeping track of the spent money. Any attempt to copy the digital money, is identified by the observer thus preventing any fraudulent transaction. Being a tamper-proof chip, the database in the observer cannot be meddled with unless the smart card is damaged permanently.
 - *By using cryptographic protocols:* Cryptographic protocols reveal the identity of the double spender by the time the e-money returns to the bank. This increases the chances of a double spender getting caught. The advantage of this method is that it does not require implementation of smart cards and the whole system can be implemented on ordinary machines.

Answer: [c] A unique number issued by the bank that represents a real sum of money

Explanation: Online transaction may or may not involve digital cash. So digital cash should not be confused with money involved in online transactions, since online transactions sometimes use real money (using credit cards etc.). Hence it is not same as digital cash.

Question: Which of the following is not a component of a digital wallet?

- [a] Digital cash
- [b] Communication manager
- [c] User profile manager
- [d] Wallet controller

Module 6- Digital Wallets

Specially designed software that stores transaction information, user identity to provide the user with a convenient means to pay in e-commerce transactions, is referred to as a digital wallet. Quite similar to a real wallet, a digital wallet holds user specific information (i.e. his transaction details, amount of digital cash he owns, amount of digital cash spent and digital certificates to authenticate him). Digital wallets simplify online transactions by automatically paying for the product or service bought by the user. Digital wallets also screen redundant (low-level) details involved in a payment (like payment protocol details and the like).

Typically, a digital wallet should conform to the following

- A digital wallet should be capable of handling customer's credit cards and digital cash. It should be competent enough to manage compound transactions (those which involve multiple payments) using both credit cards and digital money. A digital wallet should be capable of upgrading itself in integrating new add-ons like discount coupons without implementing extra devices.
- A digital wallet like the real wallet should be absolutely customer-driven, i.e. only the user should be allowed to activate a digital wallet, thereby avoiding a trader from activating the wallet every time the client visits his site. This will endow complete control of the user on his wallet (like that in a real wallet) and he can invoke it only when he wants to make a transaction.
- The components of a digital wallet should allow reusability. Banks and traders handle e-commerce transactions in the same way, as does a user. Hence, to simplify general transactions like validating user identity and the balance in his account the common information (like user account number and identity) should be sharable and reusable. This will allow banks and traders to make use of new financial devices with greater ease.
- A digital wallet should have universal compatibility so as to function in every software environment regardless of the platform of transaction. In order to implement this sort of generality the wallet should have a general protocol or a substitute interface (that is capable of handling a mismatch in the environments).

Structural design of a digital wallet:

The chief components of a digital wallet are:

- *Instrument manager*: An instrument manager makes all sorts of financial devices functional and is responsible for interactions between the customer and the banks/vendors. It manages all kinds of transactions involving credit cards, digital certificates and digital cash.
- *Protocol manager*: A protocol manager activates all the protocols a wallet uses in a transaction. It gets data for processing low-level communications from the communication manager.

- Wallet controller: A wallet controller is responsible for concealing trivial details (at low-level communications) and assists the user in interacting at the higher level.
- User profile manager: As the name suggests, a user profile manager maintains user specific information like his credit card numbers, access to different modes of transactions (either through credit cards or digital cash), user passwords and the names or identities of people who have transacted with him.
- Communication manager: All the low-level transmissions like establishing a connection, maintaining communication sessions (during a transaction), encryption and decryption of data are managed by the communication manager.
- Interfaces: There are different kinds of interfaces like GUI, API and the like that simplifies user interactions and customisations.

Answer: [a] Digital cash

Module:6

Reference No:M6053

Question: Which of the following is not a feature of Automated crime software?

- [a] Automated crime software is a readymade tested crime
- [b] Automated crime software executes the crime perfectly
- [c] Automated crime software expunges the evidence
- [d] Automated crime software helps to identify the crime

Module 6- Automated Crime

Protection of Information from Automated Crimes

Introduction

Illegal users of information systems have become so intelligent that they can commit a crime at the bat of an eye without leaving any evidence of crime. Using computers and automated processes they follow a perfect crime methodology. They adopt other crimes and modify them according to their needs. Hence, it is essential to identify the future tactics of criminals.

Malware

In a Malware type of software, for instance, well-conceived crimes are packaged and supplied or sold to criminals. The term Malware refers to the malicious programmes like viruses, worms, Trojan horses etc. The programme attacks and destroys the physical assets of the company. It may contain hacker tools, malicious Java codes, viruses and worms that affect the software. The software also provides crime designers written instructions to execute the crimes.

Automated crime

Automated crimes are an improved version of malware. Readymade crimes, which have been tested, are available to the criminals. This helps them execute the crime perfectly and expunges the evidence so that victims are not aware of the crime. The software automatically identifies the victims and completes the work. A single computer programme provides all these features. Once the programme is executed the crime is carried out automatically. Automated crimes software maintains perfect anonymity, so victims as well as perpetrators are not aware of the type of crime and its results.

Malicious hackers use several types of valuable security tools for illicit.

Automated crime process

- *Selecting the systems to attack:* A freeware programme such as SATAN helps identify the target system for attack. It scans the systems without disturbing them.
- *Identifying the weaknesses to attack:* SATAN can identify the weaknesses in network computers.
- *Exploiting the weaknesses to attack:* The identified weaknesses are exploited to gain access through the techniques like IP spoofing.
- *Executing the criminal act:* This can be done in several ways. For example, a Trojan horse can be used to place the secret commands of the criminal in the application programme of a victim.
- *Deriving benefit from the activity:* In this step, the perpetrator is provided a criminal gain. It could merely be a satisfaction to the criminal that he has successfully disrupted the victim's system or financial gain. For example, if the perpetrator is involved in a banking system fraud, the gain may be the transfer of funds from one banking system to another.
- *Expunging the evidence:* Perpetrators must eliminate all evidence to prevent detection of a crime and prosecution.

Automated security

High-level information security is required to detect and prevent automated crimes. Security software like anti-virus programmes and intrusion detection systems should be built- to identify and prevent the attacks. It should happen in computer time without involving anyone. Care must be taken to ensure that the programmes do not damage the systems in any way. Moreover they should provide all the evidence required for a civil litigation.

Answer: [a] Automated Crime Software indicates the victims about the crime

Module:6

Reference No:M6054

Question: Internet banking facilitates customer access to his account

- [a] Only at the bank
- [b] Anywhere, anytime in the world through World Wide Web
- [c] Within the country
- [d] At an Internet cafe

Module 6- Internet Banking

Retail Financial Services are becoming more efficient with the introduction of the Internet. Provision of banking products and services via the Internet is known as Internet Banking. Such provisions include a wide range of offerings from basics functions like providing access to the data of the deposit account - to sophisticated products like integrated sales.

An effective Intranet banking solution should provide the following benefits:

1. Outstanding Saving, IRA and CD rates
2. No charges for checking, bill payment and ATMs etc.
3. Low rates on credit cards

4. Applications for accounts, personal loans, mortgages available on online.
5. 24 hour access to the account
6. Improved quality of customer service

Internet Banking provides many benefits both to the customer and financial institutions in terms of cost-effectiveness. It has removed access barriers in the global market. The World Wide Web allows customers to access their accounts anywhere, anytime in the world. Internet banking enhances customer loyalty thereby reducing customer switchover and draws new customer attention. It also has provision for a variety of services with improved quality.

Internet Banking in India

Though Internet banking is still in its nascent stages it poses severe competition to the banking industry. The banking industry deregulation has eased the entry of global competitors into the market. Even non-traditional banking institutions are providing banking and financial services on the Internet. Most banks provide only basic services over the Internet. Nevertheless, the number of banks adopting Internet banking is increasing.

Future challenges

It is predicted that Internet banking will face the following challenges:

- Demand for low cost services
- Demand for more transparency due to increased customer awareness
- Increasing number of global players
- Possibility of integration and disintermediation of banking services
- International transactions becoming easy with the deregulation movement
- Increased importance for 'Banking Portfolio'

Banks have to keep pace with the emerging challenges in the light of the continuous changes in the Internet technology. Those fail to do so will not be able to stay in the business.

Security and Internet banking

Security of Internet banking is an important concern owing to its World Wide access. Consumer privacy protection and fraud control are two essential elements of security of Internet banking. Firewalls, filtering routers, digital certification and encryption are components of security architecture that prevent unauthorised access to customers' accounts. Firewalls and filtering routers for example prevent unauthorised access and encryption ensures the privacy of data flow.

In the increasing trend towards on-line and real-time, banks have to risk integration to survive in the market.

Answer: [b] Anywhere, anytime in the world through World Wide Web

Module:6

Reference No:M6055

Question: Which of the following is not a feature of a Mobile recovery centre?

- [a] It is portable
- [b] It is a simulation of the main centre of an organisation

- [c] It meets the user requirements like workspace, computers, LAN connectivity etc
- [d] It can accommodate an unlimited workforce

Module 6- Mobile Recovery

Introduction

The control centres are the most indispensable requirement of any business organisation. . Managing day-to-day operations of the control centre is a daunting task, because even a slightest disruption can put the entire organisation in soup. Hence to avoid any fallout the control centre of a business organisation must be backed by a foolproof disaster recovery plan. Disaster recovery refers to a plan to handle probable failures in an organisation. It details how to pick up the business, and cautions against potential disasters. Different disaster recovery sites are employed for recuperating. Of these, going in for alternate sites like hot sites, cold sites and mobile sites are a viable option.

Definition: Mobile recovery refers to restoring the business, by alternate business sites that are transportable (or mobile). Mobile sites are implemented for acting as replacements during the crisis (or system failure like database crash, collapse of data centre and the like).

A *Mobile Recovery Centre* (MRC) is a customised container (portable / transportable; in fact a huge vehicle) that accommodates a fixed number (or limited) of workforces and provides all pre-configured client requirements and workspace so as to enable the employees of an organisation to continue functioning (without the need to travel to the disaster recovery site) during a system failure.

Generally, just the control centre or the heart of a business centre is reinstated with a mobile centre. These recovery sites are made mobile so as to accelerate the recovery process.

Implementation of a Mobile Recovery Centre (MRC)

A mobile recovery centre (MRC) is planned to accommodate duplicates of chief components of the organisation like the data centre / the computer room, call centre, working environments (with workstations) and the like.

Ideally a MRC should conform to the following:

- It should offer protection against unexpected power losses or interruption in accessing the computer room
 - It should offer an appropriate replacement for the data centre with the essential systems like workstations, LAN connections, link to the clients and the like.
- It should have a dedicated generator and air conditioning systems for enabling smooth functioning of the work environment.
- It should be equipped with on-site technical resources for setting up and restoring the systems.
- Since, mobile centres are meant to be portable, they are compact whereby only a limited workforce can work in an MRC. Each of these mobile centres should have the facility of getting connected to other such mobile centres implemented for the organisation.
- It should have a well documented invocation procedures and local account management support.
- It should meet all safety requirements like multiple entry/exit points, fire-extinguishing systems and the like.

Advantages of using a Mobile centre

- Mobile recovery centres accelerate disaster recovery process by making the disaster recovery (DR) workforce operate from sites that are closer to home. Providing the DR

workforce with computing resources and transitory workspace (i.e. a mobile recovery centre) makes the job easier and effective.

- Implementing mobile recovery centre is a more realistic and cost effective approach, as the DR workforce need not travel long distances to the disaster recovery site to operate.
- Further by implementing mobile centres, the organisation can simulate the recovery process before the disaster strikes, thereby, ensuring that the recovery plan of the organisation is tested.

Answer: [d] It can accommodate an unlimited workforce

Module:6

Reference No:M6056

Question: In an Automated Teller Machines, the card reader takes input from

- [a] What the customer types on the keypad
- [b] The sensor
- [c] The magnetic strip of the card
- [d] The cash dispensing mechanism

Module 6- Automated Teller Machines

What is an ATM (Automated Teller Machine)?

ATMs or automated teller machines are compact machines that provide an interactive online transaction facility to cardholders (ATM cardholders) in the absence of any cashier. These machines have a monitor that prompts the user for input so as to allow him to withdraw money, along with the money receipt. These machines are found at super markets, corporate houses, travel centres and the like.

In fact, an *automated teller machine* is a data terminal that has two input points and four output points. It is connected to a host network (which is a gateway through which the card holder can access other ATM networks).

Parts of ATM

The two input devices of an ATM are:

- **Card Reader:** Card reader, as the name suggests takes the card number stored in the magnetic strip of the user's card and sends it to the host processor for using the data in routing the customer's transaction.
- **Keypad:** Keypad is analogous to a keyboard (of a computer or calculator) that allows the cardholder to type in the amount to be withdrawn. The cardholder has to type in the PIN (*Personal Identification number*). PIN number is a unique number given to the cardholder for identification and authentication of his account in the bank. The bank crosschecks the amount to be withdrawn with the balance available in the customer's account. In fact the PIN number of the customer is sent across the network in encrypted form.

The four output devices of the ATM are:

- **Speaker:** Speaker gives an auditory feedback acknowledging whenever a key is pressed.
- **Display Screen:** The screen prompts the user to type in the input (be it the PIN number, type of withdrawal, or amount of cash to be drawn) throughout the transaction process.
- **Printer:** The receipt printer produces the receipt for each transaction of the cardholder.

- **Cash dispenser:** The cash dispenser is the most vital part of an ATM. A cash dispenser comprises a safe (that holds the cash) and a cash dispensing mechanism. The cash dispensing mechanism has an electric eye that counts each currency note (as it exits the machine). It also maintains a recorded log that keeps an account of every transaction. This log is printed out as the transaction receipt for the cardholder at the end of every transaction. The cash dispenser mechanism is provided with a sensor that measures the thickness of each bill so as to ensure that only one currency note is dispensed at one time. In case two currency notes are stuck or a bill is badly damaged, it is detained in a reject bin to be retrieved later by the bank authorities.

Security issues in ATM

- The most vulnerable security concern for ATM users is their PIN numbers. For security reason, the PIN number is not printed in the transaction receipt. Further, some machines ensure additional security by printing out only the last four digits of the account number. This conceals the cardholders' account number in case he leaves the transaction receipt in the machine itself.
- To prevent the card from being swallowed by the ATM machine, ATMs are designed with dip or swipe card readers so that the card doesn't leave the cardholders' hand while transacting.

Answer: [c] The magnetic strip of the card

Explanation: The user's card number is stored in the magnetic trip of his card. This is read by the card reader and passed on to the host processor for routing the customer transaction.

Module:6

Reference No:M6057

Question: Which of following aspects must be identified to maximise server utilisation?

- [a] Improper server utilisation
- [b] Cost of server
- [c] E-mail traffic volumes
- [d] Disk usage

Module 6- E-mail Infrastructure Management

Introduction

Information can be communicated within seconds to a distant place through e-mail. The standards of business communication have drastically improved leading to greater user expectations. However, any unexpected network blockages or problems can set back the service. It is therefore essential to troubleshoot problems quickly. Further, organisations must concentrate on improving productivity of their staff and maximise efficiency of the existing technology rather than investing heavily in e-mail infrastructure like servers, bandwidth, storage etc.

E-mail traffic volumes, performance obstacles and utilisation models need to be understood thoroughly in order to provide cost-effective e-mail services and manage e-mail support matters. The following methodology helps minimise the total cost of e-mail systems and effectively manages support issues thereby enhancing service levels:

1. Resource usage management

The pressure on key resources like bandwidth, server and storage facilities has to be identified and balanced regularly as the traffic patterns and basic assumptions may change over a period of time.

- *Server:* Imbalances in server utilisation can be recognised by measuring the routing activities. Hence maximum utilisation of servers can be achieved by adjusting the routing plans accordingly.
- *Bandwidth:* Usage patterns have to be identified and planned accordingly. The next step is to understand the changes in those patterns so as to maximise bandwidth utilisation by reconfiguring the network.
- *Storage:* E-mail storage is an essential concern in the light of increasing cost in managing huge e-mail volumes. Identifying periodic disk usage and analysing it server-wise can help reduce server fluctuations. This is possible by periodically shuffling user ids among different servers.

2. Problem recognition

The second step is to identify the areas, which use huge e-mail resources. Some of the areas are -

- Sometimes small messages cause overloading problems in bandwidth, server capacity and storage facilities. Hence identifying them and educating users about alternative methods will cut down the overload problems.
- When a message has to be sent to a large group, it occupies greater storage space. Instead, it can be sent through the intranet or can be placed in a shared database, which minimises usage of e-mail resources.
- Enormous amount of resources are consumed when corporate messages are broadcasted to employees. Alternative methods must be identified to enhance network performance.
- One particular user may block huge storage space if he sends heavy attachments such as digital photos, etc to several people. In such instances, properly monitoring the execution of the policy will solve the problem.
- The cost and performance of e-mail systems are seriously affected when organisational networks are used for personal purposes. Hence such usage must be identified and controlled.

3. Policy development

The next step is policy development. Policies must be precise and helpful in solving problematic issues. They must be explicitly communicated throughout the organisation. It should include corrective actions and rewards for habitual offenders and efficient users respectively.

4. Policy enforcement

Policies developed must be effectively monitored in order to achieve the desired results. There is a possibility of ignoring policies if they are not enforced and monitored regularly.

E-mail traffic Metrics

The next requirement in managing e-mail networks is the availability of e-mail traffic management solutions at the enterprise level. These are common and efficient reporting tools. They help to improve staff productivity, minimise the cost of infrastructure and enhance capacity planning. These tools also help in building and executing e-mail policies and service levels. Further, strategic projects like system migrations, mergers and server consolidations can be implemented more

effectively.

The above-mentioned methodology along with e-mail traffic metrics enables organisations to improve e-mail support response times and provide cost effective e-mail services. .

Answer: [a] Improper server utilisation

Module:6

Reference No:M6058

Question: An Automated Security system is capable of:

- [a] Selection of systems to attack
- [b] Expunging the evidence of automated crime
- [c] Protecting evidence of automated crime
- [d] Exploiting the weaknesses in systems to attack

Module 6- Protection of Information from Automated Crime - Part I

The previous article titled "Protection of Information from Automated Crime", explained automated crime and its process. . It is a readymade fully tested crime available to the criminals. It executes the crime perfectly and expunges the evidence so that victims are not aware of the crimes. The present article focuses on the security strategy to be adopted for protecting information against automated crimes.

As it is possible to automate the crime process like any other business process (accounts payable or payrolls), an automated security is also essential to protect against automated crimes. This requires an understanding of the structure of automated crime.

Structure of an Automated crime

There are six steps in the automated crime process

1. Selecting the systems to attack
2. Identifying the weaknesses in order to attack
3. Exploiting the weaknesses to attack
4. Executing the criminal act
5. Deriving benefit from the activity
6. Expunging the evidence

First a network probe like SATAN can be used to identify the weaknesses in the targeted computer system. Before performing a criminal activity the weakness can be exploited by gaining authority of IP spoofing. to then. In the fifth step the criminal activity is converted into some benefit. The evidence is eliminated in the last stage.

Automated Security

Similar to the automated crime process, the automated security process also has six steps. These steps are framed such that they counteract the steps in the automated crime process. It is a general framework that can be modified according to the future requirements.

Steps in the Automated Security Process

1. *Critical system security:* Firewalls and security buffers can ensure critical system security. Filtering software placed in the hubs, network servers, and routers constrain the automated crime communications.
2. *Detection and prevention tools:* Automated security systems though a vulnerability assessment tool identifies the perpetrators programmes and stops misuse of the weaknesses. The weaknesses are eliminated frequently by regular software updates.
3. *Prevent exploitation of weaknesses:* Automated security should prevent exploiting the identified weaknesses. The most advantageous method is preventing opportunity before the attack.
4. *Prevent corrupting attempts:* corrupting attempts must be prevented. If not at least the loss must be minimised by mitigating the act. Specific defensive controls such as cheque summing, independent balancing and transaction checking help to prevent corrupting attempts.
5. *Prevent unintended transactions:* Criminal loss to the victim may occur in the form of false inventory changes, payments to bogus employees, processing private information, or unauthorised services to customers. The conversion points like cheque printing, ATM cash dispensing places or the network gateway must be checked for the authenticity and integrity of the transactions.
6. *Protecting evidence:* An automated security system safeguards the audit logs and transaction register copies thus preventing removal of evidence of the crime. It also provides the replicates of buffer contents and maintains independent records.

Preventing the perfect crime

An accurate information security framework that foresees the automated crimes is essential as an automated crime is very perfect in nature and can carryout crime without the victim's knowledge. . Therefore, to prevent a perfect crime the availability, integrity, confidentiality utility and authenticity, the information possessed must be protected in the information security.

The growth of sophisticated automated crimes is inevitable. Hence an automated security that can prevent the criminal action instantly is desirable. The perpetrators and victims will come to know about the crime only after its completion. The perpetrator will win if the automated crime is effective and victim if the automated security is effective.

Answer: [c] Protecting evidence of automated crime

Module:6

Reference No:M6059

Question: Which of the following ensures maximum security of information and data to the organisation?

- [a] One size fits all security toolbox
- [b] Information security programme that brings together the hardware and software to achieve the desired policies
- [c] Technology added in bits and pieces
- [d] Implementation of technology at different business units individually

Module 6- E-commerce Security Architecture

Introduction

100% security of transactions, data, infrastructure and operating environment through a single

security toolbox is a daunting task. Instead, an organisation can ensure maximum security through an information security programme that brings together the different types of hardware and software to achieve the desired policies. An effective security programme needs to accumulate the cooperation and support of the entire organisational personnel. The description of such a process is referred as Security Architecture.

E-commerce security architecture

The investment in e-commerce applications and implementation of infrastructure solutions is on a downslide. And the models of those companies that have a full-scale implementation of e-commerce technology may not suit the requirements of other companies. Therefore, development of security architecture for the entire organisation is important. It is an essential means to integrate all the tools in order to achieve present requirements and determine the future needs.

Design of the architecture

Determination of the security goal is an important step in the design of the security architecture. The goal of the security should represent the strategic vision of the organisation. The following are some of the security goals:

- Securing the confidentiality of the data
- Ensuring the prevention of unauthorised access
- Ensuring the availability of the data.
- Checking the authenticity of a person dealing with business transactions.

A detailed architecture design consists of particulars relating to selection of a product, its development and implementation. It facilitates an organisation in the development of infrastructural activities like servers, middleware and networks etc.

Reasons for architecture design

The following are the reasons that demand designing the enterprise level e-commerce security architecture: -

Size of the network: In the absence of security architecture planning process, technology is added in bits and pieces according to the upcoming needs. Finally the size of the network increases unintentionally due to the accretion of technology in parts. Hence a standard planning process helps to add technology by considering the future needs also.

Communication: Various business units of a particular company might be planning to undertake an e-commerce application, but the proposal of one unit may not be known to others. In that case multiple solutions are implemented simultaneously. This will increase the complexity of the system, which is not desirable. Security architecture presents a standardised solution, which aggregates all the necessary functionalities, with the involvement of entire organisational personnel.

Further an options menu, which includes options for different types of consolidated requirements, can be provided. It minimises the consumption of time and money.

Business process: Integration of functionalities is ensured through business process. Hence architectural design based on those policies ensures the incorporation of security controls in the initial stages of project development. Such business processes can be developed on the basis of software development process, life-cycle process etc.

Others: Infrastructure (like firewalls, network access controls) is not the sole criterion of the

security policy. Development of non-technical controls and integration of security practices with business cycles is also important.

Answer: [b] Information security programme that brings together the hardware and software to achieve the desired policies

Module:6

Reference No:M6060

Question: What does the institutional services manager of the disaster recovery team do?

- [a] Evaluates the damage and formulates the steps to be taken for the recovery
- [b] Notifies the recovery team about the damage
- [c] Chooses the members of the recovery team and organises them
- [d] None of the above

Module 6- Roles and responsibilities of people involved in DRP (Disaster Recovery Planning)-I

An overview on disaster recover planning

A strategic preparation to facilitate the normal functioning of the organisation even during potential disasters is referred to as a disaster recovery plan (DRP) or business process contingency plan (BPCP). It also involves precautions to be taken in anticipation of potential disasters, like database crashes, system breakdowns and the like. Disaster recovery plan differs from company to company and it can either be devised by the company itself or bought as a service from a disaster recovery provider.

This article will elaborate on the roles and responsibilities of people involved in disaster recovery planning. Disaster recovery chiefly involves two activities, viz., *damage assessment and damage recovery*.

Roles and responsibilities

In order to see the disaster recovery plan through completion successfully, it is essential to device definite roles and delegate specific responsibilities to them. These responsibilities are delegated on the basis of whether the role is to evaluate the loss (damage assessment) or to execute the recovery process (damage recovery). Each of these roles and their respective responsibilities are discussed as follows:

People involved in damage assessment

- ***Manager of institutional services:*** The institutional services manager as the name suggests is in charge of the physical assets of the organisation like the building, internal wiring and the like. He is responsible for ensuring the safety of the building. Apart from ensuring safety of the physical assets, he is also in charge of taking care of the safety of the workforce. Thus, the chief functions of an institutional services manager include personnel safety, checking for any damage that has affected the building, evaluating the damage if any and reporting it to the higher authority. In gist, he formulates the steps to be taken for recovery and thereby evaluates the recourses needed in the recovery plan.
- ***Assessment Director:*** Assessment Director is in charge of reporting or notifying the recovery team of the damage. He is also in charge of evaluating the damage occurred and instructing his subordinates who are involved in the disaster recovery plan. He even finds out in-house assistance and recommends it if found satisfactory. All the major decisions like allocating funds, extra workforce, dealing with the governance of the organisation and the like are taken by the director.

- **Assessment Team Leader:** Being the assessment team leader, he is the authority for choosing his disaster recovery team and delegates specific functions to each one of them. He is responsible of instructing his teams how to go about the disaster recovery implementation. This includes inspection, verification, reporting, and documentation.
- **Assessment team:** The assessment team comprises a group of people (led by the assessment team leader) who are responsible for investigating the damage, assessing the loss incurred (i.e. type and severity of damage), and ascertaining the early or initial steps for recovery. In a sense, the assessment team decides on priorities related to disaster recovery plan.
The next article focuses on the roles and responsibilities of people involved in the recovery process, i.e. in the second phase of disaster recovery plan.

Answer: [a] Evaluates the damage and formulates the steps to be taken for the recovery

Module:6

Reference No:M6061

Question: What role does a conservator play in the disaster recovery process?

- [a] He formulates the complete recovery plan to be followed by the recovery team
- [b] He maintains a record of available resources and the ones in use to assist the recovery director
- [c] He leads the recovery team and instructs the recovery team on how to go about the recovery plan
- [d] He is responsible for coordinating the requests made by the recovery team

Module 6- Roles and responsibilities of people involved in DRP (Disaster Recovery Planning)-II

Disaster recovery plan also referred to as business process contingency plan is a strategic preparation to enable normal functioning of the organisation even in times of potential disasters. The whole process of disaster recovery is classified into *disaster assessment* and *disaster recovery*. The roles and responsibilities are also accordingly delegated. The previous article discusses on the roles and responsibilities of the damage assessment team. The damage assessment team comprises:

- Manager of institutional services
- Assessment director
- Assessment team leader
- Assessment team

Damage assessment is succeeded by damage recovery process. This article discusses the responsibilities of people involved in the damage recovery process.

People involved in damage recovery

- **Recovery director:** The actual recovery process starts at this level. Prior to this only the assessment and evaluation of the damage is executed. The recovery director governs the full recovery process that includes delegating responsibilities to his team members, generating reports on the improvements made, enlisting the problems encountered in the recovery plan and maintaining a record of the actions taken. Based on the problems faced by the recovery team, the recovery director also predicts future risks. Some companies have a single person functioning both as an assessment director and recovery director.
- **Recovery secretary:** Recovery secretary assists the recovery director in the sense that he is in charge of coordinating the requests for resource allotment made by the recovery team.

In other words, the recovery secretary maintains any information that may be asked for by the recovery team and keeps track of the available resources and in-house assistance. For this the recovery secretary needs at least a telephone connection so that he can keep the recovery team apprised about what requests have been made by the recovery team, thereby assisting the recovery director in forming the initial picture of the recovery process and enlisting his priorities. This helps the recovery director in making his decisions regarding resource allotment, instructing the recovery team and the like.

- **Conservator:** The conservator as the name suggests is basically involved in conserving the company's resources during disaster recovery. He works hand in hand with the recovery director and advises him on available resources. He keeps track of the equipment used and supplies and raw materials required for recovery. This helps the recovery director in choosing priorities according to the available resources and allocating supplies or resources in disaster recovery procedures.
- **Recovery Team leader:** As the name suggests, the recovery team leader leads the recovery team. He is responsible for instructing and guiding the people involved in the recovery process all through the execution of the disaster recovery plan. The recovery team leader reports to the recovery director and updates the director on the progress made by the recovery team.
- **Recovery Team:** The recovery team comprises of a group of people who are actually responsible for executing the recovery plan as instructed by the higher authority. This may consist of workers, skilled staff security workforce etc. They are in charge of relocating the materials from the site of disaster to safer locations. This involves proper packaging of the materials to be transferred, making place for storing them properly, organising lost scraps of records and re-labelling them. Last but not the least, the recovery team also maintains record for keeping track of the materials moved from the disaster site, the lost records/inventories and photographs of the site.

Answer: [b] He maintains records on available resources and the ones in use so as to assist the recovery director

Module:6

Reference No:M6063

Question: Which of the following functions is the first step in designing the e-commerce security architecture?

- [a] Identifying risks and constraints
- [b] Determining the scope of the project
- [c] Identifying the connection among applications
- [d] Determining the maintenance plan

Module 6- E-commerce Security Architecture - Part II

Part I of the E-commerce article discussed the importance of E-commerce security architecture and the reasons for designing it. Security architecture for the entire organisation is an essential means to integrate all the security tools in order to fulfill the current set of requirements and determine future needs. The present article dwells on the appropriate methodology of designing the architecture, which has been illustrated through an example, describing the process in detail.

The process

Identifying risks and constraints in a business is the primary step in an e-commerce project. These

risks are then compared against business gains. But risk identification is not always an easy task. It requires perfect coordination between unit managers knowledgeable of how the business functions and technical personnel with the relevant skills and know-how.

The scope of the project, applications involved and an analysis of the relationship between the two are necessary to assess the risk. After identification of risks, a risk mitigation plan has to be developed. It also helps to undertake a cost/benefit analysis. After which development, integration and implementation can be undertaken. Here, the main criterion is to develop secure applications. To ensure this, proper training on cryptography tools and web-based authentication methods must be provided to application developers.

Security and functionality testing prior to production, and a maintenance plan required in the post-production stage need to be developed. However, a standard format for designing an e-commerce security infrastructure does not exist. Hence an organisation needs to develop its own solutions. The security architect has to integrate the existing infrastructure with applications.

For instance, if a company is involved in the design of security architecture, the following security requirements must be adhered to:

1. Protection of critical assets like customer information, and other confidential information related to company and infrastructural assets
2. Identification of critical threats like cyber threats
3. Identification of critical activities data access, data storage and recovery
4. Comparative ranking of confidentiality, integrity, availability, auditability and non-repudiation aspects of security goals.

The process includes technical and non-technical aspects. The former comprises of software and hardware elements and the later, of processes and procedures. The company's security architecture addresses the following technical aspects:

The software infrastructure is protected against attacks by implementing best practices.

- The design of the application strictly prohibits access and data capturing.
- User ID and password for users and strong authentication for system administrators, and firewall at the network level provides access control.
- Encryption of data ensures the safe transfer of data via web.
- Networks, database, operating systems and application layers are monitored regularly.
- Back-up and recovery of data is ensured through encryption and offsite storage
- Loads on application and Web server are balanced to improve performance

The following non-technical aspects need to be addressed along with above-mentioned technical aspects:

- Security architecture is designed for all the stages of project development.
- Risk assessment is conducted on an annual basis.
- Security vulnerabilities are evaluated and managed regularly on a day-to-day basis.
- Adequate training is provided to users and clients.
- The required level of staff involvement is encouraged.
- Physical security is ensured through a secure hosting facility.
- A flow chart and a decision tree are created for detecting and monitoring the intrusion on real time.
- Internal audits are conducted frequently.

- Procedures are established for change management process including testing, approving and documenting the changes.
- Availability of the system is examined regularly.
- A disaster recovery plan for physical devices as well as infrastructural facilities exists.

A full-time job: Designing a security architecture that is effective in addressing security related risks is a demanding job and requires organisational cooperation.

Answer: [a] Identifying risks and constraints

Module:6

Reference No:M6064

Question: Which of the following is an important criterion in finding appropriate email deployment systems?

- [a] Type of the information to be transmitted
- [b] Provider support to the user
- [c] Message options
- [d] All the above

Module 6- Email Deployment Systems

Several considerations (including specific user requirements) go into the deployment of appropriate e-mail systems. The foremost consideration being, the type of information to be transmitted. This is because the level of sophistication required in systems depends on the level of information needs.

The following are some of the points that need to be considered in selecting e-mail deployment systems:

1. **Simple to use:** The system must be simple to use and self-explanatory. It should be easily understandable to the users and enable to work better.
2. **Service:** The type of the services, response time for problems, availability of facilities like access to email, phone and service charges must be considered.
3. **System:** Guarantee for the system, the number and volume of the mail servers and back up system must be identified. The expected time taken for delivering the mail is to be calculated.
4. **White hats and ISPs:** The consequences of Spam complaints and support provided by the tool must be recognised.
5. **Services list:**
 - Check if the provider offers the service of hosting the list
 - Determine the options provided for data merge - the number of fields that can be adapted in a message
 - Examine the options for downloading the data in other reporting tools
 - Evaluate the options for new list uploading
 - Determine the facility to store additional data fields
6. **Click-through data:** Check whether data is stored at the aggregate level or at user level. Determine the facility to track links with important names.
7. **Reporting:** Check the efficiency of reporting facilities available.

8. **Bounces:** The number of bounces and the ability to recover the addresses from bounces is to be checked.
9. **Forms and surveys:** Know the support by the provider in sign-up forms in case if they host the data.
10. **Viral marketing:** The benefits available for referring the product to others and ease in such process needs to be verified.
11. **Address options:** Check the facility to use personal e-mail addresses apart from those provided by the supplier.
12. **Reply management:** Find the options available to locate the mail addresses with the user to send or forward the mail.
13. **Send format options:** Check the formatting options available and evaluate whether the system allows sending HTML to large recipients with the help of multi-part messages. Further check how the AOL addresses are interpreted by the system.
14. **Message options:** The facility to set messaging according to actions, time periods, or some other specific interests.

Price of the system may be an important consideration. But the above factors take precedence over the prices. Price can be negotiated based on these comparable tools.

Answer: [d] All the above

Module:6

Reference No:M6065

Question: Which of the following is not an advantage of Electronic cheque truncation?

- [a] Saves time spent in collection
- [b] Requires less investment
- [c] Provides floating benefit to the customers
- [d] Eliminates wastage and cuts cumbersome processes

Module 6- Cheque Electronification

Banks have had their interests diverted to electronic cheque truncation that has been developed using new technology.

Electronic cheques

Electronic cheque presentment saves time spent in collection, and in paying banks for the posting process. Truncation technology is used in bank back-end offices for electronic cheque presentment instead of using it at a retail point of sale. Further, major investment is not required in building a truncation infrastructure if the back-end processing has already been set-up. MICR readers can be acquired at a small amount.

But customers show less interest in cheque electronification. They enjoy a floating benefit in payment through paper cheques as banks take three to four days to collect payments. They use returned cheques as proof of purchase. However, the scenario is changing. Customers have started appreciating the benefits of electronification.

Electronic cheque truncation

In a cheque truncation process, a cheque is handed over to the cashier at bank. He then marks it as void and passes it through the Magnetic Ink Character Recognition (MICR) reader. . It is then converted into an electronic equivalent after the information contained in the MICR is scanned.

After receiving the cheque again, the customer signs on the receipt, authorising the electronification.

Automated Clearinghouses, Automated Teller Machines or Credit Card Networks are used to process the transaction. This doesn't require investment in image-scanning machines, and the customer doesn't have to surrender the cheque. Customer account is debited on the basis of real-time or delayed process. Therefore, customers can know the status of the account immediately depending on the method of transaction processing.

The following are the benefits of electronic cheque truncation to the bankers and customers:

- Elimination of wastage: Significant volumes of cheques that are folded, spindled or mutilated are being returned without processing. Electronification eliminates such wastage.
- Easy access: Through electronification, customers can access their demand deposit account to know the balance at any time. The complex process of checking the history of a customer and his personal records is not required.
- Simple process: Electronic processing reduces labour requirements and cuts out the cumbersome process of handling paper cheques.

Options

ACH (Automated clearing house) is the major processor for cheque truncation. Customers' familiarity with the system helps them handle all cheques drawn on all banks. The ACH system doesn't process in real time; and accounts are settled at night.

Visa systems: ACH or Visa systems are involved in the process of verifying cheques drawn on other banks. It processes electronic cheque transactions in a similar manner. Various range options like finding the probability of cheque payment are offered by Visa.

Selection of options depends on the requirements. Some banks may choose ACH, while others who deal with high-value and high risk cheques may want to choose a system which processes the transaction in real time.

Answer: [c] Provides floating benefit to the customers

Module:6

Reference No:M6066

Question: ----- is an example of logical attack on an e-application

- [a] Hardware failure
- [b] Virus attack
- [c] Power disruptions
- [d] Property damage

Module 6- E-Business continuity

E-business continuity can be defined as technologies and strategies that a company utilises to ensure the continuous, high performance operations of an e-business application in the event of unexpected disaster/ interruption.

E-business continuity is different from traditional business continuity in the following aspects:

1. Type of events that can cause a disaster
2. The impact of such a disaster
3. The issues that are concerned with e-business continuity
4. Impact on other e-business organisations.

Impact of such a disaster on the business of an e-application

Since the major part of such a business depends on the performance of the e-business application such an outage/ disaster might have serious financial implication. The market perception of such companies may also go down.

Events than can cause such outages

These events could be both logical disruptions as well as physical disruptions. Some of the physical disrupting events could include hardware failure like server failure, power disruptions and physical damage to the building and the property. The logical disrupting events could include virus attacks; denial of service attacks, authentication failures, lack of adequate performance- the performance could include both system performance and capacity performance.

Impact on other e-business organisations.

Due to the integrated nature of the Internet, any disaster/outage can have multiple effect. For instance, any disruption in a web site cannot only disrupt the flow of customers to its website, but the company also faces the risk of losing a business partner. All the stakeholders that are linked to the website will also face the impact.

Strategies employed to deal with e-business continuity

Some of the strategies that are being used by organisations to prevent such disasters are

- Net traffic redirection
- Geographical load balancing
- Call centre fail over

Net traffic redirection

In this case a secondary web server is maintained. All the traffic is rerouted to the second server. This will not have a negative impact on the performance of the e-application in the case of a disaster.

Geographical load balancing

In this case alternate web servers are maintained. These servers are geographically maintained. All the web traffic will be automatically distributed between the dispersed web servers based on the availability on the capacity load.

Call centre fail over

Here, an offsite call centre is maintained. This call centre will consist of personnel and equipment that can handle all the customer queries and undertake product orders. All the web traffic will be rerouted to the call centre.

Role of an auditor in the e-business continuity plans

The auditor can play active role in the implementation of such plans by advising the organisations on ways to plan. He can also assess the effectiveness of such plans. The assessment of such plans is much in the same way as in any traditional environment.

Answer: [b] Virus attack

Module:6

Reference No:M6067

Question: Which of the following features doesn't play a role in exposing an Attendant console of a PBX system to security risks?

- [a] Password access
- [b] Administrative features
- [c] Physical connection
- [d] Authorisation access

Module 6- Private Branch Exchange (PBX) - Risks

With the increase in security threats and risks associated with a PBX, it is essential to make a study on the potential vulnerabilities and the counter measures. Relevant to this issue is the risk analysis of remote access or administration of a PBX.

Remote access risks

Remote administrative access comes as a double-edged sword as it is very useful feature of a PBX and at the same time vulnerable to intrusion. An administrator is able to make changes to the system settings database through the help of an attendant console or a system terminal, which is located in a remote place. A dial-in line with a modem could accomplish this.

Attendant Console

There are several factors that determine the degree of vulnerability of remote access through an attendant console. Some of them include password access, availability of administrative features and physical connection access. In case, there are no formal methods of password protection then the other factor of physical access to the console becomes more important. An intruder can break into the network to get access to administrative functions between the PBX and the attendant console if the connection is same as the one with telephone instruments.

Remote access terminal

When a dumb terminal is employed for access to administrative features, then there is more scope for intruders. A modem connected to a terminal port and dial-in line would give a comfortable access to the PBX system administration. The same is true with the case of an adversary. In addition to this, if an improper password facility coupled with backdoors (a special key sequence, which can bypass the authorisation levels) would be big blow to the security of the PBX system. Testing a system for remote access can be done through following a methodology:

- By connecting a modem to the administrative or maintenance terminal port
- Another similar modem could be connected to a terminal and a line on the Public Switched Node
- Dial into the administrative or maintenance port from the remote system
- Find out the extent of access available with the configuration
- As one gets logged onto the system, disconnect the line and call back. Check if the login session is terminated automatically after the hang-up.

Counter measures

- If the attendant console is linked to the PBX with a different physical and/or electrical connection than that of the telephone instruments, vulnerability can be checked to a considerable extent.
- A kind of line configuration feature could be introduced by which a line could be specifically configured for link with an Attendant Console. In such a scenario, a telephone instrument may not duplicate an Attendant Console to gain access to the administrative features.

Alarms and audit trails

Alarms in a PBX can buzz for a variety of reasons like hardware failure, thresholds exceeded and the like. They set off depending on the functionality lost or operating in a degraded mode. A system administrator can use alarms as a mechanism to detect any deviations or malfunctioning. . An audit of the database will be helpful to pinpoint any modifications such as a user line enabled for silent monitoring which was not authorised for it. The success of an audit shall depend on the merits of the configuration management applied during switch operation.

Answer: [d] Authorisation access

Explanation: Authorisation access, since the other features determine the degree of vulnerability of an attendant console to intrusion

Module:6

Reference No:M6068

Question: In which of the following modes of communication can an intruder employ a Digital to Analog converter to listen to a speech?

- [a] Analog Voice with or without Separate Control Signals
- [b] Analog Voice with Inclusive Control Signals
- [c] Digital Voice with Inclusive Control Signals
- [d] Instrument modifications

Module 6- Private Branch Exchange (PBX)-Hardware Vulnerabilities

The various components of a PBX system are exposed to a number of threats from intruders or adversaries. Hence, a detailed study of these components is very important in the light of a PBX system, an inherent part of most organisations. The hardware components could also be reviewed to analyse the different forms of threats.

Tapping

A PBX is exposed to tapping wherein it is dependent on the mode of communication between PBX and other peripherals. This communication shall be of any form like voice, data, or signalling information. Signalling information issues commands to the instruments like indicators, microphones, and speakers to check with the status of those devices. Three of the general modes of communication shall be taken up for discussion here.

Analog Voice with or without Separate Control Signals

Analog voice information exchange takes place between the PBX and the other devices either through a single pair of wires or two pairs (one for transmitting and the other for receiving). All other form of signalling communication between the PBX and the any peripheral is done through wires that are separated from the voice pair(s). The voice data is transmitted in the same form as received by a microphone. A speaker could directly reproduce this form. It is possible to tap this voice line easily.

Analog Voice with Inclusive Control Signals

Here, analog voice and control signals are passed between the PBX and the device on either a single pair of wires or two pairs (one pair for transmitting and another for receiving). A high impedance differential amplifier could be attached to the pair. And then, the signal could be passed through filters to separate the voice and data information. More specific data can be recovered by demodulating the carrier tone.

Digital Voice with Inclusive Control Signals

In this mode, voice and control signalling data are made to pass through the same pair of wires. Two pairs of wires, one for each direction, or both directions could be deployed or else one pair of wires could be used. In case, different pairs are used to transmit and receive, each pair could be tapped. This will give access to transmit and receive digital bit streams. This in turn will help to find out the digital format of the data being transmitted. Then a DAC (Digital to Analog Converter) could be used to convert the digital data into analog voice which can listened to or recorded.

Instrument modifications risk

There are several methods to prevent eavesdropping on an analog telephone. One method is by using some special kind of telephone instruments. They come under the documentation purview of the Telephone Security Group (TSG) standards. For, digital instruments similar kind of threats exists. Ideally, any intruder has two main goals:

- To create a situation wherein the voice data will be transmitted to the PBX while giving a picture as if the instrument is on-hook.
- To modify the device so as to keep the microphone live while in an on-hook condition.

Answer: [c] Digital Voice with Inclusive Control Signals

Explanation: Authorisation access, since the other features determine the degree of vulnerability of an attendant console to intrusion

Module:6

Reference No:M6069

Question: Where does the call processing routine feature in the system architecture study for possible vulnerability analysis in a PBX?

- [a] Administrative terminals
- [b] Switching algorithm
- [c] Dual connections
- [d] Function allocation

Module 6- Private Branch Exchange (PBX)-System Architecture

Introduction

There are several aspects of addressing the methods by which an intruder shall be able to exploit vulnerabilities that are present in the system architecture. The following are the loopholes in the system architecture that can be exploited to an adversary's disadvantage.

Separation of switching and administrative functions

Computer processors controlled by software based stored programs are found in most of the modern PBXs. Microprocessors are another important component of a PBX that aid in real time

signalling and supervisory control with the help of a central processor. Operating system, maintenance access and database management functions are found in some terminals and ports. These functions help the administrative personnel with separate or distributed access as per the requirement.

Administrative Terminals: A switch is to be examined carefully. This is essential to find out if the administrative functions are carried out by the terminals connected to the PBX through the same kind of ports that switch the voice and data traffic, or by dedicated ports. In case, the connection is by the same type of voice and data ports then, an unauthorised user could switch into them unknowingly. This could be done even without a modem. On the other hand, if the ports are dedicated for use by these terminals, this threat is reduced. Even then, in certain cases, it is possible for an intruder to gain access by using a modem coupled with an unauthorised connection to a switched port. This will enable the intruder to dial in and make database modifications.

Switching algorithm: Time division multiplexing switching is done. Here each digitised voice and data port is assigned a time slot. By controlling the call processing routines, incoming time slots are connected to outgoing time slots. Switching components function normally when the number of incoming slots is not more than the number of outgoing slots. This is referred to as non-blocking switching.

Dual Connections: To check for any kind of intrusion threats, routing of another incoming time slot to an outgoing time slot in addition to the intended time slot should be done. This could be done by a database entry or by a modification to the PBX control software. Then, the test calls to verify the dual connection and to check if the calling or called party can detect the false connection must be done. If the PBX has a provision for status or maintenance query features, the modification would be analysed accordingly. The documentation is an important tool to learn the structure and operation of a PBX. In addition to this, technical discussions with the manufacturer would be beneficial in understanding the implementation details of PBX functions. There is another possibility of the manufacturer providing training on the operation and maintenance of the PBX.

Function allocation: Since most of the PBX functions are performed by software, its specific features should be studied so that potential intrusion can be explored. For example, conferencing facility could be implemented by hardware or software. Once, the design implementation is known it is easy to determine if any of the functions are vulnerable to the exploits of the adversary.

Answer: [b] Switching Algorithm

Module:6

Reference No:M6070

Question: Which one among the following is a passive attack on a Private Branch Exchange (PBX) system?

- [a] Service threat
- [b] Data modification
- [c] Denial of service
- [d] Traffic analysis

Module 6- Private Branch Exchange (PBX)-Introduction

What is a PBX?

Private Branch Exchange (PBX) has become an integral part of any organisation, be it government, private or defence. A sophisticated computer-based switch, which could be conceptualised as a small, in-house, phone company for the organisation in which it operates, is a PBX. Security is a high concern aspect for the PBX and its protection is considered high priority for any organisation. A small lapse in security in a PBX can result in disastrous consequences, eg, exposure to toll fraud, theft of private, proprietary or confidential information, and loss of revenue or legal complications.

Areas of focus

An analysis of a Private Branch Exchange (PBX) has become absolutely necessary in the light of identifying security vulnerabilities. For digital-based PBXs, which are in wide usage, the following areas require special mention:

- System Architecture
- Hardware
- Maintenance
- Administrative Database/Software
- User Features

Why is security so important?

As mentioned earlier, even a small lapse in security in a PBX can result in disastrous consequences. The growth of software-based PBXs has come as a boom to a plethora of communication capabilities within these switches. But this boom has also simultaneously opened up newer avenues for a competitor to exploit the PBX in a variety of ways, viz., by using its features for an unintended purpose.

Common Threats

As PBXs comprise sophisticated computer systems, many of the threats and vulnerabilities associated with operating systems are shared by them. The threats to PBX telephone systems depend on the goals of attackers. Some of the common threats include:

- **Information Disclosure:** This refers to information or data being disclosed without authorisation, either deliberately or accidentally. Some typical examples include eavesdropping on conversations, unauthorised access to routing, address data, etc.
- **Data Modification:** Includes data alteration by reordering, deleting or modification. For example, an intruder may change billing information or modify system tables to gain additional services.
- **Service Theft:** Or toll fraud, which is a very common motive of crooks.
- **Unauthorised Access:** These include actions that allow an unauthorised user to get access to system resources or privileges.
- **Denial of Service:** Any action that prevents the system from functioning in accordanceh its intended purpose, fall under this threat. A typical example is a piece of equipment or entity being made inoperable or one that operates in a degraded state.
- **Traffic Analysis:** In this form of passive attack, an intruder can observe information about calls and make inferences about the source and destination numbers, or frequency and length of the messages being exchanged. For example, an intruder may observe a high volume of calls between a company's financial department and the stock exchange and conclude that an IPO is in the offing.

Answer: [d] Traffic Analysis

Question: The major difference between PBX security and Operating system lies in_____

- [a] The evaluation approach
- [b] Switching system
- [c] Feature richness
- [d] Local administration

Module 6- Private Branch Exchange (PBX)-Security

As the usage of digital-based PBXs is universal in every organisation, security issues and the amount of risks involved have also increased manifold. There has also been a gradual increase in software-based PBXs that resulting in a wealth of communications capabilities within these switches.

Even the most basic PBX systems can perform a wide range of functions , done previously by large-scale switches. It is important to examine the different vulnerabilities associated with PBXs and the computer-based systems deployed in them. As digital PBXs house a computer- based switching system, the security threats are shared by the ones prevalent in operating systems too. Yet, there is some difference in the nature of threats involved.

Differences in operating system security

The two important ways in which PBX security is different from conventional operating system security are underlined below:

- *External access control:* Remote maintenance is an important function to be performed in switches. These include operating system updates and patches. Therefore, the switch manufacturer, in lieu of relying on local administrators, installs the updates remotely. Remote maintenance ports and access to the switch have to be accomplished by a large number of suppliers or outside parties.
- *Feature richness:* The wide variety of applications available on PBXs like administrative features and conference functions are vulnerable to unexpected attacks from outsiders. Often, the applications interact in unpredictable ways. This will lead to a system compromise, even if each component works in accordance with its security requirements and the system is operated and monitored correctly. Many of the features are common for all the PBXs but its implementation is bound to vary. For example, most PBX vendors have proprietary designs for the digitalsignaling protocol standards between the PBX and the user instruments. Due to this reason, digital instruments are incompatible with PBXs of different manufacturers. The degree of vulnerability depends on feature implementation as applicable to each PBX.

Evaluation approach

Some features of a PBX function on different methods of investigating vulnerability. For other issues, the approach is essentially dependent on architecture and needs further explanation. The nature of skills, evaluator requirements, the length of time required to perform the evaluation, among other functions, do not fall under a fixed pattern. They depend on the size and complexity of the PBX under scrutiny. By evaluating the organisation, the nature of perceived threat and the seriousness of any discovered vulnerabilities could be arrived at. Subsequently, any corrective actions will depend on the cost outlay. An evaluation carried out by two or more individuals will be

highly efficient since it would be helpful to share observations and gain the advantage of multiple insights.

Answer: [c] Feature richness

Module:6

Reference No:M6072

Question: ----- provide the hardware, software and networking solutions for online traders

- [a] Metamediateries
- [b] Technology providers
- [c] Software solution providers
- [d] All of the above

Module 6- Introduction to e-commerce

Towards the turn of the century, e-commerce was touted to be the newest wonder of the world. E-commerce was the latest panacea to bring customers back by droves and make every company's counters ring. While this did not happen as forecast, e-commerce or Internet commerce has emerged as one of the most interesting manifestations of the Internet. "Content has been the King" for a long while on the Internet; but, content alone does not translate into a big revenue model on the Net for all. Rapid advancements in communication technology & networking, better perceptions about online security and improved last-mile connectivity into homes has made global sales interactions possible, at vastly reduced costs. This has revolutionised the way traditional businesses operate and allowed even small companies to transform their operations and migrate easily into the digital economy.

Just another shop? Or is it much more?

E-commerce refers to buying and selling products or services through the Internet. E-commerce deployment involves:

- Setting up an online shopping mall or a virtual storefront,
- Driving traffic into the store
- Allowing visitors to browse and pick up products
- Encouraging visitors to "try them on virtually"
- Enabling them to add the choices into an online shopping cart
- Setting up varied payment options, including the easiest one allowing you to just use your credit card online
- Tying up with a third-party logistics player to deliver the products & services to customers at a pre-scheduled time, decided at the time of completing the transaction.

E-commerce undoubtedly expands the company's reach by drawing in customers from geographic locations not yet covered physically. More importantly, it allows the marketing department of companies to track customers' personal preferences and buying habits by enabling cookies in the customers' web browser. Companies can then build and establish strong relationships with different customer groups or even customise their deliveries based on individual preferences. No wonder then that everyone is looking to join this bandwagon.

Can't do it on your own? Help is on its way.

The increasing demand for virtual malls by online traders has given birth to a new genre of service providers widely referred to as "metamediateries or market makers" and "technology providers"

Metamediateries focus on specific industries and employ various market-building mechanisms to attract buyers and mediate online transactions. They also provide supply chain solutions to online traders apart from creating a customer base for the company. Such marketplace providers charge commissions based on the gross amount of each transaction and the amount of advertising space provided on their sites. Some examples of such marketplaces in India include Seekandsource.com (Industrial products & services), Itnation.com (IT products in India) and Indiamart.com (auction of a range of products & services).

Technology providers as the name suggests, provide technical support to those who wish to set up their online shops. They offer hardware and networking solutions required for online trading and software solutions like online shopping carts, digital cash solutions, PKI solutions, smart card solutions et al. Technology providers also take responsibility of maintaining the software platform and application programs to ensure that the virtual malls function smoothly without any technical hitches. ActivCard (provides solutions to manage and secure smart card transactions), Entigrity (provides solutions for public key encryptions), Shopsite (solutions for shopping carts) and Exchangenext.com (with a suite of software products from India) are some examples of technology providers.

Answer: [b] Technology providers

Module:6

Reference No:M6073

Question: ----- is an audit requirement in an online audit

- [a] Privacy issues
- [b] Security issues and their loopholes
- [c] Issues pertaining to breach of contract and violation of intellectual property rights
- [d] All of the above

Module 6- E-commerce and audit implications

The Internet has probably brought out the latest paradigm change in the way companies look at providing products and services to their customers. If the Steam Engine brought about Industrial Revolution and the now ubiquitous Integrated Chip brought about the Digital Revolution, Internet can be credited with bringing about a Geographical Revolution. Access to customers has expanded dramatically; information is now available at the click of a mouse and cross-comparisons are readily offered by middlemen and other shoppers. So much so that the Internet today directly influences the conduct of business. It offers competition to companies in new-fangled areas; areas that were completely inconceivable before online business / business on net came into existence - online auctions and digital marketplaces are some newfound industries that the Internet has enabled.

Expanding the auditor's role

With the expansion of e-commerce firms, auditors are becoming sought after saviours by e-commerce firms. E-commerce systems involve more complexities than conventional trading systems. Many of these intricacies are not under the direct control of the owner of the site. Problems are compounded due to little or no technical knowledge of the end-user or the customer. Vulnerabilities in the system like hacking, denial of service attacks, and cyber-laundering bring out

the need for good controls to be built-in at the foundation instead of a post-mortem later on. Thus, auditing is becoming a significant facet of online business.

Thanks to e-commerce, audit has found new dimensions, including

- Handling of liability insurance coverage for breach of security and credit card frauds
- Maintaining customer privacy
- Legal counseling and regulatory compliance

Online business has brought about a new breed of auditor, who actually acts as an Internet law expert, to scan online sites for any overlooked loopholes that could make the vendor liable for damages.

Auditing privacy policy

The increasing demand for audit has also been triggered by a significant rise in privacy violations. For example, enabling cookies on one hand allows sites to evaluate and understand customer's buying preferences, while on the other hand they infringe on buyer's privacy. A poorly drafted privacy policy could lead the company into complicated lawsuits. An auditor plays a vital role in such cases in providing legal counsel to e-commerce companies in drafting appropriate privacy policies.

Compliance with the law

E-commerce has augmented the amount of trans-border data flow - data transfer across national borders. This includes information pertaining to international trade, scientific exchanges, corporate interactions, government relations etc. Such information exchange across international boundaries involves threats of violating privacy protection laws and laws against security breach pertaining to individual nations. Scrutinising such dataflow becomes a vital concern in online business. The auditor's role in inspecting such acts that are not uniform internationally, is crucial.

A total online audit therefore must, at the minimum, address

- Privacy issues
- Security issues and their loopholes like credit card fraud and other cyber crimes
- Issues pertaining to breach of contract and violation of intellectual property rights
- Violation of statutory duties and defamation issues

Without an audit, companies clearly run the risk of alienating their customers and being caught up in legal wrangles. An audit might, thus, be a small price to pay in the long run.

Answer: [d] All of the above

Module:6

Reference No:M6074

Question: ----- is one of the approach used to tax online transaction incomes

- [a] Permanent establishment
- [b] Residence-based
- [c] Income based classification
- [d] All of the above

Module 6- E-commerce and tax implications

Taxes are charged and collected typically in the place of residence of a company. In the case of e-commerce, where companies can transact purely online, it becomes difficult for the taxation authorities to collect the taxes. So what are the problems and how is the taxman viewing this?

Direct taxes: Tracking business on the Internet is difficult compared to offline sales, since

- There are virtually no intermediaries
- There may be no physical place of business
- Transfer pricing maybe involved

Indirect taxes: In cross border sales, the tax authorities can collect indirect taxes by coordinating with shipping companies, courier companies and the like. But difficulty arises in case of online sale of services, e.g. software downloads, e-books, as they do not have any physical existence and the entire transaction can be completed online with no offline intermediation.

Tax implications: Different approaches have been proposed, but none of them have helped the taxman to plug all the loopholes.

Residence-based: In the residence based taxation, it becomes difficult to determine the residency of an online company.

Permanent establishment (PE-based): The issues that arise in such cases are:

Does the server located in a different country constitute a PE of the company, which is in the jurisdiction of taxation authorities of this country? This issue is further complicated by whether the server is used for

- a. Advertising purpose only;
- b. Advertising and taking orders;
- c. For advertising, taking orders; and accepting the payments and
- d. Advertising, taking orders, accepting payments and digitised delivery of goods.

Can the communication channel alone constitute a PE?

Classification of income based: With the ability to sell products like books, music and the like physically and in the electronic form, it becomes complicated to classify the transaction as sale or royalty income.

Indian Tax scenario

In India, the tax implications of e-commerce transactions are at an infancy stage. A work group set up by the Income Tax Department stated that the computer terminal that is used to receive and send any information passing the Indian borders is to be regarded as PE. The work group has also stated that tax be imposed on the person who receives the asset. While these recommendations have not been implemented yet, serious thought is being given to bring about taxation of electronic commerce.

A case in example is Computerised Reservation Systems Company that provides reservation for air tickets globally through travel agents. It offered routers and software in India to direct airline companies to do their bookings on a secure server hosted outside India. The income tax authorities taxed the booking fees as income accrued in or arisen from India as the company had routers present in India.

The CRS Company went into a legal battle on the grounds that the presence of equipment cannot be considered as PE unless some business activity is conducted through such equipment. Apart from that, routers are not a vital part of equipment that are used to conduct the business. The Commissioner of Appeals held that electronic communication "crunches time & collapses space" and the company is deemed to have a presence in India and that the income be taxed.

Global tax scenario

United States: US has adopted the principles of neutrality, fairness and simplicity. As per this it treats economically similar income equally.

United Kingdom: The tax rules and compliances will be same for EC and other transactions. Only some changes will be made for effective operation of VAT system.

Australia: From the tax point of view, delivery through the Internet is no different from physical delivery.

Answer: [d] All of the above

Module:6

Reference No:M6075

Question: ----- is a type of tool for realising online transactions

- [a] Physical terminal transaction systems
- [b] Software terminal transaction systems
- [c] Virtual terminals or gateways
- [d] All of the above

Module 6- E-commerce payment systems

A robust payment solution system is a must for online business. Since there is no personal interaction between the buyer and the vendor, the system needs to provide simple, effortless and secure schemes to pay for online buys. Apart from being simple to deploy and use, these payment solutions must safeguard both the customer and the vendor against fake transactions. Typically, online transactions are initiated and handled through Merchant Accounts. These are analogous to bank accounts that allow companies to electronically collect and transfer funds based on their online transactions and are enabled by Merchant Account Providers.

The tools

The tools used for realising online transactions include:

- Physical terminal transaction systems
- Software terminal transaction systems
- Virtual terminals or gateways

Physical terminals are typically used in stores to process credit cards. Such terminals comprise a magnetic strip reader and a keypad. The magnetic strip reader reads the credit card information (typically the PIN number) when the card is swiped in. A keypad is used to key in the transaction details to be printed in the cash receipts. Data is transferred through telephone lines and dialing up the processing servers to confirm that payment has been received.

Software terminals are application programs that run on the buyer's PC. These application programs validate and process credit card charges and credits, after the credit card information is received by the vendor through fax, phone or mail. Data is transferred through modems and telephone lines. These terminals do not allow online real-time transactions (i.e. the customer has to wait for an acknowledgment from the vendor after having sent the information). Moreover, there is no assurance that the information has reached securely and to the right hands. Some examples of such terminals include IC Verify and Tellan.

Virtual terminals or gateways are application programs that run on the Payment Gateway service provider's servers. Such application programs allow a secure, encrypted method for transferring the credit card information in real-time. These are also incorporated into many online shopping cart applications. They provide reviews of previous transactions and generation of reports. The information submitted by the customer is stored in the service provider's server and it is their responsibility to securely store the credit card information. This reduces the merchant's liability. Cybercash, Signio Payments and Cybersource are some virtual terminal solution providers.

ICICI Bank in India offers an integrated solution - Payment Gateway services and also offers to become the acquiring bank and the settling bank - i.e. it acquires the online transaction by capturing the details of the order and verifying the credit or debit card particulars and also releases the payment to the merchant, once proof of delivery is established.

Answer: [d] All of the above

Module:6

Reference No:M6076

Question: ----- is a component of an online store.

- [a] Shopping cart
- [b] Customer databases
- [c] Inventory control systems
- [d] All of the above

Module 6- Conducting business through e-commerce

The Internet has revolutionised the way companies look at providing products and services to their customers. If the steam engine brought about Industrial Revolution and the now ubiquitous integrated chip brought about the digital revolution, Internet can be credited with bringing about a geographical revolution. Access to customers is simpler than ever before; information is now available at the click of a mouse and cross-comparisons are readily offered by middlemen and other shoppers. So much so that the Internet today directly influences the conduct of business. It offers competition to companies in new-fangled areas; areas that were completely inconceivable before online business. -Online auctions and digital marketplaces are some newfound industries that are extensively Internet enabled.

The e-business implementation process involves application of information technology to transact online and integration of tools that give the customers a real-time shopping experience. Online business is conducted by deploying either an electronic marketplace / online store software or online auction stores software, depending on the method of conducting the business. Additionally, a number of e-commerce tools need to be deployed to enable payment, allow for personalisation and categorisation of products and services.

Buying online

One needs to deploy a virtual storefront or be part of an electronic marketplace to offer products and services through the Internet. Customers can browse these stores and carry out transactions after registering. These stores are customisable with integrated online shopping carts, credit card processing systems, customer databases (to maintain customer browsing and shopping preferences), and inventory control systems. After the buyer places an order for a product or service, a logistics partner delivers it at his doorstep on payment.

Bidding online

Online auction is the same as a live auction. Buyers place their bids for items and the goods get sold to the highest bidder. The buyer is notified about the status of his bids through e-mail. Status of a bid includes information on whether the buyer is outbid or has won an item. In order to bid, buyers have to register themselves with the portal. They can place their bids through bidding forms provided by the web portal. Every new bid should be higher than the previous one by a specified increment known as a bid increment. The seller sets the amount for bid increment, and sells the product to the highest bidder.

Paying online

Electronic payment technologies have paved the way for a new way to pay - through electronic cash. Electronic or digital cash enables a secure transaction for online buys and maintains the anonymity of the payer. Quite similar to the real cash, digital cash is managed in specially designed wallets referred to as digital wallets. Ecoin and Digicash are some of the digital cash solutions. More about paying online is discussed in the subsequent article.

Answer: [d] All of the above

Module:6

Reference No:M6077

Question: Business through the Internet effects the direct taxes due to

- [a] Absence of intermediaries
- [b] Non-existence of physical place of business
- [c] Transfer pricing
- [d] All of the above

Module 6- Tax implication and e-commerce

Income tax is an area that is residence based. In the e-commerce era where business can be conducted without any physical presence, it becomes difficult for the taxation authorities to collect the taxes as it removes tax collection points from the tax system.

Direct taxes

Direct taxes are the most common type of tax on income. Business on the Internet effects the direct taxes due to:

Absence of intermediaries: In the usual business functioning manufacturers deal with wholesalers who in turn transact with retailers who form the tax collection centres. Even in case of imported goods tax authorities can collect tax from wholesalers and retailers. But in e-commerce business these tax collection centres disappear as the manufacturer can directly sell to the consumers.

Non-existence of a physical place of business: The traditional business has a fixed place of business. The fixed place of business can be an office, workshop or any building. This fixed place of business allows the tax authorities to collect income based on business nexus i.e. to collect tax on income derived from sources within that jurisdiction. But in the absence of physical place of business in e-commerce era, tax authorities have no means to collect taxes from such e-commerce sites that function outside their jurisdiction but deal with customers within their jurisdiction.

Transfer pricing: With the automation of the business process companies can easily set up many Internet businesses and transfer prices between the sister concerns.

Indirect taxes

Indirect taxes are based on the consumption of the goods and are paid by the consumers of such

goods. When sales take place across the borders in the e-commerce era it is easy for the tax authorities to collect taxes by coordinating with shipping companies, courier companies and the like. But the difficulty arises in case of sale of services, as they do not have any physical existence.

The government must find ways to trap these transactions to collect taxes. Some of the initiatives that can be taken are entering into multilateral and bilateral agreements with the government of other countries and the like.

Tax implications

Residence: In the residence based taxation it becomes difficult to determine the residency of an online company.

Permanent establishment (PE): The issues that arise are

- Does the server located in a different country constitute a PE of the company, which is in the jurisdiction of taxation authorities? This should be further analysed whether the server is used for
 - a. Advertising purpose only
 - b. Advertising and taking orders
 - c. For advertising, taking orders and accepting the payments and
 - d. Advertising, taking orders, accepting payments and digitised delivery of goods
 - Can the communication channel constitute a PE?
- Classification of income: With the possibility to sell the products like books, music and the like physically and in the electronic form it becomes necessary to classify the transaction as sale or royalty income.

Answer: [d] All of the above

Module:6

Reference No: M6023

Question: Which of the following is not a measurement criterion for the Personal Software Process?

- [a] Defects
- [b] Time
- [c] Task
- [d] Lines of codes

Module 6 – Software Configuration Management – Personal Software Process

With the increasing use of information technology in different sectors, the software industry is hard pressed to innovate and develop useful software. The focus in software development should be to develop quality products quickly. Adopting appropriate processes and methods would help in efficient cost control and release management. Analysts are of the opinion that the most important area that requires improvement in the overall software development life cycle is the development process.

In early 1990s, the SEI (Software Engineering Institute) at Carnegie Mellon University in Pittsburgh developed the 'Disciplined Software Development' model also known as the Personal Software Process (PSP). The objective of this process is 'to enable individual developers to deliver high quality software products as quickly as possible'. The PSP assigns tasks to developers for planning, coding, translation and module testing. The different stages the PSP are illustrated in the following diagram –

The MKS Integrity Manager creates task/entity, for which a detailed process is defined at each stage. Once the task is assigned to the developer, he can work on it.

The integrated Software Configuration Management (SCM) system in the PSP allows administration and control of workflow of such assigned tasks. Analysts have identified that the major problem in software development processes arises, when changes in the product/ process are not documented/ communicated properly. Change management includes the process and the procedures for the identification, documentation, validation and release of software changes that the software configuration management system administers.

The SCM tool in PSP ensures that the developer records all necessary elements while completing his task. The elements to be recorded usually include the original source code and design documents. Once this is documented, the SCM tool automatically records every change done by the developer in his task. In addition, it also reproduces all connections between the original task and the sum of all changes. These are termed 'change packets'.

The following figure illustrates the change package and development tasks -

To ensure quality and continuous improvement in the software development process, PSP covers three important measures -

Defects - The process records defects that occur during the development process. This information is recorded in the designated Defect Entity (See Figure 1). The defect entity measures the defect at each stage of the PSP and then forms the metric by assigning each defect to the task stage. This metric forms the basis for evaluating the PSP quality model -

Time - PSP records the time spent to complete each task. This is possible in two ways - either the defect entity already have corresponding time related information or the PSP introduces a new entity (See Figure 1) for timekeeping that is related to different tasks/defects. This time entity is important because it helps in resource planning, and estimating the time required for future projects.

LOC - This is an automated field as it automatically calculates the Lines of Codes (LOC) generated/changed. This is done with the help of SCM tools that keep track of changes that are made to elements.

Conclusion

PSP is a very effective tool for ensuring quality as it eliminates individual and common errors. Based on the list of recorded defects, PSP comes up with a checklist to avoid those defects in future projects. This ensures quality, minimises expenses and reduces the time cycle taken to finish the project.

Answer: [c] Task

Module: 7

Reference No: M7001

Question: Difference between the spiral model and the incremental model is:

- [a] The former is an evolutionary process, the latter is a classic process
- [b] The former is time consuming, the latter is time saving
- [c] The former does not ensure delivery of product after every iteration, the latter does
- [d] None of the above

Module 7- Spiral Model

Classic process models were never designed to deliver a complete product, because they entailed the completion of a linear sequence. Also, these models assumed that the customer or the end-user knew what he wanted at a very early stage of the software development lifecycle.

The reality however is that requirements change in the production stage itself. Besides, many iterative activities take place, because of the evolutionary nature of software production. To accommodate these necessities, several evolution process models were proposed.

Evolutionary Software Process Models are defined as models, whose stages consist of expanding increments of an operational software product. There are several methodologies that subscribe to the evolutionary model. One such methodology is the Spiral Model.

Spiral Model

This methodology, developed by Boehm, differs from other methodologies in several respects. It is cyclic rather than linear in nature. This methodology combines iterative aspects of prototyping with controlled and systematic aspects of a linear model. In contrast to the incremental model, the spiral model is more of prototyping and less of linear sequential.

This model emphasises the use of risk management techniques, and concentrates on risk-avoidance rather than being release-driven. It comprises a number of framework activities that are termed task regions, and include:

Customer Communication

This task requires establishing effective communication channels between the customer and the developer. The customer and the developer meet to define objectives that the software is intended to address. It usually involves interviewing a number of users, representing all departments or aspects of the existing system.

Planning

The objective of software project planning is to provide a framework that enables managers to make reasonable estimates of resources, costs and schedules. These estimates are made within a limited time frame at the beginning of the project, and regularly updated during its course. Estimates should also attempt to define best and worst situations, keeping in mind the contingency factor.

Risk Analysis

These are a set of tasks that help the software team to understand and manage uncertainty. Risk is a potential problem, hence it is always a good idea to identify and assess its probability, as also develop a contingency plan.

Engineering

This stage deals with designing the final product, and makes use of various tools and algorithms, to represent the flow of data. User-interfaces are decided upon, and the database structure is established.

Construction/Release

Here, the software is developed using relevant technology, incorporating all the features required by the customer. The product is then tested and installed. This stage also deals with providing documentation and training to the customer, to get acclimatised to the new working environment.

Customer Evaluation

Feedback about the product is obtained from the customer, during this stage. The customer might come up with a few suggestions, which may have to be included in the software.

These tasks represent one complete spiral. The software engineering team moves in a cyclical manner. The first cycle might result only in the development of the specification, while the second might only produce the design. This means that all the activities of a conventional process viz. requirement analysis, design, etc. have to undergo different stages of the spiral model, and each iteration can be taken as a separate project. But unlike the Incremental Model[1], the spiral model does not ensure the delivery of a product after every iteration.

[1] Incremental Model is also one of the Evolutionary Software Process Models. This follows the guidelines of the classical processes but with an iterative nature.

Answer: [c] The former does not ensure delivery of product after every iteration, the latter does.

Module: 7

Reference No:M7002

Question: Design phase in the linear sequential model deals with: [a] Designing the data structure

- [b] Designing the user interfaces
- [c] Designing the algorithms
- [d] All of the above

Module 7- Linear Sequential Model

A software process model is a strategy that encompasses the process, methods and tools together to effectively manage and deliver a software product. This consists of four stages - problem definition, technical development, solution integration and the current state of affairs.

While the first stage seeks to identify and define the problem, the second stage aims to find solutions to them. The solutions are then implemented in the third stage,. The fourth stage aims at analysing the current state of affairs and providing a feedback to the first stage, thus completing the problem-solving loop. Based on the above process, many models have been designed to effectively manage the process of software development. One such model is the Linear Sequential Model.

Linear Sequential Model

This is also called the classic life cycle or the waterfall model. This is defined as "systematic approach to software development beginning from the system level and progressing through analysis, design, coding, testing and support". The linear sequential model was the earliest software engineering model and is patterned after the traditional engineering cycle. Let us consider the different stages separately for better understanding:

Software Requirement Analysis

At this stage, the developer and the customer meet to discuss the objectives of the software and define the new system requirements. This usually involves interviewing a number of users, representing all the departments or aspects of the existing system. The developer has to understand the information flow within the organisation i.e. where the information is being generated and whom it is meant for.

Design

Design of software is spread across four different stages and deals with aspects like data structure, user interfaces, algorithms and the like. Designing the data structure involves deciding the number and kind of database tables to be used and the relationship between the different tables. The interface design should be user-friendly. . Design of algorithms is a very important part of the software development process as it deals with the controls associated with the execution of different tasks. These designs are then documented for further use.

Code Generation

This is the stage where the design is converted into machine-readable form. More the effort that goes in setting up the design, less time consuming is writing the relevant code. With the development of technology, code generators are now available that take design specification as the input and produce the relevant code as output.

Testing

Code generation is followed by testing the software for logic, and ensures that it suits the requirements of the end-user. The software has to be scanned for any possible "errors" and "defects" that are either already present or are likely to crop-up in the future. While errors are faults in the software that are detected before it is delivered, defects are faults that are recognised once the product is in use.

Support

Change is bound to occur in the software not just because of the "bugs" that might creep in from time to time but also because of the changing external environment. The organisation might have come up with new services or operations, representation of which would have to be incorporated in the existing software. Software support or maintenance, as it is sometimes called, is aimed towards applying these changes to the existing programs.

Answer: [d] All of the above.

Module: 7

Reference No: M7003

Question: In terms of Software Configuration Management, baseline refers to:

- [a] Point of first release of the software
- [b] Point of latest release of the software
- [c] Point of latest change to the software
- [d] Point of change approved in the software and added to the project database

Module 7- Software Configuration Management

The only thing that is constant is change. Software development is no exception. It becomes complicated if changes are not tracked. Increasing number of changes can cause confusion, so changes should be analysed and recorded, before being implemented.

Software Configuration Management (SCM) can be defined as a set of activities to manage and control change, throughout the life cycle of software. One of the biggest problems in software development is poor documentation of changes that results in loss of vital information. SCM counters this loss of information by identifying all elements involved through control mechanisms, and examining changes made to these elements. It also produces a report system that reviews the status of the product.

SCM tracks and manages change with the help of:

Baselines

A baseline is a SCM concept that states that once accepted a specification or product serves as a basis, and is fed into the project database. No change can be made to this baseline, without following formal change control procedures. This is like a safe locker that is accessible only to authorised persons. Once some changes are approved and implemented, it is again added to the database.

Software Configuration Items

Output of any software process can be divided into three major categories. They are:

- Computer programs, both the source and executable code
- Documentation related to the software i.e. requirement specifications, design specifications, data flow diagrams
- Data that the program uses

These outputs are collectively referred to as *Software Configuration Items (SCIs)*. These items are organised to form configuration objects that have name, attributes and a relationship with other such objects. Configuration objects may be data models, source code to design specification and the like. These items are of vital use in tracking changes. If the items are monitored properly from time to time, it will be easier to understand the process of change, over a period of time. Many companies also baseline different tools used in a program, to maintain the version of tools like editors, compilers, etc.

Applications

Other than managing change and identifying SCIs, SCM can be put to other uses as well. It is used for Version Control of software-by monitoring the change in the software process and documenting all changes, it helps in deciding when to come up with the new version of the software.

Answer: [a] Point of change approved in the software and added to the project database.

Module: 7

Reference No: M7004

Question: In Reverse Engineering, _____ deals with the restructuring of existing source code.

- [a] Abstraction
- [b] Completeness
- [c] Interactivity
- [d] Directionality

Module 7- Reverse Engineering

Reverse Engineering originated in the hardware industry. An organisation that seeks to launch a new product in the market may disassemble a competitor's product to understand its design and manufacturing secrets. Design specifications are provided in the documentation, and the owner has proprietary rights, which cannot be violated. Reverse engineering helps to provide one or more specifications by breaking down the product.

Reverse engineering for software is quite similar. The difference here is that instead of a competitor's product, the company disassembles an earlier version of its own product. Also, because of the hyper-competition companies are eager to develop new products, as quickly as possible. The complete process of software engineering has many stages, starting from identifying requirements/specifications to designing, coding, testing, implementation, and maintenance. The traditional approach is time-consuming, hence companies prefer to start with coding, and then trace it back to the design and specification stage i.e. from a lower level of abstraction they move to a higher level of abstraction.

Technically, reverse engineering can be defined as "the engineering process of understanding, analysing, and abstracting the system to a new form at a higher abstraction level." The higher the level of abstraction, the easier it is to understand the system.

Characteristics

Abstraction Level

The abstraction level refers to the degree of design information that can be obtained from the existing source code. For example, procedural design is a low-level abstraction; whereas data and control flow models are relatively higher level of abstractions. Data and control flow models and entity-relationship diagrams are even higher levels of abstraction.

Completeness

Completeness of reverse engineering refers to the level of detail that can be extracted from the source code. In actual terms, abstraction level is inversely proportional to the degree of

completeness i.e. completeness decreases as the abstraction level increases. For example, with a given source code one may be able to derive all the design specifications, but it is relatively difficult to obtain all the data flow diagrams.

Interactivity

This refers to the degree to which the user is integrated with the tools that are used to create an effective reverse engineering process. Completeness has a direct relationship with the interactivity involved in reverse engineering. The higher the level of interaction between the user and the process; the higher will be the level of completeness.

Directionality

This refers to the direction in which the information flows after it evolves from the reverse engineering process. If the flow is unidirectional, all the information is provided to the software engineer who uses it for maintenance of the product. If the flow is bi-directional, the information can be fed into a tool or a software to restructure or regenerate the old product.

Answer: [d] Directionality

Module: 7

Reference No: M7005

Question: The prototyping approach to software development is most suitable when:

- [a] Reusable components are available.
- [b] The user is not fully aware of the requirements.
- [c] There are time constraints.
- [d] Minor changes have to be made in an existing product.

Module 7- Prototyping

Software Engineering involves the use of sound engineering principles to cost-effectively develop software that works efficiently in the real time environment. Various methodologies are used to design and develop a new software product. One such method is the prototyping method or the 'prototyping model'.

Prototyping Model

There might be instances when a user is not very clear about his requirements. He might define objectives that have to be met by the software, but might not be able to identify the input, processing and output requirements. Also sometimes, a developer himself may not be certain of the efficiency or reliability of an algorithm, or the interface that has to be set up between the user and the machine. In such cases or like situations, a prototyping model offers the best approach, and is an early approximation of a final system or product. It is an iterative, trial-and-error process that involves both developers and users. A prototype produces "running" software that becomes "working" software, after the entire development process.

The Process

The prototyping process begins with requirements gathering. Here the developer and the user meet, to define objectives that have to be met by the software. The requirements are defined in great detail, after interviewing a number of users from different departments.

This leads to the construction of a quick design or a preliminary design that is followed by the creation of the first-prototype. This is usually a scaled-down system, and roughly represents the final product.

The user then tests the mock-up, and thoroughly evaluates the first prototype. He notes its strengths and weaknesses- what needs to be added and what should be removed. The developer collects and analyses remarks from users, and fine-tune the software. Changes are made and a second prototype is developed.

The customer evaluates the second prototype in the same manner as the first one, and the preceding steps are iterated as many times as necessary, until the user is satisfied that the prototype represents the final product desired. The software is again developed based on the final prototype, and routine maintenance is carried out regularly to prevent glitches that may occur.

Disadvantages

Often, the approach tends to overlook maintenance of the software design process. When customers see a working model of the final product, they tend to ignore backend activities, and want it to be delivered as quickly as possible. They seem to forget that the model may offer problems in the long run, because the final product may require adjustments to be made in accordance with the real environment.

However, continual change tends to corrupt the system structure, leading to expensive long-term maintenance. Also, if the number of cycles performed in designing and evaluating is high, both the customer and developer may lose focus, and it could result in a poorly designed product.

Answer: [b] The user is not fully aware of the requirements

Module: 7

Reference No: M7006

Question: CASE Tools do not help in

- [a] Understanding requirements
- [b] Code generation
- [c] Security Labels
- [d] System prototyping

Module 7- Computer Aided Software Engineering (CASE) Tools

Tools are devices that help in improving the performance of a task.

CASE refers to systems development tools consisting of five components:

Diagramming Tools: Support analysis and documentation of application requirements. They contain features required to develop data flow diagrams, data structure diagrams, store data internally and program structure charts. If changes are to be made, they are fed into the system, which then automatically redraws the diagram.

Information Repository: It helps in analysing, processing, distributing and storing data. Also called Data Dictionary [1] it has all the information pertaining to system components such as data items, data flows, and details regarding the volume and frequency of each activity. These dictionaries allow easy access of information and include built in controls and safeguards that preserve the accuracy and consistency of system details.

Interface Generators: With the help of system interfaces, users enter or receive information. Interface Generators capable of preparing prototypes of user interfaces are therefore important for application prototyping.

Code Generators: Code generators enable the conversion of system specifications into executable source code. They can be used in any application area such as manufacturing control, investment portfolio analysis, or accounts management. Code generators integrated with a central information repository create reusable computer code. On being fed with details from the data dictionary the new code can be easily generated.

Management Tools: Management tools assist project managers in scheduling analyses and design activities, and allocation of resources to different activities. Some case tools allow project managers to specify customised elements like graphic symbols to describe processes, people, departments, etc.

Benefits of CASE Tools

Revising application: Applications are generally used over long periods of time. Case Tools help in easy revision of application by providing a basis for definitions and standards for data.

Facilitates System Prototyping: Changes like in- screen and report designs are made only to the interface in order to present it to the user. The code is not generated when the designs are projected. Prototyping can help produce a working system where input and output features are developed along with procedural code and data files.

Code Generation: As discussed above, the major advantage is faster coding of a program. It ensures a consistent and standard program structure, which will help during maintenance, thus minimising the occurrence of errors.

Supports Iterative Development Process: System development is an iterative process. Therefore CASE Tools support iterative steps eliminating the tedious process of diagramming, cataloguing and classification.

Weaknesses of CASE Tools

Depending on Structured Methods: Since CASE Tools are built on structured methodologies and traditional systems development life cycles; the entire organisation may not be using structure analysis methods.

Absence of Standard Levels of Methodology Support: As there is no standard CASE Tool, care should be taken while selecting a tool.

Varying of Diagrams: Tools vary in their use of diagrams. Some vendors use 'graphics only' tools for focusing on diagrams for input and analysis. Alternatively diagrams are also regarded as documents and accept input via form or specification languages and sometimes even graphic input.

Limited Scope: CASE Tools only describe the document, but do not analyse it.

Human Role: Even though CASE Tools provide assistance in modelling, verification, clerical data management and the like, the human role is necessary to understand and produce the desired output.

Answer: [a] Understanding requirements.

Module:7

Reference No: M7007

Question: Incremental Model as an approach adheres to:

- [a] More of linear sequential, less of prototyping
- [b] Less of linear sequential, more of prototyping
- [c] Best practices of both linear sequential and prototyping
- [d] Is an independent approach.

Module 7- Incremental Model

Classic process models are not designed to deliver a production system due to the assumption that an entire system will be delivered only after the linear sequence is completed. Moreover classic models also assume that the customer knows what he wants at a very early stage in the software development lifecycle.

The reality in the software development process is that, a lot of requirements change during the course of production. Also, many iterative activities take place because of the evolutionary nature of software production. To cope with product evolution in a manner so as to accommodate the changing environment, several evolution process models were proposed. These were called the Evolutionary Software Process Models and are models whose stages consist of expanding increments of an operational software product. There are several methodologies that subscribe to the evolutionary model. One such methodology is the Incremental Model

Incremental Model

In the Incremental Model, product development is done step by step. Each step follows the guidelines prescribed in the *Linear Sequential Model* i.e. design, coding, testing and support. The difference here is that while the linear sequential model performs these tasks only once, the incremental model performs them repetitively. Thus, the Incremental Model combines elements of the linear sequential model with the iterative philosophy of the prototype model. Hence it is more of linear sequential and less of prototyping.

Each stage in the incremental model is called an "increment". The first increment given to the customer is often the "core product" where the basic requirements of the customer are addressed. This is an overall architecture of the system over which the detailed increments and releases are planned. The customer might revert with changes about the existing product. These suggestions are analysed and a plan is prepared to accommodate them in the next increment. With each increment, the functionality of the software is improved and every increment is an enhanced version of the previous one. This process is repeated until the customer is satisfied and all his requirements have been addressed.

Benefits

- This model is particularly useful when resources are not enough to carry out the whole project simultaneously. By breaking down the project into small and simpler tasks, unavailability of the resource can be countered.
- It is easier to understand and test smaller increments of functionality as compared to larger ones. This also helps in managing technical risks like the changing hardware and software environments.
- Use of successive increments provides the opportunity to incorporate user refinements resulting from experience with earlier releases into subsequent releases; the resulting software is more adaptable by design.
- Software released in increments over a period of time is more likely to satisfy changing user requirements than if it were planned as a single overall release at the end of the same period.

Answer: [a] More of linear sequential, less of prototyping.

Module: 7

Reference No: M7008

Question: As a basis of determining the size of the project, COCOMO model uses:

- [a] Function points
- [b] Object points
- [c] Lines of code
- [d] None of the above

Module 7- COCOMO Model

The success of companies increasingly depends on the development of customised software solutions. Yet, many ongoing software projects overrun schedules and budgets by more than 50%. The success or failure of any software project depends heavily on estimation principles that are used.

In software estimation, it is important to recognise strong relationships between cost, schedule and quality. They constitute three sides of a triangle. Beyond a certain point, it is difficult to increase software quality without increasing either the cost or schedule or both. Similarly, development schedule cannot be drastically compressed, without hampering the quality of the software product and/or increasing the cost of development. Software estimation models can play an important role in effectively balancing these three factors. One such model is the COCOMO Model.

COCOMO Model

The original model was first published by Dr. Barry Boehm in 1981 and was known as COCOMO'81. Over a period, software development techniques changed, and the emphasis shifted to reusing existing software, and building new systems using off-the-shelf components. With this view in mind, COCOMO II was developed.

COCOMO or Constructive Cost Model is a hierarchy of three different models:

Application composition model

This is used when the project is in its nascent stage i.e. when prototypes are being developed and user-interfaces are being designed.

Early design stage model

This model is used after the preliminary activities of software development have been completed, and the software architecture is ready.

Post-architecture stage-model

This is the most detailed of all the *COCOMO* models, and is used during the construction of the software.

Any software estimation model requires knowledge of the size of the software. There are three different kinds of sizing options available. They are *function points* [1], *object points* and *LOC* [2]. The *COCOMO* model uses object points for software estimation. Object points are the number of screens, reports or other components required to build the application. Each object point is categorised into three complexity levels i.e. simple, medium and difficult. After the complexity level is decided, object points are weighted as per the specifications given by Boehm [BOE96]. The object point count is then determined by multiplying the number of object points with the weight assigned to it. All object points are then added to get the total object point count. To adjust the number of object points, if components designed earlier are being used, the formula is :

$$\text{New Object Points or NOP} = (\text{object points}) \times [(100 - \% \text{reuse}) / 100]$$

where percent of reuse is the extent to which the components are being taken off-the-shelf.

Productivity rate (PROD) is then achieved by dividing NOP by the product of number of persons hired and the their time of involvement with the project

$$\text{PROD} = \text{NOP} / \text{person-month}$$

After the productivity rate is determined, estimated effort can be derived by

$$\text{Estimated effort} = \text{NOP} / \text{PROD}$$

So, if the effort put in is always under review, it will be easier to monitor the cost incurred during the lifecycle of the project.

[1] Function Points are a measure of size of software that takes into account different measurement criterion such as number of inputs, outputs and the like.

[2] LOC stands for Lines of Code. This measures the size of the project on the basis of number of lines of source code written for each functionality.

Answer: [b] Object points

Question: The concurrent development model is used when:

- [a] The project under development is very complex
- [b] Two projects have to be tracked simultaneously
- [c] Various projects have to be tracked simultaneously
- [d] Various activities within a single project have to be tracked simultaneously

Module 7- Concurrent Development Model

Classic process models are not designed to deliver a production system, because they assume that the entire system can be delivered only after the linear sequence is completed. Classic models also assume that the customer knows what he wants at a very early stage in the software development lifecycle.

However, the reality in the software development process is that many requirements change, during the course of production. Several iterative activities take place because of the evolutionary nature of software production. To cope with product evolution in a rapidly changing environment, Evolutionary Software Process Models were proposed. These models had stages that consisted of expanding increments of an operational software product. There are several methodologies that subscribe to the evolutionary model. One such methodology is the Concurrent Development Model.

Concurrent Development Model

A project involves many complex activities ranging from design specification to end-user support. Besides, there are many concurrent activities that are carried out along side the main process. For example, the project might be in the coding phase, but there may be personnel working simultaneously on the development phase, as well as, writing specifications and setting up the design. It is difficult to track the progress of complex projects using simple models. The concurrent development model was hence developed to cater to the needs of project managers, who seek to keep track of parallel activities within a single project.

The Concurrent Development Model also referred to as *concurrent engineering* can be defined as a series of technical activities, tasks and their associated states. For example, engineering is an *activity* that comprises of *tasks* such as analysis, requirement specification and the like. Activities associated with various phases of the project are grouped together and defined as a *state*. The Concurrent Development Model defines six major states and maps the relationship of one activity with another.

For instance, customer communication is one of the foremost activities of any software process model. It begins at the 'under development' stage. Once this is over, customer communication moves on to the stage of *awaiting changes*, while analysis that was done earlier moves to the 'under development' stage. If the customer proposes changes, the analysis activity will then move to the awaiting changes stage. The under revision stage incorporates customer requirements into the product, and the customer examines it again, in the 'under review' stage. If the customer approves the design, it is baselined, and the activity is considered to be completed.

This example depicts a situation where two different activities are carried out simultaneously, in different stages. While customer communication was *awaiting changes*, analysis was *under development*. The concurrent development model can also be defined as a series of events that trigger transitions from state to state for each software engineering activity. For example, a change in customer communication from *under development* to *awaiting changes* triggered analysis activity from *none* to *under development*.

Answer: [d] Various activities within a single project have to be tracked simultaneously

Module: 7**Reference No: M7010**

Question: The data flow diagram can be used to:

- [a] Determine how to do a function efficiently
- [b] Restrict the number of times a function can be performed.
- [c] Determine requirements of user.
- [d] It makes the data requirements in a system permanent

Module 4- Tools For System Analysis

The system analyst takes care of user requirements. As and when changes have to be made, he has to make modifications, and also keep the user informed by showing it in the form of a model. This can be done with the help of models such as the Data Flow Analysis. It defines process, which build up the system, type of data used in each process, entry and exit of data and place of data storage.

Three tools used in system analysis are:

Functional Diagram: This diagram shows functions to be created for the system, process of implementation of data and number of times each function appears in the system. Each function is further broken down into smaller units. New functions should be included after careful consideration. The functional diagram shows the entry and exit of data, description of each function, information processing being done. This makes it easy for the system analyst to understand the system requirements. The functional diagram only shows what to do and not how to do.

Data Flow Diagram (DFD): The Data Flow Diagram is used to provide information required for efficient implementation of the function. It takes care of four main aspects.

- Determination of requirements of user.
- Communication between analysts and users
- Solutions by sketching the plan of a required system.
- Indicates key functional components of systems requirements and system design

Components of Data Flow Diagram

- **Process:** Graphically represented as circle or rectangle with rounded edges, it describes what transforms the input data into output. E.g. people, procedures, devices.
- **Data Flow:** Represented by an arrow, it describes the flow of information from one system to another. E.g. Document, letter, telephone etc
- **Data Storage:** Indicates the data stored or referenced by a process in the system. Represented graphically with two horizontal parallel lines.
- **Internal Factors:** Indicates system functions and process. Represented by a rectangle without one side (the breadth).
- **External Factors:** Represents a person or an organisation not within the system, but related in some way. Represented by a rectangular box without one side (the width) and an extra line at the opposite side

- **Entity Relationship Diagram (ERD):** The above tools describe effectively the functions of the system, and the manner in which information flows from one function to another. ERD describes relationships in the data flow. Data requirements in a system may change, and new applications will have to be developed. So it is important to focus on entities in database and application design, to manage future changes.

Components of ERD are:

- **Entity:** It is an event or subject related to the future system. It is determined based on the outcome of systems function analysis, and is represented by rectangles with round corners.
- **Attributes:** These are characteristics of an entity displayed by fields or columns of a table.
- **Relationships:** Relationships are indicated diagrammatically with the help of arrows.

Answer:[c] Determine requirements of user

Module:7

Reference No: M7012

Question: Which of the following is true with regard to White Box Testing?

- [a] Output of the program code is not required before the beginning of the code.
- [b] It is not very expensive.
- [c] It may involve testing every line of code.
- [d] It shows errors caused by omission.

Module 4- White Box Testing

Writing error-free software programs is not easy even for the best programmers. Testing the code in a program may take over half of the time taken to produce the program itself. A thorough testing of the software should be done to make it error free. White Box Testing is one such testing technique.

White Box Testing: It is a software testing technique in which focus is more on internal knowledge of the software to help in selection of test data. White box testing uses specific knowledge of programming code to examine outputs. The test would be correct only if the tester knows the requirements of the program. White box testing is also referred to as Structural testing, Clear Box testing, Open Box testing, Glass Box testing etc. However this testing method does not check omissions.

Types of White box Testing

Static and Dynamic Analysis: Static Analysis techniques do not require the execution of the software, while Dynamic Analysis generally referred to as testing, involves execution of the system.

Statement Coverage: Here, every line of the code is tested at least once.

Branch Coverage: A series of tests are performed to ensure that all branches are tested at least once.

Path Coverage: This involves testing all the paths.

All-definition-use-path coverage: This testing involves identifying and testing all paths between the definition of a variable and the use of that definition.

White box testing usually leads to modification of the program. Also, testing values have to be changed and there is a need to generate a complete set of input data so that all path and branches are covered. This form of testing may be enough for small programs but does not suit large programs, as it takes a lot of time and will not run without major modifications. Most white box testing tools change the executable in one way or another, or check for certain classes of failures. A good White box testing tool will allow a program interface of the program to be tested. Using this, "patches" can be generated over the program which are executable for performing certain functions or collecting particular information. There are also tools which will run patches as a part of the application itself, without invading the application and using it only for experimentation.

White box testing needs clarity into the executable to determine what to test and the outcome of the test. It can output values from within the application in a most non-invasive manner.

Advantages of White Box Testing

- Time: White Box Tools speed up testing and debugging, as they do not require waiting for test support code to be inserted into the program.
- It forces test developers to reason carefully about the implementation. This helps in exclusion of unnecessary code.
- Hidden errors otherwise very difficult to find, are revealed.
- It helps in optimising code.
- Increase in quality of the software.

Disadvantages of White Box Testing

- Very expensive.
- It does not guarantee that the complete specification has been implemented.

Although white box is a powerful software testing technique, it can be cumbersome when source code modifications are needed. However, source-level patching of the executable gives an invaluable insight into the way a program works. Since testing does not require source code changes, an extensive testing can be done in shorter time.

Answer: [c] It may involve testing every line of code.

Module:7

Reference No: M7012

Question: Method used for identification of risk is called:

- [a] Risk chart
- [b] Risk graph
- [c] Risk item checklist
- [d] None of the above

Module 7- Risk Identification

Risk Identification is an attempt to identify specific threats to the completion of the Project Plan. This includes identifying all the known and predictable risks. By doing so they can be at least controlled if not avoided completely. Risks that cannot be prevented can at least be planned for.

One of the methods is to run a risk item checklist. This checklist plays a major role in risk identification and is based on the use of known and predictable risks. Let us now understand the major kinds of risks along with the checklist so as to plan for them.

Product Size

Risks associated with the overall size of the project are **product size** risks. It is often said that the bigger the project, bigger the risk of undertaking it. The checklist comprises

- Estimated Lines of Code
- Estimated size by number of programs and files
- Number of users and the like.

Business Impact

Risks that come with constraints imposed by management or the marketplace are **business impact** risks. Management is often driven by what is going on in the marketplace, and this can often put unrealistic time constraints on technical development. The checklist comprises:

- Effect of the product on company income
- Feasibility of a final deadline
- Governmental constraints, and the like.

Customer Characteristics

Risks that are associated with knowledge level of the customer as well as the developer's ability to communicate to the customer are Customer Related risks. Customers vary with their choice. While a product serves one customer to the optimum, for the other it might well be a crap. The checklist comprises:

- Has the development team worked with the customer before?
- Does the customer know what he wants?
- Does the customer understand the software process? and the like.

Process Identification

Risks that are associated with defining the software development process is **process definition** risks. The checklist comprises:

- Is the process similar for all projects?
- Does management support a written policy for the projects? and the like.

Development Environment

Risks associated with the availability and quality of the tools to be used to build the product are **development environment** risks. This refers to the environment the developers will be working in. The checklist comprises:

- Are analysis and design tools available?
- Are the tools appropriate for the project?
- Is the staff trained in using the tools? and the like

Technology to be built

Risks associated with the complexity of the system to be built and the relative 'newness' of the technology of the project are **technology risks**. New technologies pose risks due to the level of understanding the developers have, as well as the reliability of the technology. The checklist comprises:

- Is the technology new to the organization?
- Is the type of software to be developed new to the organization, and the like.

Staff size and experience

Risks that come with the available manpower and knowledge of those working on the project are staff size and experience risks. The checklist comprises:

- Are the best people available?
- Do the people have the right combination of skills?
- Does the staff have the necessary training? and the like.

Answer: [c] Risk item checklist.

Module:7

Reference No: M7013

Question: Which of the following is not a subsystem of Decision Support System (DSS)?

- [a] Language System
- [b] Knowledge System
- [c] Transaction Processing System
- [d] Problem Processing System

Module 7- Decision Support Systems

Management can be described as a process by which organisational goals are achieved, through the effective use of resources. A manager has to have good interpersonal, informational and decision-making skills. Of these skills, decision-making is the most important. There are various factors that affect the decision-making process such as technology, competition, markets, political stability, government regulations and the like. With so many factors to consider, the process of decision-making becomes quite complex. To make life easy for managers, system designers have developed a system that assists managers in making key decisions. The Decision Support System (DSS) has been the outcome of their effort.

Before considering the intricacies of DSS, let us first understand different types of problems encountered by a manager:

Structured Problems

These are routine and repetitive problems with standard solutions. These require a well-defined decision making procedure i.e. given a well-defined set of input, a well-defined set of output is obtained.

Semi-structured Problems

These have some structure i.e. some inputs; outputs or procedures are not well defined.

Unstructured Problems

Here, all phases of the decision-making process are unstructured and have no well-defined inputs, outputs or procedures.

Decision Support Systems

Decision support systems couple the intellectual resources of individuals with the capabilities of the computer, to improve the quality of decisions. It is a computer-based support system for management decision makers, who deal with semi-structured or unstructured problems. A DSS consists of three interacting components:

- *Language System*: A mechanism to provide communication between the user and components of the DSS.
- *Knowledge System*: The repository of problem domain knowledge embodied in DSS either as data or procedures.
- *Problem Processing System*: A link between the other two components, it consists of one or more of the problem manipulation capabilities required for decision-making.

Basic themes of DSS

A decision support system is used to support people and not replace them. DSS focuses on effectiveness and not on efficiency of the system. While both may seem the same, there is a slight difference between the two. While effectiveness is "doing the right things", efficiency is "doing things right". The system is very interactive and user-friendly. A DSS has a backend database that may contain information regarding past experiences, and may also incorporate some problem-solving models.

Benefits

- Facilitates more effective decisions
- Enables decision makers to tackle large scale, time-consuming, complex problems
- Shortens the time period for decision-making
- Improves reliability and consistency

Limitations

- Lacks human talent and intelligence
- Has Inadequate understanding of human information processing constraints
- Only works on pre-conceived situations

Answer: [c] Transaction Processing System.

Module:7

Reference No: M7014

Question: Risk mitigation deals with:

[a] Avoiding risk

[b] Transferring risk

- [c] Accepting risks
- [d] All of the above

Module 7- RMMM Plan

Risk management does not completely eliminate risks, but is helpful for successful completion of a software development project. The process of managing risks starts with identification. Once they have been identified, the next step is to plan a strategy to avoid, monitor and manage risks. This process is called the Risk Mitigation, Monitoring and Management or RMMM.

Risk Mitigation, Monitoring and Management

Risk Mitigation

Risk mitigation not only deals with reducing the probability of risks, but also deals with avoiding, transferring, and accepting risks. A risk can be avoided by having an alternate plan. Transferring a risk involves getting someone else to share the consequences of that risk. Finally, risk acceptance is not only accepting the risk, but also creating a contingency plan, tracking the risk and implementing the plan.

Risk Monitoring

The project manager must constantly monitor the risk areas lest the problem goes out of hand. The project manager should also monitor the effectiveness of risk mitigation steps. If a risk crosses its pre-defined threshold, risk control is activated. During this phase the project manager should be documenting milestones. Also, if a non-critical task has gone beyond its estimated duration, but not beyond its threshold, a re-assessment of risks may take place.

Risk Management

Risk management comes into picture, when despite best efforts the situation goes beyond control. In such an event, resources must be dedicated to resolve the crisis. Resolving crisis has two major steps viz. managing the crisis and recovering from the crisis.

Let us take an example to understand the process of RMMM. Let us assume a scenario where an organisation is faced with the risk of late delivery of software product. It will then follow this procedure.

Mitigation

The cost associated with a late delivery is critical. In case of late delivery, the customer will not provide a letter of acceptance, which can set a bad record for the organisation. Steps have to be taken to ensure a timely delivery by gauging the scope of project based on the delivery deadline.

Monitoring

A schedule is established to monitor project status. Falling behind schedule indicates chances of late delivery. The schedule has to be followed closely during all development stages. Also, the project manager may establish milestones to ensure smooth flow of the project.

Management

Late delivery is considered to be a sin in software development. If it becomes apparent that the project will not be completed on time, the only course of action available would be to request the customer for an extension of the deadline.

Although risk management is not a panacea for all the problems, it gives the organisation a systematic process of predicting and handling risks. If no risk management process is defined then the organisation will find itself always in crisis management with little hope of success.

Answer: [d] All of the above.

Module:7

Reference No: M7015

Question: Business risk does not include:

- [a] Risk of developing software that has no takers
- [b] Risk that effects the entire project plan
- [c] Risk of developing software for an outdated business strategy
- [d] Risk of losing the support of the management, due to change in business focus.

Module 7- Types of Software Risks

A simple definition of a "risk" is a problem that is likely to cause loss or threaten the success of a project. . Often, the risk involved might have an adverse impact on the cost, schedule, quality, team morale or success of a product / project.

Risk Strategies

Two strategies are adopted to tackle unforeseen problems that may crop up from time to time. Reactive risk strategy does not believe in worrying about the problem, unless it has occurred. A project manager who follows this approach will set aside resources to deal with problems merely, as and when they arise. This is also referred to as fire-fighting. Proactive risk strategy, on the other hand, is an intelligent alternative. This strategy begins before the technical work does. It seeks to identify potential threats and their likely impact, and then develop an action plan accordingly.

Software Risks

Software risk is generally considered to consist of uncertainty and loss. Uncertainty is the probability estimation about whether the risk will occur. Loss is the direct consequence of the risk actually occurring. These two characteristics of software risk are what need to be calculated, when a risk is identified. Software risks can be divided into several categories.

Types of Risks

Project Risks

Project risks are those that have an effect on the plan that has been laid down. In other words, these risks cause time delays or cost overruns. This includes personnel, customer, resource, budgetary, scheduling and requirement risks.

Technical Risks

Technical risks are those that have an effect on the quality or the completion of the software. These risks can hamper implementation of the project, or even make it impossible to do so. When the specification of the software is not precise, programmers are uncertain about its implementation. . Technical risks are also inherent when the technology is rather new.

Business Risks

Business risks threaten the viability of the software and may jeopardise the project. Few common business risks are:

- *Market risk*: Developing software that has no "takers".
- *Strategic risk*: Developing software for an outdated business strategy.
- *Management risk*: Developing software not backed by the management, due to change in focus.
- *Budget Risk*: Developing software that may lose focus of budgetary or monetary commitments.

Predictable Risks

Predictable risks are those that can be identified based on past experience. Experience is often the difference between seeing a risk that looms large over the project, and completely missing it. Identifying risks and documenting its is also essential.

Unpredictable risks

Unpredictable risks can adversely affect project planning. These are risks that are difficult to foresee. Since they cannot be planned for, they can have a devastating effect on the project.

Answer: [b] Risk that effects the entire project plan.

Module:7

Reference No: M7016

Question: Processes in a Transaction Processing System are:

1)Data Validation 2) Data Preparation 3) Data Entry.

The order in which they are performed is:

- [a] 2,3,1**
- [b] 1,2,3**
- [c] 2,1,3**
- [d] 3,1,2**

Module 7 – Transaction Processing System

Organisations conduct their day- to-day business, by interacting with the external environment, which in turn affects their internal processes. These interactions, be it inter/intra-organisation/s, are termed as transactions. Transactions are involved at every stage in an organisation, be it for paying bills or generating sales orders.

Before the advent of computers, transactions were processed manually, but now computer based data processing has improved the speed and reduced the complexity. The transaction processing system should not be confused with a software or technology. It is an organisational activity that uses the existing information system to support management activities.

Transaction Processing Cycle

A transaction processing cycle begins with the recording of a transaction. Earlier this was done manually, but today transactions are recorded directly on to a database with the help of online terminals. Transactions once recorded, trigger a transaction document that contains the relevant data, which can later be used to update master files. Let us now consider, three important phases of a transaction processing cycle:

Data Preparation

Many transactions involve complicated procedures that a data entry operator may not be able to understand. Hence, the data should be presented in a format that is easy to understand, or else technology should be used to feed the data directly into the system from the source. There are two such technologies available:

- *Optical Character Recognition (OCR)*: It is a high-end technology that records data in a machine-readable format, and recognises special fonts and characters. The source or paper having data is exposed to an OCR device that loads a copy of the text onto the system.
- *Magnetic Ink Character Reader (MICR)*: Characters written with a special kind of magnetic ink are encoded with a device, and fed directly to the system.

Data Entry

There are two methods for data entry. These are:

- *Manual recording*: Data is recorded manually by the data entry operator like details are entered in a sales order form by a salesperson.
- *Terminal entry*: Data is fed directly into the system rather than then putting it on paper first, and then entering the details.

Data Validation

This refers to the testing of input data. The methods involved are:

- *Missing data*: Verifying whether any data has been omitted, in the process of entering.
- *Valid item size*: Checking whether the size of the data is appropriate, in accordance with the specifications
- *Range testing*: Scrutinising whether data lies within the range of values specified.

Transaction Processing Methods

There are two basic methods for processing a transaction. They are:

- *Batch processing*: In this method, the data to be processed is accumulated for a period of time, and fed into the system. Transactions processed in this manner are done periodically like reports, payrolls, etc.

- *Online Processing:* Some transactions may require the database to be updated in real time. If this data is held for longer periods, it could well effect future transactions. For such data, online processing is used so that the master file is up to date. Online processing is primarily used for inventory management.

Answer: [a] 2,3,1.

Module:7 Reference No: M7017

Question: Which one of the following options is not a characteristic of structured analysis?

- [a] It uses bottom up approach.
- [b] It uses several tools and techniques.
- [c] It uses physical and logical models
- [d] It incorporates several steps simultaneously.

Module 7- Structure Analysis

Structure Analysis is a method to analyse an existing design or system to develop a new or modified system. The system could be a hardware or network or corporate entity. Structure analysis facilitates a logical study of events in a system, without overlooking even the minute details. It does not specify the requirements of the system or its implementation, but merely states the output of the system. Structure analysis helps to increase the chances of success for the system.

Components

The system analyst uses several components for structure analysis such as:

- *Graphic symbols:* These are icons and conventions used to identify and represent various components of the system, and relationships among them.
- *Data dictionary:* It describes data present in the system precisely, so that the user and the system analyst have an easy understanding of the input, the output and the process thereof.
- *Procedure and process description:* They describe activities that form an important part of the system.
- *Rules:* These are standards laid out for describing and documenting the system accurately, unambiguously and completely.

Characteristics

Structured Analysis uses a -down approach. The whole system is written from the root to finish.

- It uses several tools, techniques and models such as function diagram, dataflow diagram, data dictionary and the like to analyse the present system, and prepare a design for a new system.
- It uses a physical model to examine the existing model, and a logical model to determine future requirements.
- It carries out different processes simultaneously, instead of sequentially improving existing ones.
- It makes even complicated procedures very easy to understand.

There is no clear-cut approach to system analysis. Different users develop their own methods of doing it. Given below are steps that are commonly followed:

- Study the operations of the system.
- Find out the requirements of the new system.
- Work on developing a new system.

The method of working should be in accordance with the guidelines provided by the system developers. Check to ensure that changes required are being incorporated into the new system, using appropriate tools, techniques and models used. Also, ensure that the documentation is easy to understand.

Importance Structure analysis primarily involves end users, system analysts, and programmers and the like. The system as an end product should be more efficient and user friendly than the previous version. Different people are involved in different stages -programmers while designing the system, analysts for preparing technical specification, diagrams etc, and users while using the end product. If the analysis is done carefully and correctly, the system will work efficiently in the real environment.

Answer: [a] It uses bottom up approach.

Module:7

Reference No: M7018

Question: If a program cannot be executed, then it requires:

- [a] Adaptive maintenance
- [b] Preventive maintenance
- [c] Perfective maintenance
- [d] Corrective maintenance

Module 7- Software Maintenance

Software maintenance is a set of activities, which is done after the software, has been delivered to the customer, and is operational. Maintenance accounts for 60-80% of the cost spent on software. Maintenance activities can be divided into two types:

Modification: These activities are often a result of changes that have been made in the specification of a system.

Debugging: These activities involve ensuring that the code is error-free.

Importance

In multifunctional software systems, changes are common and adapting to these changes is essential. Changes in the structure of a company require continual adjustments to be made to the software. So, it is standard practice to try to retrofit and modify instances of the software, throughout the customer base.

Difficulty

Maintenance of software is difficult, as it requires extra effort to think like the software developer, and understand the nuances of the task. Difficulty increases when documentation of internal coding techniques and structures is done poorly, or is not available.

If the software system is not designed for maintenance, it lacks stability when changes are incorporated. A small modification may adversely affect the entire system. Maintenance becomes difficult, when key concepts are not clearly integrated in a unified software structure. This is because tracing the path of key entities through the software system to find bugs may take a lot of time, and can be exhaustive.

Considering the above difficulties, it may sometimes be easier to rewrite the entire code. This should be done, only after careful consideration, since the costs incurred earlier would then have to be written off. But in most cases, it is better to 'fix' and run the code again.

Maintenance is inevitable

Even after the software is installed, it requires maintenance. Programs when reworked may reveal new opportunities to streamline operations, better ways to acquire data or produce reports, and redefine responsibilities of employees.

Managing maintenance

Software maintenance can be of different types, and includes Emergency debugging, Routine debugging, Data environment adaptation, Hardware or Operating System changes, User enhancements, and Documentation and code improvements among others. But a considerable part of maintenance is a result of enhancements that are required by the user.

Software maintenance activities can be classified under four headings:

1. *Corrective Maintenance*: It refers to fixing a program that cannot be executed, has errors, does not give the correct answer, or violates performance requirements. In spite of being careful while developing the software, when it is implemented users might uncover defects.

2. *Adaptive Maintenance*: It refers to modifications done to adapt to changes in the data environment, such as new product code or new file organisation, changes in the application environment such as new income tax laws, or changes in the hardware or software environment. To accommodate these changes, the software also has to be reworked, and this is referred to as adaptive maintenance.

3. *Perfective Maintenance*: It involves activities like adding new capabilities, modifying existing functions to make the product better, faster, smaller, with more functions or reports.

4. *Preventive Maintenance*: This involves activities, which make changes to software that improve maintainability, reliability, or provide a better basis for future changes.

Perfective Maintenance activities constitute a major portion of such activities.

Debugging which is done under time constraints may cost more than the routine, scheduled corrections. These are generally done under pressure, and may disrupt the delivery of new releases, and allow errors to creep in.

Software Configuration Management

Software Configuration Management helps to identify and control change, provide an appropriate product/service, and keep concerned individuals posted on the changes. It tracks and controls activities from the beginning to the end of a software development project.

Answer: [d] Corrective Maintenance

Module:7

Reference No: M7019

Question: Which of the following is not true with regard to Black Box Testing.

- [a] It may leave many program paths untested.
- [b] Both the tester and programmer are independent of each other.
- [c] Requires knowledge of internal working of the program.
- [d] Tests are designed to know if the system is sensitive to certain input values.

Module 7 - Black Box Testing

Black Box Testing does not require knowledge of internal working of the item being tested. The tester is only expected to be aware of the correct type of inputs and what the expected output is. He has no knowledge as to how the output has been arrived at. Black Box testing can be considered as testing with respect to Requirement Specifications. This makes the tester independent of the programmer. Black Box testing tries to find errors in following categories:

1. Incorrect or missing functions.
2. Interface Errors.
3. Errors in data structures or external database access.
4. Performance errors
5. Initialisation and termination errors.

Equivalence Partitioning

Equivalence partitioning defines a test case that identifies classes of errors and therefore reduces the number of test cases required. It divides the input domain of a program into classes of data from which test cases can be derived. Equivalence class represents a set of valid or invalid states for input condition. Equivalence partitioning depends on an evaluation of equivalence classes for an input condition. Equivalence Classes can be defined in the following ways:

1. If an input condition is Boolean, then one valid and one invalid equivalence classes are defined. E.g. A statement being tested can either be true or false. If it is actually true then TRUE is its valid equivalence class and FALSE is its invalid equivalence class.
2. If an input condition specifies a range, then one valid and two invalid equivalence classes are defined. E.g. If the given range is from 100 to 200 then numbers less than 100 and more than 200 form two invalid equivalence classes and numbers between 100 and 200 form one valid equivalence class.
3. If an input condition specifies a member of a set, then one valid and one invalid equivalence class are defined. A number may or may not be in a given set.. If it is present it is valid equivalence ,if not, it is an invalid equivalence.
4. If an input condition requires a specific value, then one valid and two invalid equivalence class are defined. A number can either be less than or more than the specified value therefore two invalid equivalence class. The number could also be equal to the specified number, which is one equivalence class.

Boundary Value Analysis

This method complements equivalence partitioning as it selects test cases at the edge of a class since it leads to selection of test cases that exercise boundary values. Instead of focusing solely on input conditions, it derives test cases from the output domain also.

1. For input ranges bounded by a and b, test cases should include values a and b and just above and just below a and b respectively.
2. If an input condition specifies a number of values, test cases should be developed to exercise the minimum and maximum numbers and values just above and below these limits.
3. Apply guidelines 1 and 2 to the output.
4. If internal data structures have prescribed boundaries, a test case should be designed to exercise the data structure at its boundary.

Cause Effect Graphing Techniques

This method provides a brief representation of logical conditions and their corresponding actions. It is done in four steps.

1. Input conditions (causes) and actions (effects) are listed for a module and an identifier is assigned to each.
2. A cause effect graph is developed.
3. The graph is converted to a decision table.
4. Decision table rules are converted to test cases.

Advantages of Black Box Testing

- No awareness of implementation process is necessary.
- The tester and programmer are independent of each other.
- The tests are done from a user's point of view and not the designer's point of view.
- It helps in exposing the ambiguities or inconsistencies in the specifications.
- Test cases are designed as soon as the specifications are complete.

Disadvantages of Black Box Testing

- Number of possible inputs, which can be tested is very small. It is very cumbersome to test every possible input stream.
- Test cases are difficult to design in the absence of clear and concise specifications.
- It may leave program paths untested.
- It cannot be done segment specific, which may be very complex.
- The test can be of no use if the software designer has already run a test case.
- The test cases are difficult to design.

Answer: [c] The internal workings of program are required before the testing starts.

Question: Which of the following testing method is used when the loops in a program are not structured.

- [a] Flow graphs
- [b] Graph Matrix
- [c] Concatenating loop
- [d] No testing is done until loops are redesigned and structured.

Module 7- White Box Testing Methods

Basis Path Testing

In this method, logical complexity measure of a procedural design is derived and used as guide for defining a basis set of execution paths. Every statement in the program is tested at least once, by using basis set.

Flow Graphs

These are used to represent control flow in a program and help in the derivation of the basis set.

- Each flow graph node represents one or more procedural statements.
- Flow of control is represented by the edges between the nodes. An edge terminates at a node, irrespective of usefulness of the procedural statements.
- A region in a flow graph is an area bounded by edges and nodes.
- Each node that contains a condition is called a predicate node.

The quantitative measure of the logical complexity of a program is given by a metric, termed a Cyclomatic complexity. It defines the number of independent paths in the basis set and therefore gives an upper limit for the number of tests that must be performed.

Basis Set

A path in a program that introduces at least one new set of processing statements that moves along one new edge is called an independent path. The basis set is not unique as they can be derived for a given procedural design in different ways.

Cyclomatic complexity, $V(G)$, for a flow graph G is equal to:-

1. The number of regions in the flow graph.
2. $V(G) = E - N + 2$ where E is the number of edges and N is the number of nodes.
3. $V(G) = P + 1$ where P is the number of predicate nodes.

Deriving Test Cases

1. A Flow Graph is derived from a design or source code.
2. Cyclomatic complexity of this graph is determined. In the absence of flow graph it is determined by counting the number of conditional statements in the code.
3. A basis set of linearly independent paths is determined. Predicate nodes are used for determining the necessary paths.
4. Test cases, which force execution of each path in the basis set, are designed. Each test is executed and compared to the expected results.

Automating Basis Set Derivation

Graph matrix is a tool to derive the flow graph and the set of basis paths. The graph matrix is a square matrix whose size is equivalent to the number of nodes in the flow graph. Each row and column corresponds to a particular node and the matrix corresponds to the connections (edges) between nodes. By adding a link weight to each matrix entry, more information about the control

flow can be captured. In its most basic form, the link weight is 1 if an edge exists and 0 if it does not. Link weights can also be represented in the following ways:

- The probability that an edge will be executed,
- The probability time expended during link traversal,
- The memory required during link traversal,
- The resources required during link traversal.

Loop Testing

The White Box Testing focuses on validity of loop constructs. Loops can be defined in four classes.

1. Simple Loops: Tests applied to simple loops where n is the maximum number of allowable passes through the loop, are as follows:

1. Skip the loop entirely
2. Pass only once through the loop
3. m passes through the loop where $m < n$,
4. $n - 1$, n , $n + 1$ passes through the loop.

2. Nested Loops: Simple loops cannot be extended to nested loops as it would result in geometrically increasing number of test cases. The following approach can be adopted for nested loops:

1. Starting at the innermost loop all other loops are set to minimum values.
2. A simple loop test is conducted for the innermost loop while the outer loops are set at their minimums. Tests are done for out-of-range or extended values.
3. Work outward, conducting tests for the next loop while keeping all other outer loops at minimums and other nested loops to typical values.
4. These are continued until all loops have been tested.

3. Concatenated Loops: Concatenated loops can be tested as simple loops if each loop is tested independent of others. If not, the nested approach can be used.

4. Unstructured Loops: Unstructured loops are redesigned and then tested.

Other White Box Techniques

1. *Condition Testing:* It executes the logical conditions in a program.
2. *Data flow testing:* Using the variables in the program, test paths are selected according to the locations of definitions.

Writing error-free software programs is not easy even for the best programmers. Testing the code in a program may take over half of the time taken to produce the program itself. A comprehensive testing of the software should be done to make it error free. White Box Testing is one such tool.

White Box Testing: It is a software testing technique whereby focus is more on internal knowledge of the software to help in selection of test data. White box testing uses specific knowledge of programming code to examine outputs. The test would be correct only if the tester knows the requirements of the program. White box testing is also referred as Structural testing, Clear Box testing, Open Box testing, Glass Box testing and the like. However this testing method does not check omissions.

Types of White box Testing

- *Static and Dynamic Analysis:* Static Analysis techniques do not require the execution of the software, while the Dynamic Analysis generally referred as testing, involves execution of the system.
- *Statement Coverage:* Here, every line of the code is tested at least once.

- *Branch Coverage:* A series of tests are performed to ensure that all branches are tested at least once.
- *Path Coverage:* This involves testing all the paths.
- *All-definition-use-path coverage:* This testing involves identifying and testing all paths between the definition of variable and the use of that definition.

White box testing mostly leads to modification of the program. Also, testing values have to be changed and there is a need to generate a complete set of input data so that all path and branches are covered. This form of testing may be enough for small programs but does not suit large programs, as it takes a lot of time and will not run without major modifications. Most white box testing tools change the executable in one way or another, or check for certain classes of failures. A good White box testing tool will allow a program interface with the program to be tested. Using this, "patches" can be generated over the program which are executable for performing certain functions or collect particular information. There are also tools which will run patches as a part of application itself, but without invading the application and used only for experimentation.

White box testing needs visibility into the executable to determine what to test and the outcome of the test. It can output values from within the application in a most non-invasive manner.

Advantages of White Box

- Time: White Box Tools speeds testing and debugging, as it does not require waiting for test support code to be inserted into the program.
- It forces test developer to reason carefully about the implementation. This helps in exclusion of unnecessary code.
- The hidden errors otherwise very difficult to find, are revealed.
- It helps in optimising the code.
- Increase in quality of the software.

Disadvantages

- Very expensive
- It does not guarantee that the complete specification has been implemented.

Although white box is a powerful software testing technique, it can be cumbersome when source code modifications are needed. Source-level patching of the executable gives an invaluable insight into the way a program works. This ability to force errors requires a thorough testing.

Since testing does not require source code changes, an extensive testing can be done in shorter time.

Answer: [d] No testing is done until loops are redesigned and structured.

Module:7

Reference No: M7023

Question: Which of the following is done at various testing points in the production process.

- [a] Regression Testing
- [b] Vee Testing
- [c] Black Box Testing
- [d] Integration Testing

Module 7- Other Testing Methods

The most popular software testing types are white box testing and black box testing. Other testing types are Regression testing, Vee testing and Integration testing.

Regression Testing

It is a selective retesting of a modified software system to ensure that previous versions of the software have not run into problems due to fixing of bugs, failures due to reparations, and newly added features. This is generally done after the programmer has fixed the problem or has added source code to a program. Therefore it is also called as Verification Testing. The regression testing is more of quality control measure to ensure that the newly modified code still complies with its specified requirements and that unmodified code has not been affected by the maintenance activity.

Vee Testing

It consists of complete testing strategy at various points in the production process.

The construction of the software is indicated on the left hand side of the figure V. The first step is to determine the requirements and lay down specifications, thereafter. The design phase is concerned with the design of modules and the code phase with the detailed design and construction of subprograms.

The testing actions are indicated on the right hand side of figure V and correspond to each stage on the left side. Unit testing checks the subprograms; assembly of the modules to produce the application is done by integration testing; validation ensures that the application meets its specification; system testing ensures that the applications meet the requirements and fit into its environment.

In practice, the stages overlap to a certain extent and it is difficult to clearly demarcate the operations. The operations often reappear in different stages. Unit testing primarily relies upon white box testing techniques. Integration testing and the initial stages of validation testing make more use of black box testing techniques. White box testing is also used in Integration testing when the major paths of control through the application are considered.

Integration Testing

The integration testing can be broadly classified into down or Bottom up.

In the down integration testing, high level control routines are first tested and may keep the middle level control structures as stubs. The down testing can be done in depth-first or breadth-first manner.

In depth-first integration, each module is tested in increasing detail, replacing more and more levels of detail with actual code rather than stubs. In contrast, breadth-first would proceed by refining all the modules at the same level of control throughout the application. Generally in practice a combination of the two techniques would be used.

Initially modules may be partly functional possibly to deal with non-erroneous data. These would be tested in breadth-first manner, but over a period of time each would be replaced with successive refinements, which were closer to the full functionality. This allows depth-first testing of a module to be performed simultaneously with breadth-first testing of all the modules.

In the bottom up integration testing, an individual module is tested. A set of individual modules after being tested is combined into a collection of modules called builds, which are then tested by a second test harness. This process continues until the build consists of entire application.

Generally, in practice a combination of -down and bottom up testing is used. In a large project where a number of sub teams build different modules, individual bottom up testing is conducted before releasing them to an integration team, which would assemble them together for down testing.

Answer: [b] Vee Testing

Module:7

Reference No: M7024

Question: Which of the following is true regarding software testing?

- [a] Debugging is same as software testing.
- [b] For better results, software testing is done after implementation of the software.
- [c] Irrespective of the size of software, the documentation must be of fixed size.
- [d] Tests are designed after each level of software specification has been written.

Module 7- Software Testing I

Software Testing is the process of executing software in a controlled manner, to check for compliance with specific requirements. A good software testing has the following objective-

- Executes a program to detect errors.
- Has a high probability of finding an as yet undiscovered error
- A successful test case detects an error that may go unnoticed.

The software testing is done in a stepwise manner.

1. Software specifications and testing.
2. Test design documentation.
3. Test Case Design.
4. Test Results Documentation.
5. Results and Conclusion.

(The first part covers the software specification. Software testing in detail, is dealt in the second part.)

A software testing systematically uncovers different classes of errors with a minimum amount of time and effort. It helps in ascertaining whether the software is working as per the specifications. The test results are an indication of the software's reliability and quality. However there is no way to ensure that the software is 100% error free. Only those errors, which are identified using the test data in various paths will show. If the test data is incomplete or if there is an omission of certain path, or module, defects in those areas will not be detected.

Tests should be designed to answer the following questions:

1. How is the function's validity tested?
2. What classes of input will make good test cases?
3. Is the system particularly sensitive to certain input values?

4. How are the boundaries of a data class isolated?
5. What data rate and data volume can the system tolerate?
6. What effect will specific combinations of data have on system operation?

Accordingly, test cases should be derived such that they-

1. reduce the number of additional test cases, and
2. also mention the classes of errors, than merely the error associated with the specific test.

Software testing involves verification and validation to a large extent. Verification is checking the items, including software, for conformance and consistency. Validation is the process of checking whether the specifications are same as the ones the user actually wants.

Debugging is an activity that supports software testing. It is the process of analysing and locating bugs when software does not respond as expected. Static Analysis and Dynamic Analysis are also related to software testing. Static Analysis checks the source code of software, looking for problems and gathering metrics without actually executing the code. Dynamic analysis looks at the behaviour of software which it its executing, to provide information such as execution traces, timing profiles, and test coverage information.

Software Specifications and Testing

Depending on the size of the development and the development methods, the specification of software can range from a single document to a complex hierarchy of documents.

A hierarchy of software specifications contains three or more levels of software specification documents.

- Requirement Specification: It specifies what the software is required to do and may also specify the constraints.
- Architectural Design Specification: It describes the architecture design, which implements the requirements. Components within the software and the relationship between are described in this document.
- Detailed Design Specification: It describes how each component in the software is to be implemented.
- Hierarchy facilitates software testing at various levels. The various levels of software testing are:
- Unit Testing: Each unit (basic component) of the software is tested to verify that the detailed design for the unit has been correctly implemented.
- Software Integration testing: Progressively larger groups of tested software components corresponding to elements of the architectural design are integrated and tested until the software works as a whole.
- System Testing: The software is integrated with the overall product and tested to ensure that all requirements are met.
- Acceptance Testing: The acceptance of completed software is based on this testing.

Tests are designed after writing each level of software specification and conducted before the software is implemented. Results are evaluated after each level of testing. When a problem is encountered, either the tests are revised and applied again, or the software is fixed and the tests are applied again until no problems are encountered before proceeding to the next level.

Answer: [d] Tests are designed after each level of software specification has been written.

Module:7

Reference No: M7025

Question: The sequence and level of testing of an item or function is decided at -

- [a] Test strategy
- [b] Test Plans
- [c] Test Case Design
- [d] Test procedure

Module 7- Software Testing II

Test Design Documentation

Designing the tests itself is an elaborate process. They are designed taking the specification of the software into account. At the highest level the test software is designed to check whether the software to be tested implements the "Requirements Specification". The tests at the lower level verify whether the clauses mentioned in the Architectural Design Specification and Detailed Design Specifications are implemented.

Test Strategy

It is a statement of the overall approach to testing, identifying levels of testing to be applied. Strategy also includes techniques and tools to be used. It is ideal for use by organisations and for their software developments.

Test Plans

It states the items or functions to be tested, the level of testing sequence, the application method of test strategy, and description of the test environment. A test plan could approach the project as a whole, or hierarchy wise.

- Acceptance Test Plan: It describes the plan for acceptance testing of the software.
- System Test Plan: Describes the plan for system integration and testing.
- Software Integration Test Plan: Describes the plan for integration of tested software components and is part of Architectural Design Specification.
- Unit test specifications: Describes the plan for test cases for testing of individual units of software.

Test Case Design

After writing a test plan for each level, a test is designed to specify a set of **test cases** or **test paths** for each item at that level. The test cases may be documented with the test plan, as a section of a software specification, or in a separate document called **test specification** or **test description**.

- Acceptance Test Specification specifies the test cases for acceptance testing of the software.
- System Test Specification specifies the test cases for system integration and testing
- Software Integration Test Specifications specifies the test cases for each stage of integration of tested software components.
- Unit Test Specification specifies the test cases for testing of individual units of software.

Test cases are designed for both positive and negative testing. Positive testing checks the software for its intended functions, while negative testing checks for those, which it is not, expected to carry out.

Test Procedures

The final stage of test design is to implement a set of cases as a test procedure, specifying the exact process to be followed to conduct each of the test cases.

For each item, at its level of testing, a test procedure will specify the process to be followed in conducting the appropriate test cases. Test procedure cannot leave out steps or make assumptions. The level of detail must be such that the test procedure is deterministic and repeatable.

Test Results Documentation

- The output of each test execution is recorded in a test results file and then assessed against the criteria in the test specification to determine the overall outcome of a test.
- Each test execution is noted in a test log, which records the time of each test, the outcome of each test execution, and may include key observations made during test execution.
- The test report summarises the results of testing and analysis. An acceptance test report often forms a contractual document within which acceptance of software is agreed.

Results and Conclusion

- Software can be tested at various stages of the development and with various degrees of rigour.
- 30-70% of a project's effort has to be allotted on verification and validation activities, including software testing.
- The level of testing and software application in an organisation will depend on the potential consequences of undetected bugs.

Testing of software since the beginning of its life cycle increases its efficiency and quality when full regression testing is done. Bugs found in the later stages are costly enough to fix. Following are the guidelines for effective and beneficial software testing.

- Testing should be done against specification only.
- The testing process is documented specifying tests and recording test results.
- Testing is done hierarchically against each level of specification. Finding more errors at early stages will reduce costs.
- Planning verification and validation activities, particularly testing.
- Testing is complemented with techniques such as static analysis and dynamic analysis.
- Testing cases should be designed for both positive testing and negative testing.

Answer: [b] Test Plans

Module:7

Reference No: M7026

Question: Activities related to determining strategic business objectives based on market needs, or threat analysis falls under which stage of software acquisition?

[a] Predevelopment

[b] Development

- [c] Post development
- [d] Concept Exploration

Module 7 - Software Acquisition

Software Acquisition can be defined as the process of buying software and software services. In other words, it is the process of managing the acquisition of custom software systems. The main difference between a custom software and general software is that custom software cannot be developed by a small group of people (less than 10). Custom software involves a set of users who participate actively and contribute directly to the system requirements.

Most large-scale custom software-intensive systems usually fail. The main reason for this is poor technical performance, but poor management on the part of the developer and the acquirer. A clear example of this is California's Department of Motor Vehicles, which found the need to merge its driver license and vehicle registration systems. After seven years it had to cancel the project because of the time delay of 4 years and increase in cost, which was 6.5 times more than the original figure.

The Software Development Life Cycle (SDLC) involves a series of events which are performed sequentially, concurrently, or cyclically and done in the following steps:

- System Requirement Analysis
- Software Requirement Analysis
- Preliminary Design
- Detailed Design Code and Unit Test
- Software test and integration
- Subsystem test and integration
- System test and integration

Software Acquisition Lifecycle

Apart from the steps involved in a SDLC, Software Acquisition involves the following activities performed at both ends -

- Phase 0: Concept Exploration
- Phase 1: Program Definition and Risk Reduction
- Phase 2: Engineering and Manufacturing Development
- Phase 3: Production, Fielding/Deployment, and Operational Support

The lifecycle can be divided into three phases -

1. Predevelopment
2. Development
3. Post development

Predevelopment activities

Predevelopment activities are very important for the success of a project. They help in avoiding mistakes that can occur at the middle or at the end of the project. They clearly define activities, which are to be done before the commencement of the actual acquisition and are very critical to the project's eventual success. It starts with determining strategic business objectives based on the market. The need and threat analyses help in determining potential problems which may arise during the course of the project and help save a lot of time and money. In such cases, alternative proposals

are developed to meet objectives and feasibility studies are performed. Other activities include capturing system requirements, estimating project costs, capturing and continuously managing risks.

Development Activities

Development activities generally take a lot. There is also a possibility of user requirements changing even before the software is fully prepared. To deal with situations where last minute changes can be accommodated, the software acquirer must do two things. Firstly, the status of the project needs to be updated regularly, and secondly requirements that are not relevant any more in a changing environment should be identified and removed. The acquirer, who is the liaison between the user and the developer, should approve the design decisions after careful consideration.

Post Development Activities

After the software has been successfully developed, it has to be given to the user and installed in the environment. Maintenance of the software is delegated to a supporting organisation. There could be a possibility of the user rejecting the software at this stage. To avoid this, the developer should involve the user in the development and, testing phases, during the incorporation of new features, and prototype testing of the project.

Answer: [a] Predevelopment

Module:7

Reference No: M7027

Question: Software Acquisition Innovation Management and Continuous Process Improvement belong to which level of SA-CMM.

- [a] Level 5
- [b] Level 4
- [c] Level 3
- [d] Level 2

Module 7- Software Acquisition CMM (SA-CMM) 1

Software Acquisition CMM (SA-CMM) is a capability maturity model for organisations that acquire or procure software-intensive systems. This model helps them improve their systems acquisition process for software systems. SA-CMM gives them a better control over their software acquisition processes and helps them to:

- Enhance their understanding of software life cycle activities in relation to system acquisitions.
- Benchmark the maturity level of the organisation's acquisition process through careful assessment
- Improve the acquisition processes for software intensive systems
- Set goals for improvement for the senior management
- Enable the prediction of potential acquisition process performance

Acquiring a custom software system involves both the acquirer and the developer. Both have distinct responsibilities. The acquirer takes care of the requirements of end users and the developer deals with the acquirer's requirements, and delivers the specified capability.

Both the acquirer and developer have an important role to play in acquiring a software-intensive system.

Acquirer: The acquirer is responsible for describing functional requirements, managing user needs, allocating resources, and interacting with the developer and the staff project team. He also takes care of development activities like cost, schedule, performance and the like, and determines support requirements.

Developer: The developer decides on project proposals. He staffs the proposal team, estimates resources required, develops a detailed proposal, responds to post-contract awards, analyses requirements, designs solutions, develops software, tests and installs capabilities, and hands over maintenance to the support agency.

Process Capability

The Software Acquisition process capability is the ability of an organisation's acquisition process to produce planned, predictable and consistent, results. While developers use Software CMM, it is equally important for the acquirer to use Software Acquisition CMM. For developers, using the SW-CMM will help define and improve process capability, and bring in increased profit.

Organisational maturity can be classified according to Key Process Areas. As the organisation continuously improves itself in these key process areas, it moves from the present level to the next level. This indicates reduced risk and reworking.

At Level 1, focus is more on the people who are competent. They are the ones who have the capacity to improve and take risks.

At Level 2, focus is on the Project Management Process. The Key Process areas include project management, tracking of the contract and oversight, risk management, training etc.

At Level 3, focus is on acquisition processes and organisational support. The Key Process Areas include training, Acquisition Risk Management, Contract Performance Management, Project Performance Management and Process Definition Management.

At Level 4, Key process areas are quantity process management, and quantitative acquisition management.

At Level 5, Continuous Process Improvement is done along with Acquisition Innovation Management and Continuous Process Improvement as key process areas.

Answer: [b] Level 4

Module:7

Reference No: M7028

Question: A catastrophic failure in a memory chip is due to-

- [a] A short or open circuited wire
- [b] Improper chip insertion
- [c] Unconnected wires
- [d] Physical or electrical damage

Module 7- Memory testing-background

An embedded system is a specialised computer system that is part of a larger system or machine. An embedded system is usually a part of a single printed circuit board microprocessor with a ROM (Read Only Memory). Appliances with digital interface like watches, cars, VCRs, and micro ovens use embedded systems.

After the prototype hardware is ready, the person who designs the microprocessor board needs to ensure that the wiring of the address and the data lines has been done correctly. He should also see if the various memory chips are working properly. A memory test is performed to check if each storage location in a memory device is working properly. For example, if a number is stored at a particular address, that number should be stored there until another number is written on to that same address. The idea behind memory testing is to verify data by reading it after having written some other data on to each address in the memory device. The test is deemed successful when all the values re-read are the same as the ones written.

Memory lapses

Catastrophic failure is a type of memory problem caused by physical or electrical damage that happens to the chip after it has been manufactured. This may affect large portions of the chip. The circuit board is also vulnerable to problems because of the wiring between the processor and memory device, or due to missing or improperly inserted memory chips.

Electrical wiring problems: An error in the design or production of the board, or damage that is incurred after a chip has been manufactured are some of the main reasons for wiring problems. Wires that connect the memory device to the processor are of three types - address line, data line, and control line. The address line is used to select a memory location. The data line is used to transfer data. Control lines communicate with the memory device to check on which function the processor is performing e.g. read, write or identifying the location for data transfer. Damage to these wires occurs happens when they are shorted (connected to another wire on the board) or open (not connected to anything). This is shown below.

Fig: Shorted Wire

Fig: Open Wire

- **Missing memory chips:** Unconnected electrical wires are capacitive (the electrical property of any conductor which retains current) in nature. Due to this many memory tests do not detect a problem. For an example, applying the simple test mechanism of writing a value '5' to the first location in memory, verifying it by re-reading, writing the value '6' to the second location, verifying it and so on. Since the read and write operations occur alternatively, data that is re-read represents voltage remaining on the data bus from the previous write. Therefore, instead of performing the verification read immediately after the corresponding write, it is desirable to perform several consecutive writes followed by the same number of consecutive reads. If the data values are unique, the missing chip will be detected. The first value that is re-read will correspond to the last value written.

- **Improperly Inserted Chips:** If the chip is not inserted properly into the socket, the system will behave as if there is a wiring problem or a missing chip. To be precise, some pins on the memory chip may not be connected to the socket or connected at the wrong places. As long as the test for wiring problems and missing chips is done, improperly inserted chips can be detected automatically.

Answer: [d] Physical or electrical damage.

Module:7

Reference No: M7029

Question: In the Software Capability Maturity Model, the Productivity and Quality of a software project is measured in -

- [a] Level 1
- [b] Level 2
- [c] Level 3
- [d] Level 4

Module 7- Software Capability Maturity Model

The Software Capability Maturity Model (SW CMM) was designed to guide software organisations in controlling their development and maintenance of software. Organisations determine the maturity of a current process, and based on this select process improvement strategies.

Successful organisations concentrate on a limited set of activities and work hard to achieve them. This helps them to improve continuously and thereby gain more experience in software process capability.

Depending on the approach used, software organisations can be termed as mature or immature.

In **Immature organisations**, practitioners or the management do not plan software processes. Even if planning is done, it is not strictly followed. Immature organisations are more focussed towards solving immediate problems. Under the pressure of a deadline, the quality and functionality of the software is compromised and often overshoots schedules and budgets. Activities like reviews and testing which increase the quality of the product are skipped. There is no clear method to assess the product quality or to solve product or process problems. Hence, the product quality is very difficult to predict.

Mature organisations on the other hand have the capability to control software process development and maintenance through out the organisation. Software processes and the related roles and responsibilities are communicated to all the employees. Activities are then carried out in a planned manner and regularly updated. Continuous improvements are done through controlled pilot tests and cost benefit analyses. Managers continuously monitor the quality of the software and the processes that produces it. Procedures adopted are very consistent and practical. The objective is to use a quantitative basis for judging product quality and for analysing problems related to products and processes. Goals related to costs, schedule, functionality, and quality of the product are usually achieved.

Definitions

Software Process: A set of activities, methods, practices and transformations used to develop and maintain software and associated products. This improves as an organisation continues to mature.

Software Process Capability: It illustrates all possible outcomes when a certain software process is followed. It empowers an organisation to predict the nearest result which could be obtained when it undertakes a new project.

Software Process Performance: It indicates the actual results achieved by following a software process. It focuses on the results achieved when a software process capability focuses on the results expected.

Software Process Maturity: The degree to which a particular method is clearly defined, managed, measured, controlled, and the extent to which it is effective. It implies a potential growth in capability and indicates both the richness of an organisation's software process and the consistency with which it is applied to projects. The organisation consolidates the experience it gains in the form of policies, standards and organisational structures.

Levels of Software Process Maturity

As a company grows, process improvement built on small, steps and not on sudden drastic innovations. This growth is depicted by the CMM in five steps, each indicating a procedure to prioritise improvement efforts and a set of goals for stabilising components of the software process.

Level 1 - Initial Level

In the initial level, organisations are not steady in developing and maintaining software and therefore find it difficult to meet deadlines. This can result in a crisis. This level depends more on strong and capable people in the organisation and is therefore characteristic of individuals and not of the organisation as a whole.

Level 2 - Repeatable Level

Strategies for managing a software project, and procedures to practise them are established. On the basis of previous projects and the requirement of current projects, realistic commitments are decided. The process in this level is structured because of the viability of planning and tracking of the project, which is repeatable.

Level 3 - Defined Level

Standard methods for developing and maintaining software and management processes are documented. These are referred through out the organisation.

Level 4 - Managed Level

Quantitative quality goals are set for software products and processes. They are also measured throughout the organisation. The software process capability in this level is quantifiable and predictable. When a process overshoots its limits it is immediately controlled.

Level 5 - Optimising Level

The entire organisation concentrates on continuous process improvements and has the ability to identify its weakness and strengths. Unnecessary rework is removed. Improvements can occur incrementally or innovatively.

Answer: [d] Level 4

Module:7

Reference No: M7030

Question: To implement BPR, the best approach would be to:

- [a] Change marketing strategies in accordance with the data gathered
- [b] Develop a plan based on the data gathered
- [c] Opt for the latest technology, irrespective of its relevance to the business
- [d] Wait for an opportune moment, and chalk-out a short-term strategy

Module 7- Business Process Reengineering

When a customer makes a purchase at a store, he selects an item, makes a payment and then takes it home, or asks the store to deliver the item to his home. The entire **process** is considered as an activity that is essential to complete a transaction. **Business processes** are a set of activities, in which a set of input from one entity, is converted into a set of output, using different methods, people (services) and the like.

For a company to stay in competition it has to continuously improve its business. It has to provide services better and faster than its competitors. Customers today have several options to choose from. So companies have to constantly monitor customer requirements, and meet them.

They have to adopt the **Continuous Improvement Model** to constantly assess existing process, and make enhancements. First, the model documents activities, which are being performed; second, it determines a method to measure processes depending on customer requirements; third, it executes the process and computes the results; and finally it identifies different ways to improve business opportunities, depending on the data gathered. The process has to be ongoing.

In today's market, companies launch new products at phenomenal speed. In consequence, it is imperative for companies to restructure themselves, rather than making improvements slowly. Change takes place rapidly, and business cannot afford to lag behind. Companies can now adopt Business Process Re engineering to remain in contention.

Business Process Re engineering (BPR)

BPR assumes that the existing process can be improved upon, keeping in mind the requirements of the customer. Thereby, it does away with the old method, disentangles itself from the old processes and starts thinking about a new process. The company starts planning keeping in view the future requirements of its customers, the requirement of its employees, future market, future technology and the like.

To start with, the scope and objective of the reengineering project is defined. Interacting with the customers, employees, competitors, and non-competitors creates a knowledge base, which is then used to develop a plan that can be translated into reality.

Answer: [b] Develop a plan based on the data gathered.

Module:7

Reference No: M7032

Question: In which of the five stages in a system Life Cycle, is IT security implication involved?

- [a] Initiation Phase
- [b] Implementation Phase
- [c] Operation/Maintenance Phase
- [d] All the five stages of system development life cycle

Module 7 - Security Planning in Systems Development Lifecycle

A security plan for a computer can be developed at any stage in the life cycle of a system. However, it is better to plan for security for every stage right at the beginning of the life cycle itself. Moreover, it is always said to be cheaper if planning for security is done in the original design instead of implementing it midway. Very often it happens that a system exists in many phases at the same time. For instance, if a batch oriented input system in an organisation is being replaced by a new interactive user interface, the old batch - oriented system is in the disposal stage. The new

interactive system however is in the initiation and acquisition phase. In such cases, it becomes even more important to plan for every stage.

This article describes the various stages in the life cycle of a system and focuses on security procedures that are followed in each stage. Different models are used in an IT system life cycle. Most of them contain following stages -

- Initiation Phase
- Development / Acquisition phase
- Implementation Phase
- Operation/Maintenance Phase
- Disposal Phase

Security should be made an integral part of all the above phases

Initiation Phase

In this phase, the need and purpose of the system is identified and documented. Security procedures include conducting a sensitivity analysis, which involves analysing the criticality of the information that will be processed and used. General security requirements for system development are -

- Logical access controls
- Documentation of users and operational procedures
- Back up and recovery of procedures
- Determining cryptographic requirements

Another security area which is of concern is related to the issues in user requirement specification, which include following -

- 1.Impact analysis, which should cover areas such as the effect of disruption and financial loss, personal safety, legal liability and so on.
- 2.Threat analysis for conditions that arise due to technical complexity, network connectivity, and possibility of attack
- 3.Service level requirements in terms of number of service breaks, duration and periodicity of service breaks.

Development/Acquisition Phase

This phase deals with designing/purchasing, programming, and developing the system. Security procedures should be created to control and identify weaknesses in system development -

By error - This may include design errors, omissions, and misinterpretations.

Intentionally - System developers may introduce Trojan horses or trap doors into the system.

In addition, it is also important to have environmental security procedures in the development stage, which should involve access controls and planning for backup and recovery procedures.

Implementation Phase

In the implementation stage, all the security features should be tested and installed. Testing is important to determine if all the security procedures are working properly. If new controls are implemented at this stage, then an acceptance test of new controls has to be conducted to ensure that they are meeting security requirements. Security procedures should conduct the following types of testing -

- Module, program and system testing
- Load, stress and penetration testing

- Testing of backup and recovery procedures
- Design review tests

Operation/Maintenance Phase

Once systems are installed, many modifications are done in terms of hardware and software. In such cases, it becomes important to determine the stage in which systems are modified and security procedures that need to be applied. Questions related to security challenges that are faced in this stage -

- Whether technical controls are being managed effectively or not?
- Whether appropriate physical and personnel controls are working or not?
- Whether other procedural controls are being followed or not? Procedural controls include -
 - o Change and version control
 - o Configuration management and audit
 - o Incident reporting, investigating and analysis

Periodic Review is very important because security needs never remain constant; they keep changing with changes in the system. Thus periodic reviewing ensures that the continuity plan is changed to tackle the changing environment.

Disposal Phase

This is a stage in which the system, both in terms of hardware and software has lived its life and is ready to be disposed off. Risks involved in this stage are -

- Information may be revealed to unauthorised person
- Certain important information may be lost, in case it is not discarded properly

Thus proper steps should be taken to -

- Eradicate data properly
- Archive and manage important data and files

Answer: [d] All the five stages of system development life cycle

Module:7

Reference No: M7033

Question: A Software Quality Assurance team performs the job of:

- [a] Prepares an SQA Plan
- [b] Participate in the development of the projects software process description
- [c] Review software engineering activities to verify compliance with defined process
- [d] All the above

Module 7 - Software Quality Assurance

With competition increasing at an alarming pace, quality is foremost in the minds of any software development team. In general, quality is defined as a characteristic or an attribute of something. Software quality assurance encompasses all the activities involved in project development, which is an ongoing process.

Quality Assurance

Quality assurance consists of auditing and reporting functions of management. The goal of quality assurance is to provide management with the data that contains information on the quality so as to ensure its consistency with the goals. Quality assurance team ensures the following:

- Proper specifications for the team to work on.
- Proper specifications for integration, testing and configuration management.
- Changes in design to suit the market / customer and document the same following the version control procedures.
- Proper documentation for the products, user manuals and system manuals.

Software Quality Assurance (SQA) Activities

Software quality assurance is achieved by having a team in place that is responsible for planning, oversight, analysis and reporting. A SQA team has the following responsibilities:

Prepare an SQA Plan

A software quality plan is created as soon as the project starts. The plan encompasses a detailed description of the activities to be performed during the requirement analysis. Quality document also covers the risk analysis and failure mode analysis apart from specifying various standards and procedures. Procedures are framed for error reporting and tracking of errors and feedback is provided to the development team.

The plan is reviewed continuously during the project life cycle and necessary actions indicated and taken to ensure that the product meets the desired objective. The deviations are documented and non-compliance items tracked until they are resolved.

Participate in the development of the projects software process description

Here the software team develops a process for performance of the task, which is then reviewed by the SQA group. The SQA group then reviews the process description, checking for its compliance with the organisational policy and externally imposed standards like the ISO series.

Review software engineering activities to verify compliance with defined process

This group identifies, documents and tracks deviations from the process and verifies whether the corrections have been made. These deviations may be encountered in the project plan, process description, applicable standards or technical work products. Periodical reports are then sent to the project manager informing him/her about the progress of project.

Answer: [d] All the above

Module:7

Reference No: M7034

Question: While acquiring software which of the following criteria should be applied?

- [a] Useful life
- [b] Resale value
- [c] Cost of capital
- [d] All the above

Module 7 – Hardware Acquisition Plan

Information technology today represents the largest single line item in corporate budgets. IT expenditure is growing rapidly and is becoming increasingly decentralised. In this environment, financial executives are constantly faced with the challenge of ensuring effective management of IT operations. Also, with economy being in a state as it is, Chief Financial Officer or CFOs like to be informed about the latest technologies and devices available in the market and the cost variance between different products with the same features. They like to be informed whether the organisation is spending wisely on the latest tools and technologies.

Key acquisition criteria

While it is seemingly insignificant deciding whether to lease or purchase hardware actually makes a difference. Financial executives can benefit by closely scrutinising important acquisition decisions. Three fundamental criteria are applied to any major hardware acquisition. They are:

- *Useful Life* - In other words this means how long the equipment will last. Generally speaking, a stable, durable technology should be purchased, while rapidly evolving technology that can be replaced quickly and easily should probably be leased.]
- *Resale value* - This determines the cost of equipment in the long run. Technology bought today but will be of relatively less worth, three years from now should probably be leased.
- *Cost of Capital* - This includes corporate financial issues such as the interest rate paid when equipment is acquired, opportunity cost, etc.

When these criteria are applied to different types of mainframe hardware, significant variations can be identified. For example, CPU hardware has low resale value and is of maximum use only for three years, while the useful life of tape storage devices and printer technology can be longer than five years. In other words, based on these considerations, some types of mainframe hardware should be purchased, while other types should be leased. The particulars of individual organisations also influence lease vs. buy considerations. For a small organisation with relatively flat growth, purchasing CPU hardware might be a feasible strategy, despite significant price reductions. Large, fast-growing organisations should generally lease CPUs to efficiently leverage the benefits of new technology.

The Argument Continues...

One of the key issues in implementing a selective approach to hardware acquisition is communication between financial and IT executives. Each side must educate the other on its key issues and concerns. There is a constant debate between the two whether to go in for a lease or a purchase. Even if the basic corporate strategy is to lease, tactical purchases can still be used to advantage. As a general approach, neither leasing nor purchasing consistently delivers better unit costs for organisation hardware. By sharing their respective areas of expertise, managers and financial executives can work together to acquire hardware under the most appropriate and favourable terms.

Answer: [d] All the above

Module:7

Reference No: M7035

Question: The cost incurred in collecting data comes under:

- [a] Prevention cost
- [b] Appraisal cost
- [c] Internal failure cost
- [d] External failure cost

Module 7 – Cost of Software Quality

Cost of Quality is an accounting methodology introduced in the early 1950s to support the management practice of investing in process improvements to create higher standards. With the passage of time, as computers and technology became one of the vital factors of business, a new terminology was introduced: Cost of Software Quality or CoSQ.

The question that arises is why do we need new terminology for quality assurance in software. The reason is because work-culture that is a breeding ground for high quality software is not a fertile ground for other activities in a software project such as requirement specification, methodology, quality assurance and the like. In a typical manufacturing organisation these activities lay the foundation for any project. However, this is not so in software development. System Analysts came up with a concept that would help project managers budget their projects.

CoSQ is based on two factors, *cost incurred due to lack of quality*, and *cost incurred in maintaining and achieving quality*. Let us now take a look at the different kinds of quality costs:

Prevention Costs

This cost incurred in maintaining quality standards and preventing any quality hazards from taking place. Such costs are related to-

- *Quality planning* - Having a detailed plan describing a stepwise procedure that needs to be followed.
- *Training* - This includes the cost incurred in training personnel to implement quality.
- *Data Collection* - Cost incurred in collecting data over a period of time to derive software quality metrics.

Appraisal Costs

This includes the costs incurred in activities performed to gain insights into the product condition when it passes for the "first-time" through each process. Appraisal costs include:

- *In-process and inter process inspections* - This includes cost that is incurred in inspections that are performed during and after each process.
- *Maintenance* - This kind of cost is incurred in maintaining the quality once a desired state is achieved.
- *Testing* - This includes the cost incurred in performing periodical tests to maintain quality.

Failure Costs

Failure costs are of two kinds - Internal failure costs and External failure costs.

Internal Failure Costs

This cost is incurred when the defect is detected prior to its shipment to the client. These include:

- *Rework* - Costs incurred when the entire software is "reworked" i.e. the entire code is generated again.
- *Repair* - Costs incurred when one of the processes of the software is not working and requires some modifications.
- *Failure Mode Analysis* - Costs incurred in analysing the reasons for failure by collecting data from the client

External Failure Costs

Costs that are associated with defects found after the product has been delivered to the customer. Examples are:

- *Complaint resolution* - Cost incurred in providing customer care by having a separate team dedicated to resolving problems.
- *Product return and replacement* - Cost incurred in returning or replacing a defective product.
- *Help line support* - Cost incurred in having a customer care team that responds and notes down all complaints and suggestions from clients.

Answer: [a] Prevention Cost

Module:7

Reference No: M7036

Question: System flowcharts:

- [a] Depict relationships that link the input, processing, and output of an information system.
- [b] Evaluate and describe internal controls within the process
- [c] Illustrate the sequence of logical operations performed by a computer while executing a program
- [d] Depict the arrangement of hardware components in a computer system

Module 7- Flowcharts

After design specifications are ready, the next step in the process of software development is to write a code that adheres to the specifications given by system designers. These designers use various techniques to make the task easy for programmers, and help them to understand the system better. One such technique or tool is a flowchart. A flowchart is a diagram that uses graphic symbols to depict the nature and flow of steps in a process. It consists of boxes, diamonds, and other shapes connected by arrows, where each shape or symbol represents a step in the process, and each arrow shows the order in which the step or activity occurs.

Symbols Used

Processing: Used to denote processing steps wherein operations are performed.

Decision Making/Branching: Used to indicate decision- making situations or branching

Connector: Used to connect to other flowcharts or different stages of a flowchart.

Types

- *Document flowcharts*: It illustrates the flow of documents and information between areas of responsibility, and tracks documents from beginning to end.
- *Internal control flowcharts*: It evaluates and describes the internal control, within the process.
- *System flowcharts*: It depicts the relationship that links the input, processing and output of an information system.
- *Program flowcharts*: It illustrates the sequence of logical operations performed by a computer while executing a program.
- *Computer configuration flowcharts*: It depicts the arrangement of hardware components in a computer system.

Construction

Steps involved in the construction of a flowchart are as follows:

- Define the process and the purpose.
- Involve all members involved in the process people to develop a flowchart.
- Establish process boundaries i.e. start and end points.
- List steps, processes and decisions in a chronological sequence. Sometimes, it is easier to have a bottom-up approach.
- Assign flowchart symbols such as boxes, diamonds and the like.

Interpretation

A flowchart helps in understanding the process and uncovers ways to improve it. Interpreting the flowchart will help in determining, individuals involved in the process, and those responsible for implementing changes. The sequence of steps involved in interpreting a flowchart:

- Examine each process to look for bottlenecks, weak links, poorly defined steps, etc.
- Examine each decision symbol. Check for decisions that go one-way more often and remove the decision point.
- Examine each activity symbol. Does the step help to build or improve quality in the end-product? If not, it can be eliminated.

Answer: [a] Depict the relationship that links the input, processing, and output of an information system.

Module:7

Reference No: M7037

Question: An attribute that can have more than one value is termed:

- [a] A Composite attribute
- [b] A Multivalued attribute
- [c] A Derived attribute
- [d] None of the above

Module 7- Entity Relationship Diagrams

While designing a system, many factors have to be kept in mind. One among them is the ease of data flow between applications. Applications tend to access the backend database, so the data flow is within. A database, in itself, has a very complex structure and managing the storage and movement

of data requires a lot of expertise. To make life easy for system designers, the concept of entity relationship diagrams was introduced. Let us understand a few basic terminologies, before going into the intricacies of the concept.

Entity

Any object existing in the universe, with unique characteristics that differentiate it from other objects is referred to as an entity. It is required in the designing of a system, and is created after a thorough analysis. For example, a bank account number can be considered as an entity.

Attributes

These are unique characteristics associated with an entity, and help in their identification. They can be of different types.

- *Composite Attribute:* An attribute made up of many sub- parts like customer address that comprises street no., house no., etc.
- *Derived Attribute:* An attribute that can be derived from different attributes like the difference between an employee's date of joining and the current date can give the number of years he has been with the organisation.
- *Multivalued Attribute:* This is an attribute that can have more than one value as an employee can have multiple skills.

Relationship

These are the terms and conditions that indicate the relationship between one entity and another. It illustrates the way in which entities share information. For example, a bank has a client who has an account. Both the client and the account are independent entities, and are related to each other by the act of either depositing or withdrawing money.

Having understood the basic concepts, we can now move on to find out what exactly an entity relationship diagram is.

Entity Relationship Diagram

An Entity Relationship (ER) diagram is a diagrammatic representation of the flow of data and the logical structure of a database. It models relationships among entities involved in business processes. It is one of the most popular data modelling tools, and helps designers in creating efficient databases.

A mention of a few major symbols used in the ER diagrams:

Any existing object different from the rest on the basis of some characteristics.

An entity that relies on another entity to exist.

Characteristics that differentiate entities from each other.

Attributes that can have more than one value.

Attribute whose value is derived from another attribute.

Illustrates the way entities are linked to each other.

Answer: [b] Multivalued Attribute

Module:7

Reference No:M7038

Question: Companies use Enterprise Resource Planning (ERP) packages to:

- [a] Plan future requirements
- [b] Integrate the work of various departments
- [c] Utilise minimum resources
- [d] Find errors in a database

Module 7- Enterprise Resource Planning (ERP)

ERP is a software package used by a company to integrate all its departments and their functions into one computer system. Each department (finance, HR, logistics and marketing) can have its own computer system that is used for day-to-day activities. ERP combines these systems into an isolated and integrated software program. A single database is maintained for all the departments, so that they can communicate and share information with each other more conveniently. An ERP package is divided into a number of modules, and each module serves the purpose of a particular department. There are also a few ERP packages that are so flexible that it is possible to buy and install selected modules, depending upon the need of the company.

Role of ERP in improving a company's performance

When a customer places an order for a product, he expects quick delivery. ERP steps in to help and simplifies the order-processing stages for different departments in a company. The ERP package takes the customer order and provides a software base for automating the various steps involved in the process. When an operator enters the details of the customer order, he has all the information relevant for the completion of the order such as-Customer's credit ratingCompany's inventory levelSchedule for shipping. Etc.

People in each department update information regarding orders This information is automatically transferred to next department via the ERP system. One can even trace the profile of the order at any particular point in the order processing cycle. In this way, customers get their orders processed faster and without too many errors.

As soon as the operator enters customer details (say customer name and quantity of order) into the computer using the ERP package, the ERP screen shows information regarding:

Customer's credit rating from the finance department Whether the customer makes payments on time or not

The product's inventory level from the warehouse Whether orders are being delivered on time by the company or not.

This information is passed on to the respective departments to keep track of their responsibilities. However, in addition to the facilities that the company is enjoying because of the software itself, it is also important to know if any change is actually taking place in the company's business or not. The value of ERP in a company is realised only when the results are used to improve processes like taking orders, manufacturing goods, shipment of end products and the like.

Reasons for using ERP: Companies use ERP packages to-

1. **Integrate financial information:** The finance department may have its own revenue number, the sales department may have another version for the same and so on. ERP creates a single version of truth that is not questionable because everyone uses the same system.
2. **Integrate customer order information:** Using the ERP system, the customer order is kept alive from the time the operator receives the order, to the time of shipment. Since all the information is on single software, communication between departments increases the overall efficiency of the company.
3. **Standardise and speed up the manufacturing process:** Some manufacturing companies might make use of different methods and computer systems to make the same gadget. In such cases, ERP packages use standardised methods to automate some of the steps involved in the manufacturing process. This helps in saving time, increasing productivity and reducing overhead cost.
4. **Reduce inventory:** Manufacturing processes run smoothly when an ERP system clearly shows the ordering process in a company. This can reduce work-in-progress inventory as well as finished goods inventory.
5. **Standardise HR information:** In large companies, it is not easy for the Human Resources (HR) department to keep track of an employees' schedules to fix up a time to communicate with them. An ERP package helps them do it with ease.

.Answer: [b] Integrate the work of various departments

Module:7

Reference No:M7039

Question: The testing process conducted during the "live" application of software is a _____.

- [a] Functional test
- [b] Performance test
- [c] Beta test
- [d] Acceptance test

Module 7- Types of Tests

Testing is conducted on software to ensure that it meets specific standards. There are different types of tests. Each test addresses a specific need depending on the software application for which it is used. It is essential to: -

- Ensure that a test used for an application supports the business process and technical requirements
- Ensure that adequate time is allotted for all the activities for each test
- Assist in identifying and planning resources required for each type of test
- Ensure that the type of testing used attains the test objective

There are eight types of testing methods used for applications. They are: -

1. **Unit test:** It performs basic testing at the component level. It is used for testing a particular business process, software application or system configuration. A unit test ensures that every part of the software performs what is expected of it, and is documented correctly. It ensures that specifications for input and output are related to each other and are well defined.

2. **Integration test:** It is performed on integrated software to ensure that all modules of the program run as a single program. A unit test checks if the components are working individually, whereas integration testing checks the correctness and consistency of components working together.
3. **Functional test:** Demonstrates that the functions available are in accordance with business specifications, system documents and user manuals. According to functional test-
 - Valid input must be accepted.
 - Invalid input must be rejected
 - Functions identified must be exercised
 - Output identified must be exercised

Functional testing procedures should be implemented in business process flows, data fields, pre-defined processes and successive processes.

4. **System test:** It ensures that all the requirements of an integrated software system as a whole are met, and gives predictable results. An example of system testing is the configuration oriented system integration test.
5. **Performance test:** This determines the performance of a software application at runtime. Performance testing also determines system characteristics such as processing speed, response time, resource consumption and efficiency of the overall system. Performance testing is sometimes done along with stress testing.
6. **Beta test:** This is done at the last stage when the user uses the software application, and errors are detected at this stage. End users at customer sites conduct beta testing. During test, the customer identifies all errors encountered and sends them back to the software developer. The developer then makes necessary changes in the application, to make it error free and efficient. Hence, beta testing is a "live" application of software.
7. **Acceptance test:** It is performed before implementing the software application. Acceptance testing is generally done by a client or an application specialist to determine the acceptance criteria of the application. This is done by validating requirements and considering the documentation and business processes of the organisation. Based on the results of the acceptance test, the customer accepts or rejects the application.
8. **Regression test:** A series of tests come under regression testing. These tests ensure unwanted changes in the application. A software application needs to be maintained or updated at regular intervals. At such times, regression testing ensures that no changes that are damaging are introduced into the application. Regression testing is an iterative process. It also gives confidence that the system is functioning well, even after the implementation of new requirements.

Different tests are performed at various stages in the application development process. The quality of an application improves after testing, and provides a better product to the end-user.

.Answer: [c] Beta test

Module:7

Reference No:M7040

Question: According to Gartner, the three components of systems management are

- a) Knowledge and control
- b) Policy setting
- c) Continuous improvement

Which of the following forms the foundation of systems management?

- [a] Knowledge and control
- [b] Policy setting
- [c] Continuous improvement
- [d] None of the above

Module 7- Systems Management

System can be defined as a collection of complicated tools, components and procedures interacting together to provide information in an organisation. This complex system has to be managed carefully.

Systems management: It involves managing activities & procedures, and controlling them in an appropriate manner, so that IT operations can be carried out effectively and efficiently. Systems management also attempts to ensure optimum utilisation of resources. Further, it focuses on continuous improvement in a centralised or a de-centralised environment, to meet the future requirements of an organisation.

Elements

- **Automation:** Automating the day-to-day operations will simplify business processes. And, human resources can be assigned other responsibilities.
- **Informative and timely reports:** It helps in better planning for the future requirements of the organisation.
- **Practical policies and procedures:** It makes the technology user-friendlier, and assists in ensuring that operations are running smoothly.
- **Goals supporting corporate mission:** By achieving the final goals, the value of IT can be realised in a organisation.

Components

According to Gartner, there are 34 components involved in the system management process. They can be categorised into three major groups: -

1. Knowledge and control
2. Policy setting
3. Continuous improvement.

Knowledge and control components: The components involved in this category are the basic building blocks of systems management. It assists professionals in automating repetitive processes, and preparing timely information reports

This information will act as a source for policy setting, the next step in systems management.

Knowledge and control give a competitive edge for future planning and action.

Some of the important components in this stage are asset management automation, software inventory, hardware inventory, distribution of software, virus management, backup and storage, maintenance management and the like.

Policy setting components: The components of policy setting assist in the decision making process, and allow IT professionals to add value to the organisation and its employees. Policy setting components are implemented, only after knowledge and control components are in place. For effective planning, logical and practical procedures and policies should be implemented in accordance with the organisation's requirements.

Some of the components in policy setting are vendor selection & standardisation, change management, hardware security, data security, end-user training and the like.

Continuous improvement components: An organisation needs to improve continuously to plan ahead for the long-term, and respond to the changing environment. These components come into the picture only after policy setting components have been implemented. Important components in continuous improvement are strategic planning and quick implementation, capacity planning, highly motivated staff, stability of the IT organisation and the like.

Benefits

By continuously using appropriate tools and management practices, an IT organisation can benefit in the following ways:

- Provides better services to the end-user
- Hones the skills IT professionals
- Uses resources optimally

The components of systems management described above are appropriate for all IT organisations, but the methodology that the company adopts, depends on the size of the company and other considerations.

Answer: [a] Knowledge and control

Module:7

Reference No:M7041

Question: The most efficient stress testing tool used for both front end and backend applications is:

- [a] OpenSTA
- [b] Microsoft web application stress tool
- [c] Compuware's QALoad
- [d] Pureload

Module 7- Stress testing – Tools

There are a number of tools available for stress testing a website. Stress testing tools are used to check if web applications meet expected performance criteria. They assist in both front-end and back-end testing.

Some stress testing tools are-

- **Microsoft web application stress tool:** Used for testing web applications and observing their performance under stress. This tool is mainly used for testing websites that are not involved too much in back-end processing. However, this tool is the best of its kind for front-end testing. It runs only on Windows NT, 2000 or XP client machines; and works much like a proxy server i.e. the user need not write code manually. He can simply browse, select and record actions that need to be performed, and use it as a stress test. Pages that allow meta-analysis can be grouped together if necessary. Users can also alter stress levels by increasing the number of threads or open sockets.
- **OpenSTA:** This tool is highly programmable, powerful, flexible and free. Free in the sense that a user can download a copy of OpenSTA from the Internet and directly use it for testing purposes. The latest version of OpenSTA is Version 1.2.2. . It can be used on WindowsNT, 2000 or XP.
OpenSTA can also use a browser for primary scripting. After actions have been recorded, the user is not limited to only GET and POST commands. All the commands listed under

Script Control Language (SCL) can be scripted. For this, the user needs to learn SCL, which is used for sophisticated testing as well.

- **Pureload:** It is a Java based web application-testing tool. Pureload can run on any machine help of Java Virtual Machine (JVM) i.e. it is platform independent, with the. Pureload works through scenarios or scripts written in Extensible Markup Language (XML). If the user does not understand XML, then Pureload provides another facility for assembling test scenarios that are easy to use. Pureload can be used for Solaris, Linux and Windows NT/2K/XP. It automatically converts the results into HTML and puts them in a graphical format that enables easy comparison.
- **Compuware's QALoad:** It is a multiutility application. QALoad not tests websites, assists in back-end testing (like database, distributed application) and even speeds up legacy server applications using legacy connectivity like VT100 terminals. Like other tools it also uses a scripting language that allows a user to write or use present tests for supporting protocols. It runs on AIX, HP-UX, and Windows NT/2K/XP. However because of its flexibility and capabilities, it is slightly more expensive.
- **Loadrunner:** An expensive testing tool, Loadrunner is used by few vendors like Microsoft, IBM, Oracle and Sun to test their products. It can analyse the performance of various application in real time. Some of the applications are ISS, Allaire Cold Fusion, Enterprise Java Beans, SQL Server, Oracle, and DB2 etc. The scripting and capture language built into loadrunner provides very accurate simulations of real life conditions.

Depending upon the requirement of the customer for testing back-end or front-end applications or both, appropriate tools can be used.

Answer: [a] Compuware's QALoad

Module:7

Reference No:M7042

Question: When designing a User-Interface (UI), which principle refers to the design of UI elements in a way that is easy to relate to everyday examples?

- [a] User Profiling
- [b] Metaphors
- [c] Consistency
- [d] Visualisation

Module 7- User Interface Design I

This article provides a basic overview of the principles of User Interface Design. A User Interface takes input from the user in a way that is simple to use. It then stores this information in an appropriate location.

1. User Profiling

Before designing a user-interface, the following questions must be answered:

- What does the user need to do?
- What is the skill-level of the user?
- What does the user expect from the system?

The User Interface depends on the type of software for which it is being designed. For instance, for software such as an Operating System (OS), which may be used by different

people, it may be convenient to use classifications such as "skilled and unskilled etc to facilitate an effective user interface.

Having discussions with end-users may be very helpful in learning about their expectations and skill levels.

2. Metaphor

Complex applications can be easily understood if they can be related to simple and common examples. For instance, many audio and video software programs have an interface that is similar to the audio/video players in the real world, such as "Play", "Forward", "Rewind" etc. The symbols too are similar and hence it is easy for even a novice to use. The following should be kept in mind while developing a user-interface:

- Use a metaphor consistently in the software, and not just once
- Multiple metaphors can be used without overlapping
- Use a metaphor only if the complexity of the software component is high. For instance, "Play" is sometimes better than putting a the play symbol
- Regional and cultural differences must be taken into account while using metaphors. For instance, the Mailbox symbol common in the US would not be recognised elsewhere.

3. Displaying available Functions

Both types of interfaces, a Graphical User Interface (GUI) or a command line interface must display features available in the software to the user, or else the user may not even be aware that the feature exists! On the other hand, all the features should not be displayed, as the interface will then appear to be too complex. Features should be structured hierarchically, so that the user can easily navigate to the required feature.

For instance, to change the colour of text in a Word document, the user selects the text and then clicks on "Format>, and Font" in the toolbar. Further, when an error occurs, it should be descriptive and meaningful to the user, rather than displaying a cryptic message.

4. Consistency

All interfaces should be consistent and logical so that the user can navigate through the software easily. Consistency can be classified as:

- Internal consistency - Refers to the similarity of attributes of interface elements. For instance, if the colour of an interface element is modified using a particular operation, then all the attributes of the element must be modified using a similar operation.
- External Consistency - Refers to the consistency of the program with the platform or environment on which it runs. For instance, the program's user-interface must be look the same on the OS on which it runs as well as on software that usually run on the OS.State

5. Visualisation

This is one of the most sidelined areas of interface design. The principle behind this is that any change in the performance of the program must be accompanied by a corresponding change in the user-interface. For instance, if a user has opened

several documents and highlighted some text in each of them, he could become confused about which document would be affected if he performs an operation. It may not be clear window which is currently active will be affected by the operation.

Index:

Article 1

User Profiling, Metaphor, Displaying available Functions, Consistency, State Visualisation

Article 2

Shortcuts, Focus, Visual Grammar, Help, Safety

Article 3

Context-Sensitivity, Aesthetics, User Testing, Design Perceptions

Answer: [b] Metaphors

Explanation: Complex applications can be easily understood if they can be related to simple and common examples. For instance, many audio and video software programs have an interface that is similar to the audio/video players in the real world, such as "Play", "Forward", "Rewind" etc.

Module:7

Reference No:M7043

Question: In most GUI applications, when the application is busy processing some data, an hourglass symbol is displayed. Which principle of User-Interface is in action here?

[a] Visual Grammar

[b] Shortcuts

[c] Focus

[d] Safety

Module 7- User Interface Design II

This article is the second in a series that provides a basic overview of the principles of User Interface Design. A User Interface takes input from the user in a way that is simple to use. It then stores this information in an appropriate location.

6. Shortcuts

As users become more familiar with the software, they expect faster ways of doing things through shortcut mechanisms. For instance, key combinations can be used to perform frequently used operations and "recordable macros" can be used to automate lengthy tasks.

7. Focus

A user interface design has to take into account human senses and their responses to stimuli. The human eye, for instance, has edge detection and motion detection abilities that track any change in the colour pattern or movement on the screen. This can be exploited by providing visual clues on the state of the program. For example, the mouse cursor automatically changes to an "hourglass" when the program is busy performing calculations and cannot respond to user input.

Visual clues can be effectively used to inform the user about the state of a program.

8. Visual Grammar

There is a special kind of grammar in user-interfaces. There is a "subject" (the target on which the action is to be performed) and a "verb" (" the action to be performed). There are two common grammars in UI design: "Action->Object" and "Object-> Action." In the former, the action to be performed or a tool is chosen first, and then the destination object to be

acted on by that tool is chosen. After the action is performed, the tool continues to be active, so that further actions can be performed without having to select the same tool again. This type of grammar is also termed as "modality", since tool selection is a mode in which the program operates. The best example is a graphics program, where a tool like a pen is selected and it continues to persist till a new tool is selected.

The "Object->Action" grammar is also known as the "Direct Manipulation Interface." In this, the object is first selected and then actions are carried out on it. Here, the object persists while the tool changes. In a word processing application, for instance, the text is first selected (the text is the object) and then an action like change in font size or colour is performed on it.

This grammar is also called "non-modal", since all attributes of the object can be modified at one time.

9. **Help**

A well implemented help system can go a long way in teaching users how to use the software and act as a ready-reference guide. There are five issues that a help system must address:

- Software features explanation - Providing help on what the user can do with the software.
- Description of all features of individual components of the software, e.g.: Context-sensitive help and tool tips.
- Explanation of how to perform an action, e.g.: interactive agents or wizards
- Explanation of why an error occurred, e.g.: Well-written error messages containing advice on what must be done to prevent it
- Describing how the user can navigate through the software to accomplish a task, e.g.: Intuitive and visual navigation system

10. **Safety**

Safety in UI design refers to the comfort which a user feels while navigating through an unknown software. If a UI is complex, then a beginner might find it difficult to use and hence abandon the software. On the other hand, an expert would feel frustrated with a UI which walks him through each step, even if the operation is simple.

To manage both types of users, the program must be customisable and should also provide a "safety net" which can be turned off when not necessary. For instance, an alert box asking the user if he is sure about deleting data or not would make a novice feel comfortable. An option to turn off such features would be welcomed by an expert user.

Index:

Article 1

User Profiling, Metaphor, Displaying available Functions, Consistency, State Visualisation

Article 2

Shortcuts, Focus, Visual Grammar, Help, Safety

Article 3

Context-Sensitivity, Aesthetics, User Testing, Design Perceptions

Answer: [c] Focus

Module:7

Reference No:M7044

Question: Since it is the end-users who are going to use an application, they must be consulted and their opinions must be incorporated if found reasonable. Which of the following principle of User-Interface Design reflects the above statements?

- [a] User-Perceptions
- [b] Context-Sensitivity
- [c] User Testing
- [d] Aesthetics

Module 7- User Interface Design III

This article is the third and final in a series that provides a basic overview of the principles of User Interface Design. A User Interface takes input from the user in a way that is simple to use. It then stores this information in an appropriate location.

11. Context-Sensitivity

The software must ensure that the context of the operation is maintained and communicated to the user.

For example, a user could get confused by multiple windows being open and hence a change in the visual appearance of the windows could make it clear to the user that the other windows are not relevant to the current operation.

Another example would be when a document is being closed and a confirmation box displays the text, "Are you sure?" This could make the user uncertain about which operation is being referred to by the system. A more descriptive text such as, "Do you want to close the document titled ABC?" would be meaningful.

12. Aesthetics

A fundamental principle of design is that an object must not look ugly. For instance, having a number of copies of an interface element such as a button in different sizes can spoil the appearance of the interface.

Another important area is the "speed" of the interface. Speed here refers to the animation present in the interface and not the speed with which the program runs. For instance, a plain button can be made to look attractive by using advanced techniques such as changing colour; or using a moving graphic to depict an operation. A simple example is that of the file copying operation in a GUI, where a file flying from one folder to another demonstrates the physical copying of the file. This is more pleasing to the eye rather than presenting a text saying, "File being copied. Please wait."

13. User Testing

While a software designer can spot most defects in a UI, there might be some bugs in the software, which make it behave in an unexpected manner. These bugs are activated only when some feature of the software is used or misused. To uncover such hard-to-find bugs, it is essential for the software to be tested extensively. This testing must not be from a programming point of view, but from a user's viewpoint.

For such testing, users having skill levels that are similar to end-users must be asked to test the software and report on it. The following may be kept in mind for such testing:

Make it clear to the users that the software is being tested, not their skill level. Also, they should be given the option to exit the software if they don't feel comfortable with it

- Explain the software and its objectives
- Request them to speak their observations aloud and note them down
- Tell them to use only the help feature provided by the software
- Answer any questions they may have before they can start using the software
- Ask them to document their observations on every aspect of the User Interface. Ask them to justify their observations.
- Incorporate the observations

User testing can be used at any stage in development, however, it is suggested that the "prototype model" should be used, where a sample or part of the program is developed and user-tested first before building the real application.

14. Design Perceptions

The software being developed is to help people with their tasks. The software developer may have created a useful product, but if it is not easy to use, then the end-users may not prefer to work with it. Therefore, the opinions of users must be considered and incorporated, if found reasonable. Most end-users cannot spell all their requirements beforehand and may ask the designers to incorporate some features at a later stage in the development process. It is therefore vital for a certain amount of modularity to be built into the design so that new additions can be made with minimum effect on other parts of the design.

Designers must also keep in mind that the perception of a design varies from person to person and hence other people might feel that an interface that is considered to be simple by the designer is actually very complex.

Index:

Article 1

User Profiling, Metaphor, Displaying available Functions, Consistency, State Visualisation

Article 2

Shortcuts, Focus, Visual Grammar, Help, Safety

Article 3

Context-Sensitivity, Aesthetics, User Testing, Design Perceptions

Answer: [a] User Perceptions

Module:7

Reference No:M7045

Question: Internal testing is a part of _____

[a] Stress testing

[b] Penetration testing

- [c] Beta testing
- [d] Acceptance testing

Module 7- Internal testing

A company's website or other confidential files can be hacked by external or internal sources. According to the National Audit Office 65- 80% of the attacks are internal by employees or contractors of the company. Hence internal testing, a type of penetration testing, is a mandatory.

Access control system: Physical security is the most basic type of security, and then comes desktop security. A hacker can physically access information from the system, either by stealing it, or using it without authorised permission. To counter this, stringent testing procedures should be put in place. Attacks can be of three types: -

1. *Direct attack:* A hacker can gain access to a system by using a password, through overflow attacks, and by identifying flaws in the access control system.
2. *Operating system attack:* A hacker targets the boot process, before the access control system activates and can even access the operating system of the machine, before authentication.
3. *Hardware attack:* A hacker can overcome the access control system by physically changing the machine. For example removing the hard disk and placing it in another machine.

Network security: Granting access permissions and ensuring network encryption are security features that will prevent: -

1. Employees from accessing a particular of the network
2. External attackers from accessing any part of the network

The first feature restricts an employee. It does not give privileges to access the system or important data. Users are not allowed to access network devices such as router, web server, back office application or administrator.

The second feature deals with the physical network structure, and implementing encryption and security features in them.

Internal IP test: It involves testing to ensure that the gateway security system is not disabled, and illegal activities are locked. Here, the client may be on the internal network of the organisation, but checks should be in place to prevent breach of security. For instance, a server storing pin-numbers of credit cards, should have checks in place that prevent access, even from anyone within the company.

E-commerce customers \ VPN hosts: Sometimes companies may have to provide access to external users for e-commerce applications or for third party via Virtual Private Networks (VPNs). So issues like security implementation, strength of encryption, access to other user accounts from server among others must be tested.

Covert physical testing: After clearing security the Portcullis Penetration Test Team (PPTT) enters the client premises to: -

- Gain access to workstations, servers, backup storages and the like.
- Locate user names and passwords.
- Access insecure live workstation or server.

The PPTT is performing its service since 1995 and helps its customers by attacking the target and, just as significantly, by providing detailed reports of the findings and suggested solutions to any problems.

Social engineering: PPTT uses pseudonyms to contact client employees and gather information with regard to the network, user name, password and the like. This information is used successful testing

Content analysis system: E-mails create loopholes in the security. Worms such as QAZ, Melissa, explore .zip enter PCs by attaching themselves to the mail. PPTT is involved in supplying anti-viruses like F-port and Solomon's. It now has vast experience in programming, analysing source code of viruses and weaknesses involved in the content analysis system.

Answer: [b] Penetration testing

Module:7

Reference No:M7046

Question: Which file format requires an acrobat reader to view the file?

- [a] .zip
- [b] .pdf
- [c] .html
- [d] .arc

Module 7- File Compression and file format

Data compression is very useful for communication because it allows devices to transmit the same amount of data in fewer bits.

Compression mechanism: Usually text and graphics contain repetitive sequence of identical information. The repetitive data is removed, and only a single copy of data is transmitted. This is done using compression software that uses mathematical techniques to reduce the storage space. All the files on the Internet (sent or received) are in a compressed format, so that file transfer is faster, and occupies less space for storage. The 'self-extracting' file is the most common form of compressed file used for this purpose. It will decompress the file as soon as the user runs it. For different operating systems, different compressing files are used. They are:

- For Macintosh OS: The most commonly used file format is .hex or. bin files.
- For Windows OS: The most popular file is a .zip file. In some software, .zip decompressors are preinstalled.
- Unix OS: Here, files are first 'tarred' and then 'g-zipped', i.e. files are in .tar.gz format

Some files are already in compressed format like .gif, .jpeg. So, even if they are compressed, it will not save much space. Data compression is widely used in backup utilities, spreadsheet applications, DBMS and the like.

File format and extension: Users encounter different file formats. By looking at the extension, a user can identify the file type. The extension is usually represented by a dot followed by 3-4 alphabets. The different types of file format and extensions used are: -

1. Plain text (ASCII) files

.html/.htm: For viewing this file type, a web browser such as Navigator or Internet

explorer is necessary.

.txt: These files can be viewed with the help of a word processor, such as MS-Word.

2. **Formatted documents**

.pdf: It is a portable document format that allows formatted documents to be transferred over the Internet, so that its visual effects will be uniform at all the terminals. It requires Adobe Acrobat Reader to view the file.

.ps: It is a post script file. Although a simple text file, it is readable only with postscript printer or ghost script-a on screen viewer, which is available in Mac, Windows and UNIX operating systems.

3. **Compressed and encoded files**

.arc: It is an inefficient format of file compression, and is used mostly for viewing old files on new machine or vice versa.

.exe: It is a DOS or Windows based 'self-extracting' files.

.hex: It is a Macintosh based binary file that is converted into ASCII text, so that it can be sent safely over the network.

.sit: It is a Macintosh file format that is compressed using the Stuffit program. In order to decompress the file, a program called the Stuffit deluxe is used.

.tar/.tar.gz/.tar.z/.tgz: Tar is an acronym for Tape Archive. It can archive files, but cannot compress them. So .tar files are often gzipped, and have the extension .tar.gz.

.zip: It is a commonly used compression file format for DOS and Windows. These files can be decompressed on a PC with WinZIP. Stuffit expander can also be used for Macintosh or Windows OS.

4. **Graphic files**

.gif: It stands for Graphic Interchange Format(GIF), and is the most popular graphic file format on the Internet. On Macintosh machines a shareware utility called GIF converter can be used to view and modify GIFs.

.jpg/.jpeg/.jif: Joint Photographic Experts Group (JPEG) is used for photographs and still images. The JPEG viewer is essential to view these files.

5. **Sound files:**

.mp3: It is a commonly used compressed file format for distribution of CDs. A 1MB file is almost equivalent to one-minute music. An MP3 player is required to listen to such files.

.ra: It stands for Real Audio(RA), developed by Real Networks. It allows us to listen to sound in real-time. To listen to such files, a player is required.

Other file formats used for compressing sound are .au/uLaw/MuLaw, .aff, and .wav.

6. **Video files:**

.avi: It is a standard video format for Windows- AVI video for Windows player or Windows media player for Microsoft.

.mov/.movie: It is used for quick time movies on Macintosh platform. It requires sparkle or movie player to run on Macintosh OS.

Other video file formats are .mpg/.mpeg, .qt, .ram.

Answer: [b] .pdf

Module:7

Reference No:M7047

Question: The analysis of project requirements supporting the organisation activities is done in which stage of Software Development Life Cycle (SDLC)

[a] Feasibility study

[b] Business Requirement Specifications

[c] Functional specifications

[d] Design Specifications

Module 7- Software Development Life Cycle (SDLC)

This is the first part of SDLC and here we will be dealing with four phases of SDLC i.e.

Initiation phase

Feasibility study

Business Requirement Specifications

Functional specifications

Software Development Life Cycle (SDLC)

A software development life cycle is the process by which systems are conceived, designed, implemented, and maintained. The process contains all of the necessary activities for software development. It describes how the development is managed and gives the context in which all work is done. A method defines how to undertake one or more activities of the software development life cycle and defines the inputs and outputs of those activities.

SDLC is divided into different phases for convenient. They are: -

1. Initiation phase

It is the first phase of SDLC and it involves preliminary requirements from user. Initial delivery of the system depends upon the type of request and participation of the user in determining the functional specifications of the system. Effective communication is necessary between user and system development team. Some points which determine the type of development and user requirements are:

- **Project objective**

- **Maintenance**

- The company takes user request for maintenance of software. It may be some specific changes in software product that involves specification of technical and Business requirements.

- **New system development and enhancement**

- Here the outline of business requirements in terms of its functionality should be defined. The designing will provide system specifications but actual level of information depends upon communication between user and the person who is going to do feasibility study.

- **User of the system**

- A user should define how he/she is using the system and for what purpose.

- **Criticality time constraint**

- All information regarding objective of the project, time limit in which the project is to be completed and cost/benefit analysis is to be done. These are primary requirements for feasibility study.

2. Feasibility Study

After initial phase the second stage is that of feasibility study in a System Development Life Cycle. It is done for the approval of software request for development. Feasibility study also determines the path that should be followed in developing the user's request. It is not necessary to do feasibility study for all type of software development; it is required only for new system development and for the projects that require major enhancements.

3. Business Requirement Specifications

Once the feasibility study is completed, the next phase is determining business requirement

specifications. These specifications are developed to ensure that the project requirements support the business activities. User develops business requirements specifications but it needs an effort from application development group to ensure that all business objectives are meeting requirements of user request.

4. Functional specifications

Next phase in SDLC is determining functional specifications. It is analysed from user perspective and involves analysis of business requirements to form a primary design of the system. For maintenance or enhancement of the system, functional team can make use of existing input, screens and reports. The only need is to identify what all are the changes to make. The components involved in functional specification are: -

- Data Flow Diagrams: It represents the graphical representation of business functions. it involves tracing the data from all the business activities and processes.
- Screen definition: It involves defining input fields (description and purpose for input) and range checks (the range of values that the field can hold).
- Data definition: It gives information regarding data relationship i.e. how data from different sources are related among themselves.
- Inputs: It tells about sources of input (disk, floppy, etc.) and type of data (transaction or master file) to be stores.
- Output and report definition: In this details regarding data stored in the reports are defined and the usage of these reports by the user.
- Capacity requirements: It gives us information about capacity of the system like what amount of transactional data a system can hold or is the system is capable enough to accommodate additional data in case, the company shows positive growth.
- Conversion requirement: It involves converting data from one system to another like re-typing, making use of conversion programs.
- Control and security requirement: In a system edit requirements for input control should be there and audit trials for data, from the time it is entered to the final storage should be maintained.
- Backups, restart and recovery requirements: It shows the requirement regarding how frequent the data is needed for backup and what are the backup devices (hardware) we are using.

Answer: [b] Business Requirement Specifications

Module:7

Reference No:M7048

Question: At which stage of Software Development Life Cycle (SDLC) the program development work is completed:

- [a] Design specifications
- [b] Program specifications
- [c] System testing
- [d] Unit testing

Module 7- Software Development Life Cycle (SDLC)

This is the second part of SDLC and here we will be dealing with next four phases of SDLC

Design specifications
Program specifications
Unit testing
System testing

Software Development Life Cycle (SDLC)

A software development life cycle is the process by which systems are conceived, designed, implemented, and maintained. The process contains all of the necessary activities for software development. It describes how the development is managed and gives the context in which all work is done. A method defines how to undertake one or more activities of the software development life cycle and defines the inputs and outputs of those activities.

All the activities involved in life cycle of software development process are concerned with putting user needs into the software product. In order to manage the whole life cycle, it is divided into different phases.

1. Design Specifications

Once functional specifications are met, then come the design specifications in development cycle. It first identifies the functional components of the system and based on that it determines the design of the proposed system. The application development group develops design specifications. In design phase the functional specifications are updated and reviewed by user. The components involved in design specifications are: -

- **Database requirements:** It tells the relationship between the data elements i.e. one to one, one to many, many to one or many to many.
- **File requirements:** The detail description of each file are required such as what type of information the file holds, methods to access that file, the fields used in that file (name, address, company, etc.), data attributes (numeric, alphanumeric or character) of the file and number of records in a file.
- **System flow diagrams:** These are sequential flow of program that are executed along with their relationship to input and output. This information can be represented using Computer Aided Software Engineering (CASE) tools, flowcharts, Data Flow Diagrams (DFD) etc.
- **Program requirements:** It tells what program is used for the system and the purpose of the same like update, edit or extract data. It also explains how the program works when related to other program.
- **System operations requirements:** It includes backup and recovery procedures, system start up and shutdown procedures for the applications. The operational deadlines like input/output deadlines and job processing deadlines are to be met on time.
- **Screen design:** It will explain how screen is triggered by execution of some event and all the checks on data input are performed. If some error message is displayed then description of the same should be explained.
- **Report design:** It ensures that data is filled in each field of the report.

2. Program specifications

It involves description of programming logic and processing requirements that are used to meet the requirements of software request from the user. It is developed as a part of construction phase even before the commencement of programming. It assist programmer in determining the steps involved in coding a program. Programming specifications are needed to determine only for big projects.

3. **Unit testing**

After the program specifications are once completed, the testing phase of the programs starts.

A program is divided into different modules for convenience. Unit testing is used to test the working of individual module of a program. It does not tell how the program performs when all the modules are integrated to form the entire application.

4. **System testing** After the unit testing is over, the development process enters system-testing phase. At this phase all the program development work for the request is over. The programmer performs all necessary tests to ensure the functionality of the program. it ensures that the requirements of integrated software system as a whole are met and gives expected and predictable results. The example for system testing is configuration oriented system integration test.

Answer: [c] System testing

Module:7

Reference No:M7049

Question: User acceptance testing (UAT)

- [a] Is done during conceptualisation of the product to analyse end-user likeness towards product
- [b] Is the final phase of validation and ensures that the system meets the requirements of the user
- [c] Is done after designing, but before in-house testing
- [d] Involves testing a prototype

Module 7- User acceptance testing

Introduction: Software testing plays a very important role in determining the quality of the software. Software testing helps in identifying faults (errors) in a program. It also traces the cause of the problem; thereby reducing the number of errors. Different types of errors can occur in systems and programs, which need to be recognised and removed, in order to improve the performance of software

User acceptance testing: This is the final phase of validation. User acceptance testing ensures that the system meets the requirements of the end-user. It also gives the user the assurance that the software will be easy to use. .

Components of user acceptance technique

1. **Planning and documenting user acceptance criteria:** In this phase, the criteria for testing is considered and documented. The criteria can be changed, based on the changes made to software and the document update. Criteria and requirements should be prioritised to minimise risk.
2. **Setting up and maintaining the UAT environment:** For a successful testing process, there should be a favourable UAT environment. If the complexity of the environment is underestimated, it may hamper the testing process.
3. **Designing a user acceptance test:** Different techniques are used to design acceptance tests. The white and black box is one such technique. This makes acceptance tests work more effectively and efficiently.
4. **UAT tools:** There are different types of tools, which support UAT and ensure its correctness throughout the entire process. Many problems can arise in an automated testing

process. Therefore one should strike a balance between automated and manual testing processes.

Setting up a UAT team

For better results in testing of software, there should be a testing team that works cohesively. To achieve this, the following should be taken into account:

1. **The test profile:** A questionnaire is prepared for testing the software program. In a UAT team, each person may have a different approach and may possess different abilities to test the process. The strengths of each person should be assessed to improve teamwork.
2. **Building a strong UAT team:** For a strong testing team, team members should have: -
 - Commitment towards work.
 - Proper co-ordination to achieve goals.
 - Mutual trust

Monitoring the UAT process

1. **Monitoring and control:** The software testing process should be monitored on a regular basis and appropriate action should be taken if there is a diversion from normal process.
2. **Assessing risk:** Risk assessment is a continuous process and should be given due importance at the time of user acceptance testing. Risk is analysed both at the initial stage of the testing and at the end .
3. **Documenting UAT reports:** To prepare a good document, all the relevant information regarding the software and end user are essential inputs. Reports on UAT are included as a part of the document.
4. **Fault tracking:** In a testing process, an effective fault tracing system is installed to minimise the probability of errors in the final process. The pitfalls of the system should not be ignored.

Measuring the value of UAT

1. **Measuring test effectiveness:** Measuring the quality of the software testing process enables us to predict future testing efforts and corrective maintenance required for the process. Measuring errors during and after a UAT can be done when changes are made in the testing process.
2. **Measuring test efficiency:** Efficiency of a testing process is measured in terms of time and budget. The testing process should be completed within an optimum time and budget. Two measures used for better efficiency are: -
 - Defect-based measures
 - Confidence-based measures
3. **Post project reviews:** After the successfully completing a testing process, the project should be reviewed continuously.

Answer: [b] Is the final phase of validation and ensures that the system meets the requirements of the end-user

Module:7

Reference No:M7050

Question: The process of visualising the design of a project that is yet to take shape is called:

- [a] Data abstraction
- [b] Data modelling
- [c] Data transparency
- [d] Data designing

Module 7- Data Modelling

A Model

A model is a graphic or symbolic representation of a big project, real or imaginary. Similarly, the data model helps us to visualise the data structure, and analyse the completeness and accuracy of the information system. A designer can improve the design before it is implemented on a project, but equally important is the model's ability to represent the design of the system. Details that are not relevant should be eliminated. A large amount of data should be substituted by symbolic format in a data model.

So, in essence a data model should be simple and small copy of the final structure that makes use of words, pictures, symbols, and the like. The concept of Data Modelling is to continuously improve with the evolution of new tools and techniques.

Data Modelling

The main objective of Data Modelling is to develop an accurate model or graphical representation of client's information needs and business processes. It acts as a framework for developing new applications. As business requirements change with the passage of time, so should modifications be made to the system? At this juncture, data modelling encourages both the developer and the client to make the required changes.

Benefits

1. **Abstraction:** It represents the minimum and universal set of properties of an application /information system i.e. the visualisation of a whole project in the form of symbols, graphics and the like. A well- designed model will be economic and flexible, because it uses few symbols and graphics to represent a large design. A standard design which is used for large classes of situations will eliminate:

- Recoding
- Repetitive work
- Human error

Strong methodologies and tools of data modelling provide several techniques that support abstraction

2. **Transparency:** A good data model must provide a clear picture of the project. The designer must convert complex ideas into simple -to -understand format. A data model is not merely a single diagram. To ensure transparency it should take into several dimensions and views like:

-

- Designing according to functional area and by related data structure
- Listing data structure by type and grouping
- Exploring details with symbols
- Considering data based queries, which describe the model.

3. **Effectiveness:** An effective data model is one, which is accurate, reliable and cost-effective. The tools and techniques that are used should capture not only the conceptual

design, but also translate it into workable physical database design. Issues that were skipped at conceptual level must be implemented at the physical level. These issues involve: -

- Reducing time to update
- Simplifying access views
- Enforcing referential integrity

4. **Durability:** A data model should be durable i.e. the system should be able to take care of all the unanticipated processing requirements for the long-term. In case of any new business requirement, the system should be flexible to accommodate it.

Answer: [b] Data modeling

Module:7

Reference No:M7051

Question: Which of the following is true:

- [a] Workbenches are team based
- [b] Software Engineering Environments cannot include design and documentation
- [c] In an integrated environment the project documents are stored in different places
- [d] Software developed could be delivered for target system with a completely different architecture and operating system

Module 7- Software Engineering Environments

Software Engineering Environments (SEE) can be defined as a set of hardware and software tools, which when combined, act in an integrated way to give support for the whole software process from initial specification to testing and system delivery.

"Environment" here depicts a wide range of support systems ranging from simple systems supporting program development in a single language to very large systems supporting multiple projects using many different languages and design methods.

Characteristics distinguishing SEE with CASE workbenches

- Integration of all the five levels viz., platform integration, data integration, presentation integration, control integration and process integration.
- Unlike workbenches, which are based on individual development of tools, the SEE is team based and provides configuration management support for all activities.
- SEE supports a wide range of software development activities whereby it could include workbenches supporting specification, design, documentation, programming, testing, debugging and the like.

Integrated Environment

To support integration, SEEs use a shared repository of project information. Tools are interfaced through this repository and exchange of information takes place through it. Output of one tool can become input for another. The SEE solves the major problem in CASE workbenches, which is combination of different tools for exchange of information. Interaction of tools although very obvious, at times can occur unexpectedly. The repository can allow such combinations whenever required.

Since all the project documents are stored in one place and links between these documents are

managed automatically, the configuration management costs is reduced in SEE. SEE also accommodates a range of CASE tools and workbenches to support different projects. For this purpose SEE can be considered as a set of services used by facilities providing end user support. The services are given in a three-layer model.

Workbench applications
Framework application
Platform services

Layered model of a software engineering environment

Platform Services

Host-system is the platform on which the SEE runs. Although software developed on a platform is generally installed and operated on the same, there are chances that the software being developed is delivered for a different platform with a completely different architecture and operating system. Therefore host-target system development should be done. This is supported by the following reasons:

- The software under development may be for a machine with no software development facilities, which is possible in the case of real-time systems for special purpose computers.
- The target machine is application-oriented and is not suitable for SEE.
- The target machine is already in use and dedicated to a particular application, which requires priority over software development.

Framework Services

Framework services are implemented using platform services and are extended set of services provided by the environment host. The Framework services are given by reference model for SEE and support five different forms of integration.

- Data repository services: It facilitates storage and management of data items and their relationships.
- Data integration services: They facilitate managing groups or configurations of data items, supporting the naming configurations and establishment of relationships between them.
- Task Management Services: It facilitates definition and enactment of process models supporting process integration.
- Message services: Facilitates tool-tool, environment-tool and environment -environment communications supporting control integration.
- User interfaces services: Facilitates user interface development, supporting presentation integration.

Answer: [c] In an integrated environment the project documents are stored in different places.

Module:7

Reference No:M7052

Question: Which of the following is false with regard to software engineering metrics?

[a] It helps in decision-making

[b] It does not involve activities like designing, analysis and coding

- [c] It involves measuring productivity of individual designer
- [d] Metrics could be of no use or harmful due to wrong analysis

Module 7- Software Engineering Metrics

The primary focus of any organisation is to produce high quality product within schedule and budget. In order to evolve and grow successfully, there has to be continuous improvement in its quality of products and services. A measurement programme is required in order to understand the evolution of the software. Measurement is the only way through which one can understand and quantify a set of characteristics about a certain environment or software development in this case. Metrics are the units of measurement, which aid in quantifying the various activities involving software engineering. "Metrics" also refer to a set of specific measurements for a particular item or process.

Software engineering metrics are used to measure the products, processes and people of their efficiency. A few examples are as follows.

- Software engineering products such as designs, source code, and test cases
- Software engineering processes like the activities of analysis, designing, and coding, and
- Software engineering people such as the efficiency of an individual tester, or the productivity of an individual designer.

Effective usage of software engineering metrics permits lots of benefits.

1. It quantitatively characterises success and failure, and/or the degree of success or failure of a product, a process or a person.
2. It helps in identifying and quantifying improvement, lack of improvement or degradation in products, process or people.
3. It aids in significant and constructive managerial and technical decisions.
4. It assists in keeping track of the software engineering project.
5. It helps in building calculated and meaningful approximations

Common Trends In Software Engineering Metrics

- Software Engineering Metric, only by itself is not of much use. Three or more metrics are chosen carefully with respect to the process, product or people. Metrics above five generally do not provide a considerable return.
- A large number of different metrics have to be used when a particular software project or any characteristic of software engineering is being studied. After a considerable analysis the most practical set of metrics required by process, product or a given person are adopted.
- Software engineering Metrics are interconnected and therefore when one metric is tried to manipulate it directly makes its impact on other metrics.
- To make the most out of metrics, they should be assembled methodically and frequently in an automated manner.
- To be functional, Metrics must be synchronised with reality even before meaningful decisions, based on the metrics, are made.
- Metrics could be useless or even harmful due to wrong analysis.
- Contrasts and similarities of people, processes or products should be known to obtain significant metrics-based comparisons.

Answer: [b] It does not involve activities like designing, analysis and coding.

Question: Which of the following statements is true with regard to Computer Aided Software Engineering (CASE) workbench?

- [a] A single CASE tool is more effective when used individually than when combined with more than two
- [b] It is very difficult to add a new case workbench or replace an existing one
- [c] An organisation has to depend on a single supplier
- [d] Workbench can be easily managed with the aid of the configuration management system

Module 7- Computer Aided Software Engineering (CASE) workbench

CASE workbench is a set of tools, which are used to support a particular phase or activity of software process like specification, design, implementation, testing and the like. The workbench is of great importance because a set of CASE tools can provide comprehensive support when compared to a single case tool. Workbench can then be integrated either through shared files, a shared repository or shared data structures.

Although case workbenches support most software process activities, it better supports activities such as analysis and design, programming and program testing, which are widely used in the industry. Depending on the type of software developed and the application domain, different types of workbenches are used.

Typical Components of the CASE workbench

- **Diagram Editing System:** The diagram editing system is used for creating data-flow diagrams, structure charts, entity-relationship diagrams and the like. The editor captures different entities in the diagram and saves this information in a central repository.
- **Design Analysis and checking facilities:** It processes the design and reports on errors and anomalies. These are integrated with the editing system so that the user is informed of errors during the creation of the diagram.
- **Query Language:** It enables the user to browse stored information and examine completed designs.
- **Data dictionary:** It facilitates maintenance of information about the known entities used in a system design.
- **Report Generation:** It retrieves information from the central store and automatically generates system documentation.
- **Form generation tools:** They enable users to screen and document specified formats.
- **Import/Export facilities:** They allow exchange of information from the central repository with other development tools.

Case workbenches are intended to support software process phases such as system design or a set of interrelated software process activities, which could vary from one application domain to another or even organisation wise. This requires the CASE workbenches to be open systems.

An open workbench can be defined as a system where control integration mechanisms can either be provided or programmed. The data integration protocols are public and not proprietary. The majority of data systems rely on file based integration strategy since standards for data integration are not accepted widely.

Advantages of open workbenches

- It is easy to add new specialist tools or replace already existing ones.
- Since the output of tools is files, they can be easily managed by configuration management system.
- A step-by-step process of workbench introduction and evolution are possible. More powerful tools can replace the initial tools as the demand increases.
- Organisations need not depend on a single workbench supplier and can independently buy tools from different vendors.

Closed workbench systems are those where integration protocols are proprietary to the workbench vendor. Closed workbenches allow much tighter data, presentation and control integration and can appear to the user as a unified whole rather than as a toolbox of different tools. Third party tools can be introduced in a closed workbench.

More recently, new standards are being developed where open workbenches are created with tighter integration between workbench components.

Answer: [d] They can be easily managed by configuration management system.

Module:7

Reference No:M7054

Question: The Commercial Off-The-Shelf software is

- [a] Bought on commercial basis and can be given on rent or lease
- [b] Controlled by the integrator and the customer
- [c] Installed at only one place after it is available commercially
- [d] Maintained and controlled by original developer only

Module 7- Commercial Off-The-Shelf (COTS)

For a single organisation it is tedious to completely build, install, and maintain every bit of software for even a reasonably complicated computer based system. In order to implement large, complex, reliable software systems in a cost effective manner, a software system is built predominantly by bringing together large-scale components acquired from third parties. Such a software system is called Commercial Off-The-Shelf (COTS).

There are many reasons why software organisations opt for COTS, time and money being the most important ones. There are different issues, which emanate when building or purchasing COTS software as it is akin to a black box wherein there is a possibility of architectural mismatch and a different architectural approach to reduce the evolutionary cycle time.

A system, which is built mainly by integrating a group of COTS software, is COTS based software system. To build COTS based software system the integrator buys the components from a third party and assembles them into a complete system. Therefore, only little amount of coding process is required, as most of the components are bought off-the-shelf. The coding, if at all required, is for customising the COTS software, construct the software components that are not being supplied by the commercial sources or for binding the various COTS components together.

Properties of COTS Software

1. It is obtained from the distributor and incorporated without any changes in the source code: The true rewards of COTS software can be obtained only when they are incorporated without any changes in the source code unless it is absolutely necessary to have few changes for customising. But a point to be noticed here is once the changes are incorporated, it is no longer an off-the-shelf (OTS) software.
2. The original developers of components may sometimes take care of customising provided they do not effect the source codes such as plug-ins, scripting and inheritance. Installed in multiple sites within various organisations: Different organisations could be using the similar copies of software, as it is off-the-shelf. And also no single organisation has complete control over the evolution of software.
3. Control of evolution and Maintenance of Software is not under control of users and /or integrators: The evolution and maintenance of COTS is the responsibility of original developers of the software. It acts as a mere commercial organisation for supporting customers, who do not have control over the evolution of software. The COTS based systems are classified into two types.
 1. COTS intensive System: In this system, a number of COTS components are gathered from different sources and are then bonded together as one complete system. No single COTS component dominates over others and is responsibility of the developer to define an architecture that integrates the various components. For example, a command and control system constructed from a client / server GUI system, a set of databases, data analysis tools and the like.
 2. COTS Solution System: Here, a single COTS application makes available a primary solution to the problem. This single application describes the architecture and requirements of the system. If at all other COTS components already exist, they are add-ons and plug-ins to the main application. For example, Turnkey financial applications.

Answer: [d] Maintained and controlled by original developer only.

Module:7

Reference No:M7055

Question: Which of the following is not true with regard to Commercial Off-The-Shelf (COTS) systems:

- [a] Commercial Off-The-Shelf are highly secured
- [b] The cost of developing Commercial Off-The-Shelf is very high
- [c] There is no possibility of mismatch between Commercial Off-The-Shelf components
- [d] The component user has little or no control over the evolution of component

Module 7- Benefits and Risks Commercial Off-The-Shelf (COTS) based systems

The COTS based systems provide many benefits when compared to customised components. They are as follows:

1. The most important factor is economies concerned with the development cost. The COTS based components come cheaper when compared to customised components as the cost is spread over many customers.

2. COTS components, which are present in the market for a long time, are always better than a custom built components since they are regularly improved, better designed, and are more reliable.
3. Cost of training the personnel is reduced when using a single COTS component in different applications.
4. An organisation that creates custom built software is very slow in incorporating new technologies and new standards into the products when compared to the commercial product developer.

Risks of COTS based systems

The COTS based systems are however not free of risks.

1. Access to source code: Since the developers do not have access to source code the functionality of the component cannot be changed when desired. Analysis, testing and the like have to be done in a black box [1] manner.
2. Control over the evolution of the system: The COTS components are integrated into a software system by the system developer. But the developer has no control over the evolution of the component. This means
 - (a) Update of each component may not be as desired by the developer
 - (b) It may not be portable [2] with the platform the user requires.
 - (c) It could intervene with the operation of some required functionality.
 - (d) It may not interact in a similar way with other components.
 Complete and correct behavioural specifications may not be available: The vendor specifications for COTS components may not be correct or complete. The functional description may not always be in line with that of the integrator who requires a through knowledge of COTS components as there is a probability of hidden behaviour [3] and bugs affecting the system.
3. Mismatch between COTS components: There could be a possible mismatch among the COTS components due to data model, functional mismatch, resource clash, or process model used. The mismatch could cost heavily when not found until the late development process.
4. Inability to interconnect with other components: Since most of the COTS components are intended to be standalone applications they may not interact with other COTS components and developmental software with ease. For example, the COTS components may not have integration mechanisms, such as exporting interfaces or published database formats. And even if the software is designed with the intention of integration it may not execute the functionality as required by the integrators.
5. Frequent Updates to commercial products: Since commercial products are regularly updated and distributed by the developers, they have to be regularly incorporated to obtain the desired functionality. Replacing a component with an upgraded version is a laborious task and requires the component and the system to be retested.
6. Security: The COTS systems do not have any level of security.

[1] Black Box Testing does not require knowledge of internal working of the item being tested. The tester is only expected to be aware of the correct type of inputs and what the expected output is. He has no knowledge as to how the output has been arrived at.

[2] Portable: Manageable

[3] Hidden Behaviour: Function, which is otherwise not active.

Answer: [d] The component user has little or no control over the evolution of component.

Module:7
Reference No:M7056

Question: With regards to systems development, hardware and software studies are performed in:

- [a] System analysis phase
- [b] System design phase
- [c] System implementation phase
- [d] None of the above

Module 7- Life Cycle of an Information System

The concept of the life cycle of a system is central to systems investigation. Every system moves through several phases of a life cycle during its development, after which it functions only with minor maintenance. The system gradually deteriorates to the point where it ceases to function effectively and a new life cycle begins with the development of a new system.

The life cycle concept is related to another important concept that deals with the professionals that run the show of systems management. System development has many phases. A team is formed at the time of preliminary investigation of the system. The team is likely to be expanded in the analysis phase and further more in the design phase. As each team member completes assigned responsibilities, he is either assigned additional responsibilities or is assigned to another system investigation. Thus we see that the project teams are dynamic and there is a continuous cycle of professional systems personnel which effects the life cycle of a system as a whole.

Let us now see the different phases of a system life cycle:

- **Preliminary study phase:** During this phase, a problem with an existing information system or an opportunity to usefully develop a new system is discovered and a limited amount of initial investigation takes place.
- **System analysis phase:** During the analysis phase, a problem or opportunity associated with the system is identified, strengths and weaknesses of the old system are examined, and what the new system has to accomplish is determined.
- **System design phase:** During the design phase, a new system or computer application is designed to satisfy the needs that have been determined during the analysis phase. During this phase, both hardware studies and software systems design are completed.
- **Implementation phase:** This phase involves programming, equipment installation, and other activities related to implementing a newly designed system.
- **Systems maturity and maintenance phase:** This phase involves continuous operation of the system after installation. Usually, the system achieves peak performance and then its cost effectiveness gradually declines as its environment changes. When it nears the end of this phase, the system is deemed to be no longer performing satisfactorily and is replaced.

Because activities of the various phases typically overlap, they may not be readily distinguishable from each other. For example, personnel training is a part of the implementation phase, but the lead time for training personnel to accept and use certain types of systems is lengthy and this activity often begins long before the system design is complete. Despite this, it is useful to understand and distinguish between the different stages as this facilitates better understanding of the system.

Answer: [b] System design phase

Question: During which of the following stages is user resistance encountered in Computer Aided Software Engineering (CASE) Life Cycle ?

- [a] Procurement
- [b] Evolution
- [c] Case system Introduction
- [d] Obsolescence

Module 7- Computer Aided Software Engineering (CASE) Life Cycle

The CASE tools are an expensive application to introduce and implement, and therefore require judicious planning. Adequate resources should be devoted for the procurement and support of these tools, to reap the total benefits. CASE should be maintained until the entire software, which was built using them becomes obsolete.

The case systems used in an organisation have different stages in its life cycle.

1. **Procurement:** The procurement stage involves selecting an appropriate CASE system depending on the type of software being developed. Most of the CASE systems are analysis and design workbenches (CASE workbenches are a set of tools, which are used to support a particular phase or activity of software process like specification, design, implementation, testing and the like.). The following factors are considered before procuring.
 - The system supports existing practices instead of starting new methods and standards, which could be opposed by the users.
 - Before buying case tools it should be verified whether the present hardware is in accordance with the industry standards and can be used for a long time after procurement.
 - Adequate security features should be available in the system such as access permissions and the like.
2. **CASE system tailoring:** A case system is adapted to a certain set of organisational or project requirements. Since Case systems are general-purpose tools they must be customised to conform to the specific standards and working practices of the organisation. The actions required for customisation are:
 - **Installation:** The case system should be installed and tested to confirm the hardware configuration. This could involve changing system dependent parameters.
 - **Process model definition:** When the case system is not process driven, any process model can be used to determine the type of system tailoring required. This allows the CASE manager to know where the tools can be applied and the interfaces required to connect to other tools.
 - **Tool Integration:** Case systems should be properly integrated with other installed case tools. This could involve identifying all the entities and relationships, which are required for an organisation's development process.
 - **Documentation**

3. **CASE System Introduction:** Introducing a CASE system would mean changing work patterns. Therefore, the full benefit of using the incorporated tools cannot be obtained until they are effectively used. Problems that arise due to the introduction of a CASE system are:
 - User Resistance: The user could resist case tools. This could be because of its regulatory nature and that it gives more control to the management.
 - Lack of training: Lack of formal training could make the employee think that the tools are very difficult to understand and use.
 - Management Resistance: Initially, some managers may find it difficult to accept CASE tools as they are responsible for cost control and the usage of these tools cannot be quantified.
4. **Operation:** Case system is commonly used for software development. Project managers should be actively involved in organisational decisions with the procurement of case tools. Costs involved are carefully assessed and experiences of project engineers and managers are carefully documented.
5. **Evolution:** To be useful, the case systems cannot remain static and must evolve continuously as new requirements become clearly visible and new hardware and software become available. The input output formats could be changed and new methods of tools developed. At this juncture, it is possible that either the hardware or the software becomes incompatible. In such a situation, the old hardware systems should be maintained to support the software systems and a heterogeneous network system with different machines having different operating systems.
6. **Obsolescence:** Case systems cannot be merely termed obsolete due to lack of support provided by the vendor or due to other decisions to change hardware or software. Instead, a transition phase should be planned where both the old and new systems are in use during, which period the old system should be completely keyed into the new system.

Answer: [c] Case system Introduction

Module:7

Reference No:M7059

Question: What is the cross-reference in the workbench used for?

- [a] Producing a cross-reference listing, indicating where all the program names are declared and used
- [b] Loading the executable program into the computer memory prior to execution
- [c] Processing the design and reporting on errors and anomalies
- [d] Controlling the execution sequence and viewing the program state as execution progresses

Module 7- Types of Workbenches I

1. Programming Workbench

The programming workbench is built on a set of tools, which support the process of program development. The programming workbench was the first among CASE systems dedicated to program development. The central components of a programming workbench are assemblers and compilers, which translate higher-level programming languages into machine code whereas the syntactic and

semantic information generated from a source programming during compilation, may be used by other tools. CASE tools are represented as round edged boxes and tool inputs and outputs are represented as rectangles.

Tools, which form a part of programming workbench are:

- **Language Compiler:** It translates source programs into object code.
- **Structured Editor:** It Integrates embedded programming language and edits the syntactic representation of the program.
- **Linker:** It links the object code program with components, which have already been complied.
- **Loader:** It loads the executable program into the computer memory prior to execution.
- **Cross-referencer:** It produces a cross-reference listing, indicating where all the program names are declared and used.
- **Interactive Debugger:** It helps the user to control the execution sequence and view the program state as execution progresses.

Program workbenches can be implemented as a collection of tools running under a general-purpose operating system like Unix. Programming workbenches are available for personal computers but are sold as language compilers with additional support. Examples of such programming workbenches are C, C++, Pascal and the like.

2. Analysis and Design Workbenches

Analysis and design workbenches are designed to support the analysis and design stages of the software process where models of the system are created. For example, the data-flow model and entity-relation model, and the like. They are graphic oriented((can you say so?)) and are otherwise known as upper-CASE tools. These are closed systems as they are typically integrated through a shared repository whose structure is proprietary to the workbench vendor.

Components of Analysis and Design Workbench

- **Diagram Editors:** These are used to create data-flow diagrams, structure charts, entity-relationship diagrams and the like. They not only serve as drawing tools but also capture information about different entities in the diagram and save it in the central repository.
- **Design analysis and checking tools:** These tools process the design and report on errors and anomalies. When integrated with the editing system, it traps the user errors at an early stage in the process.
- **Repository Query Languages:** These languages allow the designer to find designs and associated design information in the repository.

The Analysis and design workbenches are available for structured methods. Productivity improvements upto 40% may be achieved and the quality of the developed systems is improved with fewer errors and inconsistencies.

Difficulties in incorporating the Analysis and Design workbench

- Import and Export facilities are very limited.
- Customising and adapting a design is very difficult for certain application.
- They provide their own configuration management system, which is often incompatible with the system used in an organisation. This makes it difficult to export the system designs in a manageable form.

Answer: [a] Producing a cross-reference listing, indicating where all the program names are declared and used

Module:7

Reference No:M7060

Question: Which of the following socio-technical design principle is applicable to environmental guidelines?

- [a] Compatibility
- [b] Information flow
- [c] Boundary location
- [d] Support congruence

Module 7- Socio-technical design approach of system development process

Socio technical design involves integration of human resources in industrial setting i.e. importance of proper trade-off between technical and social system of an organisation. The technical system is concerned with the technical and economical aspects of the organisation while social system refers to social aspects in the functioning of the organisation. Human tasks are not determined according to technologically change in an organisation. In such situation socio-technical approach should be implemented to re-design the organisation structure.

Socio-technical design principles

- **Compatibility:** The designing process itself should be compatible with the work and culture of the organisation.
- **Minimal critical specifications:** It tells of minimum necessary functionalities that should be incorporated into the design.
- **Variance control:** If the problem arises at any point of time, it should be solved as close to the source as possible.
- **Boundary location:** Boundaries should not be drawn in the development process, so as to avoid constraints in sharing of information, knowledge and learning.
- **Information flow:** Information should first go to the place (person, department) where it is required.
- **Power and authority:** People who use equipment, material and other resources in an organisation should have authority to access it, so that they do not have to rely on others to carry out their responsibilities.
- **The multifunctional principle:** According to change in organisation needs, it should be adaptive enough to carry out multiple functionalities.
- **Support congruence:** Design of social support (selection and training procedure, conflict resolution, work measurement etc.) should reinforce the desired culture of the organisation.
- **Transitional organisation:** Change is a matter of concern in an organisation, so design process should be visualised from that perspective.
- **Incompletion:** Designing is a never ending and iterative process.

Socio-technical design guidelines

Guidelines are categorised into three groups:

1. **Procedural guidelines:** It is useful for planning, scheduling and control systems. Socio-technical principles support the idea of "self-organisation" with the help of following design principles:
 - Compatibility
 - Minimal critical specifications
 - Transitional organisation
2. **Design guidelines:** This can evaluate the design of production control system by design hierarchy, organisation hierarchy, and information system and decision support tools. Following principles are applicable for the same:
 - Minimal critical specifications
 - Variance control
 - Boundary location
 - Information flow
 - Power and authority
 - Multi-functional principle
 - Incompletion.
3. **Environmental guidelines:** It contains guidelines for better synchronisation between design of a production control system and its environment. Only one socio-technical system is applicable to this viz. support congruence.

Problems

Main problems encountered in the implementation of the above guidelines are:

- Stress and anxiety
- Inadequacy
- System failure
- Lack of privacy
- Fear of unemployment
- Loss of responsibility
- Deterioration of self-image

Preventive measures

- Company should take preventive measures to resolve such problems.
- Ownership of the system is important
- Staff should have timely information on the future planning of the organisation
- Total staff involvement is necessary
- Job re-design should be done depending upon the requirement
- Health and safety of the organisation should be considered.

Listening to concerns

Answer: [d] Support congruence

Module:7

Reference No:M7061

Question: -Stress testing is mainly done to test the _____.

- (a) Feasibility of a program
- (b) Database reliability.
- (c) Website
- (d) Efficiency of hardware components.

Module 7- Stress Testing-Overview

A website should be tested thoroughly before it is launched in order to avoid failure due to unpredictable number of visitors. Load testing and stress testing are the most common tests used for this purpose. Load testing gives a rough idea of number of users a site can handle simultaneously, but it will not tell the reason of failure. Here comes the use of stress testing which determines the behaviour of website under stress and methods to recover the same.

Reasons of website failure

1. **Bandwidth limitation:** There are certain tools that assist in determining the total usage of bandwidth on a system. Sometimes it happens that demand for the website exceeds the available physical bandwidth. In such situation only two options are available: -
 - Put a constraint on number of and speed of connections.
 - Implement bigger pipes or increase number of pipes.
2. **Memory leaks:** Wastage of memory results to memory leakage. It is usually due to three reasons: -
 - Careless programming.
 - Poor written components
 - Old components in operating system.

If any component is leaking then it is very difficult to identify from where the memory is leaking.

3. **Resource locking:** Sometimes it happens that a database record, some file or graphics are not available to user for a longer period of time due to exclusive hold of an site component on it. Resource locking on application level shows quick effect but at operating system level its effect is generally not visible. Bad resource locking will cause a site to fail under heavy load. One should lock the resource only if needed and unlock it as quickly as possible. Good programming practices can avoid the usage of locks.
4. **Bottlenecks:** In hardware, software or any area in a system where data flow is hindered, it causes the whole process to hang.
In website programming such bottlenecks can arise anywhere in the system like web service, data service, auxiliary or statistics gathering service. For example a particular component of the system used for large amount of data manipulation, does not respond fast to the request, resulting slow processing of data.
In order to overcome these bottlenecks, the first thing is to find the source of the problem. If we are using most recent version of software component for website programming and it is not working properly, then some detective work is required like: -
 - Are the wrong parameters being passed?
 - The formatting of data and constraints are applied correctly or not.

- Are the components called in wrong context or with wrong credentials?
- The buffer length is sufficient enough to hold the data or not.

5. **Transactional problem:** Transaction involves interchange of information between the website and user. In the backend, processing and updating of data takes place in several distributed steps. For example a user submits details for his credit card at front end, than approval or rejection of request depends upon the completion of processing at all the sites in a distributed network. These activities occur at back end.
The drawback of transaction processing is that, how the system tackles the situation if the transaction is aborted or failed. It involves:

- Freeing up allocated memory to the transactional data.
- Disposing off the temporary database tables used for holding transactional data.

For smooth functioning of website, it is necessary to ensure that cleaning process and other related tasks are performed correctly.

Hardware limitations: Sometimes hardware specifications do not support the work, the user need to do. Changing servers and transferring data is both expensive and cumbersome. So, alternatively a sophisticated server should be installed with high scalability, additional processors, more memory, etc.

Answer: [c] Website

Module:7

Reference No:M7062

Question: The component of Management Information System (MIS) that assist in planning and decision making in a organisation is/are: -

- [a] Hardware
- [b] Software
- [c] Database
- [d] All of the above

Module 7 -Management Information System - MIS

Management Information System can be defined as a systematic or organised way of providing informational support to the managerial functions of an organisation. The system utilises computer hardware, software models and a database for analyses, planning and decision-making. In other words, MIS is an automated system, which presents information (both internal and external) to the business, which helps in making decisions. Thus, the purpose of MIS is to aid but not automate the decision making process.

Functions of MIS

The basic functions of an MIS are:

- **Collecting Data:** Collection of data is a critical part of the system. Data comes from both internal and external sources. Generally data is in human-readable or machine-readable form. The cost involved in collecting data using different kinds of devices has to be

considered. For example, large supermarkets use laser scanners at each billing counter. While machine-readable data is costlier, it saves considerable amount of time, which can otherwise be used productively.

- **Analysing and presenting data:** After data has been collected, it must be analysed and the information should be included in the reports. These reports give managers the information they need to make informed decisions. Hence the information must be up-to-date.

Need for an MIS

Designing, implementing and operating an MIS is both expensive and difficult. This effort and expenditure has to be justified. One factor is that the business environment today is much more complex because of government regulations that require organisations to undertake activities that were previously unnecessary. Managing this complexity requires sophisticated information systems.

The business environment is not only complex but also more dynamic. Managers have to make their decisions quickly and in such a way that there is very little time lapsed between the emergence of a problem and reaching of a satisfactory solution. An MIS that provides sophisticated and timely information is therefore a necessary part of the organisation.

Another factor that increases need for sophisticated information systems is related to Schools of Business and Management that have upgraded the quality of managers. Managers now understand and utilise more sophisticated management techniques than their predecessors. Managers today use marginal analysis and other similar techniques that require sophisticated information than what was previously needed.

Drawbacks of an MIS

A large number of managers are not happy with the computerised information system they are using. Let us take a look at the reasons behind this:

- Much of the information needed by senior managers is future-oriented or comes from outside the organisation. It is difficult to integrate this information into a structured Management Information System.
- Many managers do not understand information systems technology well enough to appreciate its potential or limitations. This lack of computer knowledge leads to a lack of trust in the computerised Management Information System.
- Systems analysts fail to understand the management processes or how managers' minds process data. Thus, the systems they build for managers are often unsatisfactory.

Answer: [d] All of the above

Module:7

Reference No:M7065

Question: What does predictive validity specify?

- [a] Quantitative score
- [b] Assessment model
- [c] Quality assurance
- [d] Relationship between process capability and performance

Module 7 - Software Process Assessment

It is found that software projects face problems in managing customer requirements, requirement specifications, procedures to control the changes to requirements, designs and documentation, tools for trace ability requirements and the like. In order to solve this problem various practices are implemented in software organisations to improve their productivity and operations. A frequently used model for strengthening software engineering practices is the "**Benchmarking Paradigm**". The benchmarking paradigm takes into consideration the best organisation or project and documents its practices. When implemented in an organisation or the project, which is less skilled or incompetent, it is assumed that the organisation or the project identified will give an excellent result. Practices of this sort are codified into an assessment model like the Software Capability Maturity Model or the International Standard Organisation (ISO) 15504, which is an international standard on **Software Process Assessment (SPA)**.

The SPA gives a quantitative score on assessing the performance of the organisation or project. This means that the organisation improves its performance according to the assessment model under consideration. This is referred to as **Predictive Validity** of the process capability score. Adopting better practices gives a better score and therefore SPA reflects the organisations or project implementation of best practices in the assessment model. The score also gives a level of implementation of best practices and gives information related to improvement of business and means of tracking improvement efforts. An SPA is therefore considered as a measurement tool and like any other measurement it should be validated before acceptance. Measurement score should provide some inferences and during validation, evidence is collected to support the inferences.

SPAs are done on the basis that resultant quantitative scores are associated with the performance of the project and /or organisation that is assessed. The Premise consists of two parts.

1. Practices defined in the Assessment model are good practices, which will give good performance on implementation.
2. Quantitative assessment score truly reflects the level of practices implemented in organisation or project; higher the score higher is the performance.

Predictive Validity study tests hypothesised model, which shows the relationship between process capability and performance that is dependent on context factors.

The hypothesised model is tested for different units of analysis. Some of them are as follows:

1. Life cycle process
2. The project, consisting of composite capabilities of multiple life cycle processes of a single project like Software Requirement Analysis and Design
3. The Organisation, which could be a mixture of capability of the same or multiple processes across different projects.

The size of the organisation can also act as an important factor. For example, small organisation would find quality assurance function and formal documentation of policies and procedures to be very costly. This means certain processes or procedures may not be cost effective for small organisations. The organisational size as a factor could give different predictive validity results for different sized organisations.

Answer: [d] Relationship between process capability and performance

Module:7

Reference No:M7065

Question: The of information design type used for navigational aids and graphs for geographical use is:

- [a] Pictogrammatic
- [b] Diagrammatic
- [c] Cartographic
- [d] Hybrid

Module 7 - Information design

Information design involves defining, planning and speculating the contents of a message, to satisfy the needs of the end user and thus achieve organisational objectives. The Information Designer is a professional who should be capable of providing and presenting the information to the user in the best way possible. This can be achieved by:

- Redefining the designer's job description.
- Feedback about his limitations.
- Awareness regarding the needs of the user.
- This is possible only by formulating better assumptions about users, developing design methodologies and acquiring a keen sense of historical information design.

Information design includes designing legal documents, business forms, diagrams, transportation maps, charts, tables etc.

Therefore, an information system should provide-

- Appropriate and clear communication.
- Thoughtful prioritisation.
- Identification of relations and interrelations
- Visual illustrations of nonverbal concepts

Categories of information design

These include functional vocabularies for different forms of information design. There are six basic categories in an information system:

1. **Alphanumeric:** The information design that is based on lettering, verbal and numerical information. Alphanumeric are generally used in letterform design, type design, form design, etc.
2. **Pictogrammatic:** It refers to information design that is based on nonverbal communication. For understanding the information, symbols are usually used. Other pictogrammic forms are pictorial symbols, glyphs, and pictograms.
3. **Product interface:** In this category, information is represented through words or symbols which are used in:
 - User product interface.
 - User interface.
4. **Diagrammatic:** This type of information design records and compiles accurate figures over a period of time. This data is structured on an X and Y-axis. Diagrammatic information design is applied in formulating graphs, tables, bar charts, pie charts and time lines.

5. **Spatial/Cartographies:** This type of information design is used to represent maps and graphic networks for geographical usage. Spatial/Cartographies are used for mapping, navigational aids and networks.
6. **Hybrid:** This is used to provide information, explanation or instruction to the user. It includes information design features from all other categories. Hybrid information design is used in training manuals, informational graphics, instructional graphics and how-to-use guides.

Components of information design

1. **Dot:** Is a small single point that is just about visible and represents the beginning of line.
2. **Line/rule:** Is a single stroke of pencil or computer mouse. Line is employed for communication and organisation.
3. **Shape:** It usually refers to boundaries, which create a particular shape. It may be combination of straight or curved lines.
4. **Spatial organisation system grid:** It involves organising elements of information design in a specific format. A grid can be conceptual i.e. matrix grid or physical i.e. unit grid. It can be regular, irregular or progressive in rhythm.
5. **Color:** Is a visual tool, which helps in better communication and exchange of information.
6. **Imagery:** It contains a symbolic representation conveying a certain meaning (like a photograph or symbol.)
7. **Sound:** It represents the power of pictures, which are being displayed. Therefore the sound should be clear and convey the meaning of the picture.
8. **Motion:** Motion is movement with respect to time. It can be manipulated to form a rhythmic flow. For this, either the visual image is animated or unanimated.
9. **Typography:** It involves type arrangement and type specification for preparing a particular type of application.

Answer: [c] Cartographic

Module:7

Reference No:M7066

Question: Which of the following is not a congestion management tool?

- [a] Priority queuing
- [b] Custom queuing
- [c] Network traffic queuing
- [d] Weighted fair queuing

Module 7 - Quality Of Service -Architecture

The basic Quality Of Service (QoS) has three main mechanisms for implementations. They are

- Identification and marking techniques
- Single network element
- Policy, management and accounting functions

The first mechanism, identification and marking techniques,, are used for ensuring the quality of service, provided by end-to-end linking network elements. The second mechanism, provides quality of service within a single network element; and the third mechanism provides quality of service in

policy, management, accounting functions to control and administer end-to-end traffic throughout a network.

QoS identification and marking techniques

QoS can be achieved in this area through classification and reservation.

Classification:

Traffic, which is given preferential treatment is classified by:

- Identifying services that require such treatment
- Marking/unmarking the flow of packets

The classification is done **per-hop**, when the packet identified is not marked..

QoS Within a Single Network Element

Congestion management, queue management, link efficiency, and shaping/policing tools ensures QoS within a single network element.

Congestion management: When there is a heavy traffic, which is more than the speed of a link, the router has to take a decision. It can decide to :

- Hold the traffic in a queue and then let the first packet in the queue be the first packet out.
- Place the packets into various queues, and service the queue depending on the priority.

These aspects are taken care of by **Congestion Management Tools**, such as Priority Queuing (PQ), Custom Queuing (CQ), Weighted Fair Queuing (WFQ).

Queue management: The queues may some times fill and overflow. In this case, additional packets cannot be accommodated, and are subsequently dropped. This is termed tail drop.

The router cannot prevent a packet from being tail dropped. This problem is effectively dealt with using two mechanisms:

1. Care is taken to ensure that the queue does not fill up, and therefore leaves enough room for high-priority packets.
2. Care is taken to ensure that packets of lower priority are dropped before higher-priority packets.

Both the above mechanisms are provided by Weighted Random Early Detect (WRED).

Link Efficiency: The QoS depends on links too. A link with a slow speed could affect the transmission of a small packet. For instance, if a voice packet is behind a large packet, there would be more delay in sending it . This problem is effectively dealt with link fragmentation and interleave, which allow this large packet to be segmented into smaller packets interleaving (interrupting) the voice packet.(check -techie aspect)

Traffic shaping and policing

Shaping generates the traffic flow, which limits the full bandwidth potential of flow therefore preventing the overflow. In a hub and spoke design, the central site and high bandwidth result in an overflow of data to the remote site. Shaping is the best way to resolve this problem.

Policing although similar to shaping, does not buffer the traffic, and exceeds the configured rate.

QoS Management

QoS management sets and evaluates related policies and goals in the following steps:

Step 1 It determines the traffic characteristics of the network.

Step 2 After identifying the traffic characteristics, it selects QoS techniques for the target application.

Step 3 It evaluates the response of the target applications to check whether the goals have been achieved.

Answer: [c] Network traffic queuing

Module:7

Reference No:M7067

Question: ----- is an activity performed in the pre-contract phase of a software acquisition project

- [a] Identification of alternatives
- [b] Testing and acceptance
- [c] Contract management
- [d] Preparation of the invitation document

Module 7 - Audit of risks involved in system acquisition Part 1 -overview

System acquisition is a very important activity in the development of information technology infrastructure in any company. This refers to any kind of information technology acquisition- hardware, software, networking or communications architecture. This could either involve actual acquisition, or it could imply the development of an information technology system. Audit of system acquisition has been dealt in this 5-part series. In the first part we have briefly introduced the various stages or phases involved in the system acquisition process. Audit of other important stages involved have been dealt with separately in the subsequent sections.

There are basically 3 phases in any acquisition project.

1. Pre-contract phase
2. Contract and award phase
3. Post- contract / contract management phase.

Pre-contract phase-This phase involves the activities performed before any contract can be considered for any system acquisition. The activities involved in the pre-contract phase are

- **Preparation of an acquisition plan** - This involves planning of a detail document which describes the approach to be followed by the organisation in a system acquisition project. This documents helps in the overall co-ordination of the project. For example it helps in ascertaining the project staff required for managing contracts etc.
- **Needs/requirement analysis** - Here the requirements of the users are identified and listed in a needs statement. Next, the user's requirements for the new information system are analysed and the functional needs of the users are listed in a requirements statement. Here the functional needs of the users can include issues like what is the information required, how it is to be obtained, what are the sources etc. And also support details like security measures, performance measures etc are listed.
- **Preparation of specification** - Based on a requirements analysis the technical specification statement is drawn up. The complete specification of the system i.e. new equipment,

software, support requirements, controls details, security, processing of the information etc is included.

- **Identify alternatives** - After the specifications have been drawn up, viable alternatives are identified and evaluated. Based on the risk analysis of each alternative and by using cost benefit techniques the best alternative is selected.

Contract and award Phase - The activities in this phase are-

- **Preparation of the invitation document** -this document contains all the details of the project and is the basis for vendors or contractors to submit their bids.
- **Evaluation of the various proposals and negotiations**
- **Awarding of the contract.**

Post contract /contract-management phase - The activities include

- **Contract management**-this includes monitoring the performance of the contract in order to ascertain if the deliverables of the contract are being met and if the contract is progressing as scheduled in the contract.
- **Test and acceptance**-this refers to the testing procedures adopted by the organisation in order to ensure that the contract deliverables are as per the contract and meet all the technical requirements. Testing procedures are identified in the pre-contract award phase. Users approve this in the specification statement stage and based on the performance parameters of the tests, the decision is taken to either accept or reject the deliverables of the project.

Index : Audit of System Acquisition

Part 1	Overview
Part 2	Acquisition project management
Part 3	Needs, requirements, specification
Part 4	Alternatives
Part 5	Contract management-test & acceptance

Answer: [a] Identification of alternatives

Module:7

Reference No:M7068

Question: ----- is an activity conducted in the last stages of the contract before accepting an information technology product

- [a] Benchmarking
- [b] Testing
- [c] Contract negotiation
- [d] Vendor evaluation

Module 7 - Audit of risks involved in system acquisition part 5 -contract management, test and acceptance

This is the last stage in a system acquisition project. The activities involved in this stage are

Contract management: This refers to the monitoring activities performed by the project head or the officer. This includes regular review of the performance of the vendor with regard to the terms and schedule of the contract. Also control of the changes if any, is mentioned in the terms of the contract so as to continuously reflect the users requirement. This activity also includes post implementation review of the contract to see if finally the information requirements of the organisation are met. Ineffective contract monitoring may lead to delay in completion of the project. The unauthorised and irrelevant changes of the contract may lead to risks of either an expensive system irrelevant to the functional needs of the users or an inadequate system that does not fulfill the requirements of the users.

Test and acceptance: This is the final activity of a system acquisition project. Based on the various tests performed the final product that is the information technology is accepted. Various types of testing techniques are available today. In the field of software development testing the tests that can be performed could be unit testing, regression testing, system testing and the like. Lack of well defined testing procedure and non-compliance of the same may result in accepting a system, which does not meet the standards and requirements of the organisation.

Audit Objective

- 1.The contract continues to meet the requirements of the organisation
- 2.The performance of the contract is being monitored
- 3.The modifications made to the change are valid.
4. Adequate testing measures are defined in the contract
- 5.The defined tests are being adhered to.

The audit tests have been given separately for each activity mentioned above.

Contract management

- 1.Check if the organisation has an effective mechanism to monitor the changes in the contract.
- 2.Check if the users and the management have approved the changes to the contract.
- 3.Check if the contract management policy of the organisation includes review of periodical costs reports and deliverables of the contractor.
- 4.Verify a sample of the reports submitted by the contractor to ensure that the management policy is being adhered to.
5. Check the adequacy of the implementation procedures followed by the contractor.

Testing and acceptance

- 1.Verify whether the contract documentation contains a comprehensive testing measures to be adhered to before accepting a contract. The details to be included are technical parameters, types of tests, functional specifications to be confirmed to, location where the test needs to be performed, resources required for testing and the like.
- 2.Check if there are adequate procedures in the company to verify the compliance of testing requirements.
- 3.Check if finally the user has acknowledged the successful operation of the system.

Verification of testing procedures may require additional technical knowledge. The auditing team needs to ensure that adequate technical expertise is available to certify the technical procedures.

Index : Audit of System Acquisition

Part 1	Overview
Part 2	Acquisition project management
Part 3	Needs, requirements, specification
Part 4	Alternatives
Part 5	Contract management-test & acceptance

Answer: [b] Testing

Module:7

Reference No:M7069

Question: Which of the following statement is true with regard to management of an acquisition project?

- [a] User involvement in the project is limited only to requirement analysis stage.
- [b] It is not necessary for the management to be involved in an acquisition project
- [c] The project team is a mix of people with technical, functional and contractual abilities.
- [d] Acquisition plan only specifies the details regarding the schedule for the contract awardance.

Module 7 - Audit of risks involved in system acquisition Part 2 - acquisition project management

The major components in the management of an acquisition project are

- 1.Involvement and approval of the users and the senior management
- 2.Project Staffing
- 3.Project monitoring through acquisition plan.

Involvement and approval of the users and the senior management-It is very vital that there is adequate involvement of the users and the senior management in a project management. Or else the project may face certain risk viz.,

- 1.Non-compliance with the organisation's overall business strategy
- 2.The project may suffer through inadequate funding
- 3.The project may not satisfy the user's need and may not be accepted by them.

Project Staffing-Improper staffing of the project may lead to a technical risk of not meeting the technical requirements of the company. Also lack of adequate acquisition skills of the staff involved in procurement may lead to a cost overrun and a delay in the project. The project team should consist of an appropriate mix of technical, functional and contractual abilities.

Project monitoring through acquisition plan- This plan is a tool for co-ordinating the activities and the personnel involved in the project. It is also a tool for monitoring the progress of the project. The main risk involved is that if the various activities to be performed in a contract are not clearly prescribed, the project may run into time delay risks.

Audit tests have been listed separately for each of the three activities below.

Audit Objective

1. Active and complete involvement of the users and the senior management
2. The project team has the necessary mix of skills for an acquisition project.
3. Acquisition plan provides the complete plan for the review of the project performance.

Audit Tests

Users and senior management

1. Review the project documents if the project has been approved and signed by the senior management. The senior management includes people heading the information technology division, the project division and the like.
2. Check if there is evidence of continuous review of the project by the management. Evaluate if the frequency of the review is adequate.
3. The funding source for the project has been clearly identified and approved by the management.
4. In particular check if the manager is co-ordinating the various teams involved in the project.
5. Check for the approval of the evaluation criteria of various alternatives and the evaluation criteria for accepting vendor proposal
6. Ensure the involvement of the users in all phases of the project, particularly in the requirement analysis stage and the testing and acceptance stage.

Project staffing

1. Check if the project managers authority and responsibility has been clearly defined.
2. Evaluate if the project manager's qualification is adequate.
3. Evaluate the skills and experience of the various members of the project acquisition team.
4. On an overall basis ensure that the project team is qualified to handle the project.

Project monitoring through acquisition plan

1. .Check if the acquisition plan has a predetermined schedule for the various activities involved in the project.
2. .Check the adequacy of the various performance tools and techniques prescribed in the plan for project management
3. .Check if the provisions of the plan for the performance monitoring are being adhered to.

Index : Audit of System Acquisition

Part 1	Overview
Part 2	Acquisition project management
Part 3	Needs, requirements, specification
Part 4	Alternatives
Part 5	Contract management-test & acceptance

Answer: [c] The project team is a mix of people with technical, functional and contractual abilities.

Module:7

Reference No:M7070

Question: While auditing system acquisition, the auditor's objective is to ensure that the system acquisition is based on complete and accurate lists of the functional needs of the user. For this, the auditor reviews which one of the following?

- [a] The security policy of the organisation
- [b] The requirements and specifications statement of the project
- [c] The acquisition-plan document
- [d] All of the above.

Module 7 - Audit of risks involved in system acquisition Part 3 - requirements specification

In any software acquisition project, specifying "requirements" is a very important phase. This includes identifying the requirements of a new system and describing all the input and output functions in specific terms. If the requirements are not specified properly, the project may be subject to the following risks

1. Ignoring alternatives
2. Incompatibility with existing hardware/software environments
3. Increased competition from vendors
4. Increased cost and time overrun
5. Also if the security/control features are not defined properly the software can lose data/integrity of the data.

This phase consists of three stages.

First, a need statement is drawn up based on the users' functional inputs given to the project team. Based on this a requirement analysis is prepared. In the final stage, specification lists for the project are drawn up.

This section lists the various tests that could be performed to mitigate the potential risks involved in the requirements analysis phase of the system acquisition process. Audit test should cover each of the stages as stated above. Based on specific requirements and the documentation policy, the test can be modified to suit individual requirements.

Objectives of the audit

1. To determine if the requirements of the acquisition project have been clearly identified and understood and if they correspond with the overall business strategy.
2. To determine if the requirements list corresponds to users' function requirements and satisfies all the needs of the users.

Tests

- Review the "user need statement" to ensure that it is in line with the strategic objectives of the company. It clearly specifies the information system infrastructure that needs to be supported (for instance volume of work etc.)

- Check if the statement clearly specifies the changes to be made to the current systems. - For instance checking if change in speed and storage capabilities etc, clearly justify the changes.
- Review the requirements analysis for a complete description of the existing system including costs, capacities load etc.
- Check if the requirements analysis contains
 - Details about the complete information needs of the organisation -how information should be obtained, what additional information requirements are necessary, the sources of the information, security, validation, performance needs, timeliness etc.
 - Support requirements like privacy of data, record management specifications (record retention, record safety etc), and environment factors like power supply, users training needs and legal standards are to be met.
 - Other support requirements like Interface specifications, compatibility etc.
 - New equipment required, with regard to this if there are any other particular requirements like specific brands etc the same must be justified.
- Check if the specification statement contains all the factors - functional, support, and performance requirements as included in the requirements analysis statement. In addition the specification statement should also contain
 - Performance measurement techniques that test the various parameters of the data for its integrity, accuracy, processing, flexibility, transmission etc.
 - Technical details like interfaces as mentioned in the requirement analysis sheet.

The auditor also needs to ensure that the organisation evolves a methodology to control the necessary changes in the requirements documentations. All the changes need to be reviewed and approved by the respective authorities.

Index : Audit of System Acquisition

Part 1	Overview
Part 2	Acquisition project management
Part 3	Needs, requirements, specification
Part 4	Alternatives
Part 5	Contract management-test & acceptance

Answer: [b] The requirements and specifications statement of the project

Module:7

Reference No:M7071

Question: Which of the following is true with regard to the audit of acquisition risks.

- [a] Conversion costs need not be included in the cost benefit analysis of the alternatives.
- [b] Analysis of each alternative takes into account only quantifiable benefits.
- [c] The alternative analysis is not a part of the audit of acquisition risks

[d] The non-cost factor constitutes an important part of the alternative analysis of an acquisition project

Module 7 - Audit of risks involved in system acquisition Part 4 - alternatives

In the system acquisition process, the first step is to draw a "requirements" document. The next step is to select the best alternative available. Here, the organisation needs to identify and assess the various alternatives available in order to fulfill the requirements of the users. Potential risks involved in not selecting the best alternative-

1. Financial risks in terms of selecting an option with high or additional costs when compared to other alternatives
2. Technical risks in terms of choosing an alternative that does not conform to the requirements specification of the acquisition project
3. Schedule risks in terms of delays in completion of project, not meeting technical standards etc.

Activities involved

1. Identifying all the alternatives available for the acquisition of the system (software or hardware required). These could be external agencies like vendors, in-house development or up gradation of existing information systems.
2. Assessment and evaluation of alternatives identified through various cost benefit analysis techniques.
3. Selection of the best alternative, which mitigates potential risks.

Audit objective

1. The objective of the audit is to ensure that all feasible alternatives have been identified.
2. All the alternatives have been analysed for their individual costs and benefits
3. The best available alternative with low risks factor has been chosen.

Tests

1. To ensure that all the responsible parties are adequately involved in the selection process. For instance, users have approved the alternatives considered; the contract officer and the senior management have approved the final alternative selected etc.
2. To ensure if all the alternatives have been considered by the organisation .To achieve this objective the auditor needs to check if there were resource constraints in the selection of the alternatives, for instance, if there was a staff constraint or a financial constraint.
3. Review the evaluation/assessment procedure. For this, the auditor has to determine whether
 - All the alternatives have been consistently analysed for the parameters set.
 - The costs benefit analysis of each alternative supports the alternatives analysed. For this, each alternative needs to be described in detail
 - The costs considered are comprehensive. The costs that needs to be considered are:
 1. Direct costs - these include conversion costs, personnel costs
 2. Indirect costs - these include operation and maintenance costs
 - All non-cost factors have been considered. These may include:

1. Maintainability-how convenient it is to service and replace the various equipments in case of damage etc.
 2. Obsolescence- how the company is planning to cope up with the technological up gradations in the future.
 3. Scalability-how easily the software/hardware can be upgraded to meet future needs.
 4. Flexibility-how convenient it is for the system to adapt to different working environments.
 5. Security-to what extent security measures are available within the system for securing data
 6. Privacy-whether the privacy policies of the organisation can be adhered to.
- All benefits both recurring and non-recurring have been included. Non-recurring benefits may include costs reduction due to use of economical equipments etc. Recurring benefits may include reduction in operating costs etc. Even non-quantifiable benefits (increase in the brand value of the organisation etc) need to be considered.
 - Ensure that all risks both economical and technical pertaining to each alternative have been analysed and the best and the most advantageous alternative has been chosen.

Finally it is very important to ensure that both users and the senior management have approved and signed off on the alternative chosen.

Index : Audit of System Acquisition

Part 1	Overview
Part 2	Acquisition project management
Part 3	Needs, requirements, specification
Part 4	Alternatives
Part 5	Contract management-test & acceptance

Answer: [d] The non-cost factor constitutes an important part of the alternative analysis of an acquisition project

Module:7

Reference No:M7072

Question: Which of the following is a party to the escrow agreement?

- [a] Mortgagor
- [b] Lessor
- [c] Lessee
- [d] Beneficiary

Module 7- Source-Code Escrow Agreement

Most companies spend huge amounts of money to purchase software, and invariably end up approaching vendors for modifications to customise the package to their style of functioning. But what will happen when the vendor is no longer available? An escrow agreement in such circumstances is the most viable solution.

Need for an Escrow agreement

The source code escrow agreement is the most important clause in a software licensing deal. According to this agreement a third party, known as an escrow agent will have custody of the source

code. The escrow agent will not release the source code unless the vendor satisfies certain conditions. For example when the developer/vendor goes bankrupt or fails to give support required as per the agreement. This agreement assures the purchaser that his needs will be met when the vendor does not exist. It also gives an assurance to the vendor that confidential information will not be leaked.

Parties to the escrow agreement

- **Settlor:** The vendor or the licensor who deposits the source code with a third party is called the settlor.
- **Escrow agent:** The Escrow agent or the Escrowee or Trust agent is neutral to the transaction. He holds the source code and supporting materials.
- **Beneficiary:** The licensee or the purchaser of the software is the beneficiary. He will be given access to the source code under certain defined conditions.

Elements of source-code escrow agreement

The elements of the agreement will vary depending on the circumstances of the licensee. Some of the important issues that should form part of the agreement are:

- **Escrow material:** The licensor or the depositor should deposit the source code and the object code with the escrow agent. Along with the source code all other materials sufficient for any other programmer to make changes to the source code should be provided. These may include design notes, documentation and the like. The object code should be on some magnetic media so that the escrow agent can verify the contents and ensure that they are working. If the licensee/ beneficiary is entitled to receive any other material such as modifications, version change, patches and the like as per the agreement, then the same should also be deposited with the escrow agent.
- **Certificate by escrow agent:** The escrow agent may be required to certify the integrity and completeness of the deposit. He should compare the deposit made with him to the software and the documents given to the licensee.
- **Cost:** The beneficiary of the agreement is the licensee and hence he would have to bear the cost of storage and maintenance of the deposit. He would also be required to pay the escrow agents' fees.
- **Release of the deposit:** Instances of when the escrow agent would release the deposit are when the licensor:
 - o Has discontinued the business
 - o Fails to make required modifications
 - o Fails to support the software
 - o Does not agree to maintain the softwareFor the release, the licensee should make a written demand to the escrow agent stating the release event, which is stated in the escrow agreement. The escrow agent in turn should give a notice of demand to the licensor. The licensor may either agree to the release or may dispute it.
- **Dispute:** The agreement should contain a provision for arbitration cost and injunctive relief. It should state as to who would cover the litigation or the arbitration cost and the expenses of the escrow agent.
- **Title and confidentiality:** The title of the software always remains with the licensor though the licensee may be given access to the source code and the materials. The licensee will be given only the right to use the software. To maintain confidentiality the licensor may give a list of his competitors with whom he should not deal with, in case he wants to replace him.

- **Warranty:** When the source code is released any warranty that applied to the software would become void. Once the licensee has tampered with the software the warranty would expire.

The above list is however not exhaustive. The vendors may have a sample of an escrow agreement with them. Since such agreements are usually in favour of the vendor, the buyer should ask for a customised agreement than just opting for the sample.

Answer: [d] Beneficiary

Module:7

Reference No:M7073

Question: Which of the following is not an element of measurement program?

- [a] Cost to the software project
- [b] Cost of technical support
- [c] Cost of analysis and packaging
- [d] Cost to the hardware

Module 7- Cost of Measurement of Software Development

A software measurement program in a software development organisation helps in better management of software projects and the software engineering processes. It provides improved management information, which allows better process results. It also helps in producing high quality product within schedule and budget.

A software measurement program therefore becomes very much essential for any software organisation. But the companies usually have a myth that cost of measuring the software being developed is very high and that establishing a measurement program would result in high overall cost of the software. Others are of the opinion that the cost of measurement will be of no value addition to the company.

Cost of measurement should be customised to fit into the budget of any organisation. A judiciously planned program can reduce dissatisfaction and shortcut attempts to achieve a failed software measurement program.

The Budget for a software program should be carefully planned incorporating the elements, which are generally expensive during the initial stages than during the later stages. This is because higher start up cost hinders the project. There are three major cost elements of the measurement program:

- Cost of the software projects
- Cost of technical support
- Cost of analysing and packaging

The cost of the above elements differs from company to company and depends on the

- Size of the organisation
- Number of projects to be measured in the measurement program.
- Degree of the measurement program (It could be parts of the life cycle, number of measures and the like.)

The cost is minimum when establishing and operating an efficient measurement program. It varies depending on the requirement of the company, which could be the limit to which the company wants, or can pay for, to enlarge the program so as to include additional projects, studies and the like.

The software measurement program involves various aspects.

- **Cost of the software projects**

The cost of measurement of development and maintenance constitutes the smallest part. It involves cost of completing forms, participating in interviews, attending training sessions, describing measurement or technology experiments and helping to characterise project development. The cost of measurement of a start up program could cost around 5 percent of the development budget but the cost of operating would not exceed 1 or 2 percent irrespective of the number of projects, which are to be measured.

Other costs could include introducing a new measurement program to the data providers. This could be due to inexperienced organisation's program or due to programs, which require the developers and maintainers to complete the unnecessary forms or require comprehensive details of little value.

- **Cost of technical support**

Technical support covers collecting, validating and archiving the measurement data. These activities are related to the technical support such as database management, library maintenance, execution of support tools and high level reporting of summary measurement data. Various costs involved in this are cost of personnel, cost of acquiring and maintaining database software, cost of support tools, cost of automated processing aids.

The cost of technical support would be around 3 to 7 percent of the total development budget.

- **Cost of analysis and packaging:** Cost of analysis and packaging is one of the main elements of cost of measurement. The activities associated with this cost are

- Determining what is to be measured
- Analysis of the data
- Defining the purpose of measurement
- Training
- Providing feedback
- Defining standards, policies
- Training programs and capturing assessments of analysed processes

The last two activities are related to packaging. The company should plan to spend at least three times as much on data analysis and use as on data collection.

The company should allocate adequate resources for the measurement program.

Answer: [d] Cost to the hardware

Module:7

Reference No:M7074

Question: Which of the following is a feature of rapid prototyping tools?

- [a] Difficulty in modifying the screens
- [b] Interactive capability
- [c] Simulates the input of final system
- [d] Generate a product different from prototype

Module 7- Prototyping

Software users may face difficulty in defining their requirements. A systematic analysis and review of the requirements helps in reducing uncertainties. A prototype of an evolving system enables the user to try the application and evaluate their requirements before undertaking a full-fledged development of the system. Prototyping is a process of evaluating the design, functionality and user interface.

Prototypes can be of different types viz. low-fidelity, high fidelity, exploratory, experimental, operational and the like. A good ***non-disposable prototype*** should have the features of planned system and enable the usability testing to develop into a final product.

Features of a rapid prototyping tools:

- Interactive capability
- Easy creation, development and modification of screens, task and window order, animations and the like.
- Generates code required for interface design implementation.
- Stimulate the expected output of final system.
- Gives an idea of how the final system would be in operation.

Process of Prototyping

- Analyse the customer needs
- Develop a low-fidelity prototype
- Iterate the process until both users and developers agree that the desired prototype is achieved.
- Develop the product according to prototype.

Before building a prototype, selection of tools, terminating criteria and length of iteration process, extent of fidelity and functionality required in a prototype and its purpose have to be taken into consideration. Prototyping is said to be ***complete*** when the desired purpose conforms to the requirements of the final system.

Drawing software, demo-makers, animation and slide show software, 4GLs, executable specification languages, visual RAD tools and user interface management systems are a few ***prototyping tools***.

Advantages of prototyping:

1. Flexibility: Prototyping environment provides greater scope for flexibility.
2. Communication: Better understanding about the concept enhances communication between developers and customers and reduces conflicts.
3. User satisfaction: The adequacy to fit in the client's requirement brings more satisfaction to the users.
4. Attracting tool: Clients and funds to support the operations can be easily attracted through prototyping as it clearly specifies the process.
5. Control: Management can find out the incomplete requirements by assessing the progress and can prevent unpleasant surprises.
6. Continuity: Even at times of cost overrun and time-overrun of the project or uncertainties, prototyping brings some benefits and allows uninterrupted flow of work.
7. Training: Systems developed using Prototyping are easy to learn and guides the future users.
8. Reduction of time and cost: Unnecessary testing time and redesign costs can be avoided with early detection of problems. It is simpler than the conventional development process.

9. Ownership: Prototyping provides a chance for both users and developers to experience the ownership.

Risks associated with prototyping:

- Provides wide scope for users to change specifications more frequently.
- Customers are required to supply the necessary feedback for iterative procedure. Their inability and unwillingness to co-operate may give rise to problems.
- The promising features of prototyping may deceive the customers.
- Developing a back-end code for predetermined front-end interface may be difficult.
- Lack of control over the method leads to indiscipline
- Testing of functional requirements of the system is given importance, ignoring the non-functional requirements.
- System specification will not permit the prototyping process after a point of time due to time and market constraints.
- Planning and scheduling will be disturbed with iterative process.
- Changes in the later stages will affect the structural integrity of the already designed part.

Applicability of Prototyping

The success of prototyping depends on its usage. It can be used to evaluate the alternatives, market requirements and proposed interface and identify the effect of change requests. Users can be involved in the design process and motivated to participate in requirements gathering. There should not be any divergence in the opinion of both the parties. The system for which the model is developed should be large and have a significant user interface component.

Non-applicability

Prototyping is not applicable when the project is very small. High customer expectations and un-ended iterative processes result in the failure of prototyping. Prototyping is likely to fail in the absence of system's external interface.

Answer: [b] Interactive capability

Module:7

Reference No:M7075

Question: Which of the following control mechanisms has to be considered in an audit of automated change management system to ensure the integrity of the test?

- [a] Programme modules to be migrated to testing environment needs to be frozen
- [b] Concurrent development of the modules should not be allowed by the system
- [c] The system should allow for a version to migrate to testing when already a version exists in the testing environment
- [d] None of the above

Module 7- Audit Of an Automated Software Change Management System

Concept

In the earlier times, manual processes were used to manage the software change management system. However currently, automated software is available to manage this process. These automated systems have removed the lacunae in the manual change management systems. There are numerous control mechanisms in these systems, which have reduced the laborious review processes

required to manage the software changes.

This section describes review procedures that need to be followed by a IS auditor in an automated changed management system. The objective is to ensure that the required control features exist and are being effectively utilised by the organisation.

As a first step, the auditor would have to conduct reviews to determine the control mechanisms that are being used and to identify the installation option, which handles the control option.

The steps involved in the audit are

1. To ensure that the software version that needs to be installed is migrated to testing environment before installation.
2. To ensure that versions migrated to test environment are not changed.
3. Preventing overlays in testing environment
4. Controlling concurrent development

Migration to testing environment: It is very necessary to ensure that any new software that needs to be installed is tested before it is actually installed and implemented. So in an audit of automated software the auditor needs to review whether there is any control mechanism in the automated system to ensure that all new versions to be installed are migrated to a testing environment. In the absence of an automated system, the manual control mechanism that can be adopted may require a person to manually review whether all the software versions are tested prior to their release.

To ensure that versions migrated to test environment are not changed: The auditor needs to ensure that the versions to be migrated to testing environment are frozen. Most automated change management systems have this option. If this option is not available in the change management system, then the integrity of the testing cannot be assured.

Preventing overlays in testing environment: To prevent inadvertent overlays of different versions of the software, separate libraries are created for each module or version or project. All the components of a particular version are stored in the related library of the project or a module. This ensures that there is no overlay of different modules of software in a software development life cycle. However it is very difficult to achieve this objective in the testing environment. Normally a warning message is given when the promotion of a software module is taking place in the testing environment. Another control mechanism is, to make it a policy to ensure that the project in the testing environment is required to either go out of the testing environment or be installed before another version is migrated to the testing environment. Otherwise a wrong module or a wrong version may get tested.

Controlling concurrent development: Concurrent development refers to utilising the same module of software program in different projects. Allowing concurrent development is necessary because there may be modules of software programmes, which are changed in many releases. It is very important to ensure that there are options in the system to send messages to all parties, using the modules about concurrent usage by others. All changes incorporated by each project should reach other project users so that the changes can be coordinated and incorporated. And also it is very important to ensure that change management system is used at the beginning of the development life cycle to ensure that all activities are under the control of change management. Another control mechanism of concurrent development is to ensure that modules in production should be checked. If they are production then it must be ensured that the version is same as that used for making changes. The only exception to this procedure must be the third party vendors. It must also be

ensured that dormant module is not allowed to migrate forward in the change management life cycle if there is another project using the same module is in the project.

Answer: [a] Programme modules to be migrated to testing environment needs to be frozen

Module:7

Reference No:M7076

Question: Metadata contains information about other information. The major drawback of metadata is:

- [a] It imposes a load on the server
- [b] Lacks standardisation
- [c] Keyword spamming
- [d] All of the above

Module 7- Metadata strategy

Metadata

A huge amount of information resources are used by large organisations. Metadata helps to describe these resources using simple and small packages of information. This assists the user in finding any information due to its direct access to the package of information. Metadata has much wider scope in the sense that it contains descriptive information about the main content, quality of data, conditions or the features of a particular data. This is the reason that metadata is also called "data about data". For example metadata contains information like:

- Name of the file, where the data is stored
- Size and the data type of the particular attribute
- Length of the data, fields and columns
- Data location where it is stored, its association and the owner of the data

Thus, metadata acts as a catalogue to search and access information from the organisation's data warehouse. Meta data is categorised into two groups viz.

1. Technical metadata
2. Business metadata

- **Technical Metadata**

It provides the information on data, which is under the scope of information technology like location of data, its data type and other related attributes. Most of the ETL tools are able to generate technical metadata from the current source.

- **Business Metadata**

As far as the information about data is concerned, business metadata is much more informative than technical metadata. This is with regard to information in business metadata like how and where was it migrated, when was it transformed and the like. All these are derived from system specifications, business policies and technical metadata. They in turn increase the overall quality of the data.

Importance of metadata

Metadata is important to organisation because it assists in data browsing, data transfer and data documentation. Metadata is necessary for designing special data clearinghouse, which assists the user in finding the data relevant for its application. Spatial data supports software-based

standards, which make the program more user friendly and the user can voluntarily shuffle data between platforms and systems. The use of metadata standards for naming, cataloguing, and operating can be set for all departments in an organisation. This will help in better understanding and sharing resources among themselves.

Metadata standards

Nowadays metadata is being created in number of standards. Two models that support metadata standards are:

- **Metadata coalition-Object Information Model (MDC-OIM):** It is developed as a modelling standard that can share and store information between different application and heterogeneous systems.
- **Object Management Group-Meta Object Facility (OMG-MOF):** These are building blocks of CORBA based distributed environment. This improves metadata management in distributed object environment.

Pros and cons of metadata

Pros

- The use of metadata will easily identify the crux of the information resource.
- It is easy to apply and hence saves lots of time and cost.
- It offers effective infrastructure for distributed resources.

Cons

- It increases load on the server.
- Standardised procedures for use of metadata are not really efficient.
- Metadata is stored in different files. So, the problem to influence information provider for the importance of metadata arises.
- It is not supported by some of the search engines due to "keyword spamming" (Some authors repeat keywords in the metadata in order to enhance the results of their search engines)

Answer: [d] All of the above

Module:7

Reference No:M7077

Question: Which of the following is not a benefit of Object Oriented Analysis?

- [a] It is easy to change the software
- [b] They are easier to program
- [c] Programs can be reused
- [d] User requirements are communicated to the software engineers

Module 7- Object Oriented Analysis

Traditional programming development methods give very detailed procedures for execution of command. As against this, the new programming method, say object oriented model leads to execution of a command to object. The program will say "what" to do but not "how" to do. The various methods of executing the command are left to the object. The objects are responsible for

their own actions while responding to requests from clients. In the traditional methods, programming is done to perform actions on data. In object-oriented model, the objects in data will perform actions on itself. How these actions are done lies behind the screen. The objects would be described more close to the real world. The focus is on objects rather than "data flow" as in the traditional method.

Object oriented analysis is based on the idea that the real world can be depicted in terms of objects. This analysis breaks the given problem into set of objects. Each set of objects have specific attributes. The objects communicate with one another. The software engineer before developing the software tries to break the given task into objects.

The objects can be

- External entities that need or generate information - e.g. Devices, people.
- Things that are a part of the information domain of a problem e.g. Reports, letter
- Roles that are required of people within the system e.g. Managers, engineers.
- Organisational units that are part of the application e.g. Group, team.

The objected oriented analysis helps the programmers, designers and the like to develop the software. For the success of this method it is necessary to

- Communicate the user requirements to the software engineers
- Define the classes
- Define the hierarchy of the class
- Define the relationship between the objects
- Define the required behaviour of the object

The above steps should be repeated until the desired model is achieved.

Object oriented analysis is based on the five principles. They are

- Modelling of information domain
- Describing the functions
- Determination of the requirements
- Classification of the system into data, functional and behaviour model.
- Understanding the problem through the models prepared in the early stages and overcoming the problems through the models prepared in the later stage.

Over the past decade there has been a significant development due to various individual approaches to object oriented analysis. Some of the major players have joined to combine the best features of their individual analysis into a unified method called the Unified Modelling Language (UML). UML is a general-purpose notional language that allows a software engineer to specify and visualise complex software for large object oriented projects.

The benefits of OOA are

- Maintainability: Mapping to the real world. The benefit is that it requires less analysis, and less complexity in system design.
- Reusability: The analysis can be reused. This saves time and costs.
- Easy to change: As there is close resemblance to the real world objects, the object itself may not change when the requirement changes. But its application and interaction with other objects may change. This makes it easier to change the software.

- Easy to program: In this model, the codes related to "how" remain at the background and hence do not clutter the main codes related to other objects.

Answer: [d] User requirements are communicated to the software engineers

Module:7

Reference No:M7078

Question: In order to ensure authorised change initiation and approval, in an audit of software change management, the auditor should verify

- [a] Request for change is made through request form
- [b] Circumstances when the normal procedure would not be followed
- [c] Periods for which documents relating to the changes have been maintained
- [d] Naming conventions used in the application and the system

Module 7- Audit of Software Change Management – Part 1

Software installed in the system is not likely to remain constant. Organisational growth or changes in the functioning warrants changes in the software too.

Organisational changes are easier said than done. Before making any change it should take into consideration the implications of the change that can be either internal or external. Change management includes planning, scheduling, implementation, testing and acceptance.

The audit process can be divided into three stages:

- Pre-audit
- Audit
- Post audit

In this article we cover the pre-audit stage. It comprises documents and policy review, change initiation and approval steps.

Pre-audit:

General Understanding: The auditor before commencing the audit should obtain a general idea about the functioning of the organisation. He should mainly focus on the following aspects:

- Organisation structure
- Flow of information in the entire application and the system
- Naming conventions used in the application and the system
- Recent changes to the application and the system

He should also obtain from the management, change management logs, and such reports as pertaining to the changes.

Audit:

1. **Documents and policies:** The review of documents and policies related to the change management by the auditor would give an insight into the existing change control process. The auditor should review change management process defined by the management and give special attention to

- Whether any person has been specified for managing and coordinating changes
 - Flow of change management within the organisation
 - Review of the changes and the intervals at which it will be done
 - Period for which records relating to change will be maintained
 - Procedure relating to back ups before any changes are made
 - Circumstances when the normal change procedure would not be followed
2. **Change initiation and approval:** Prior to any changes in the software, its authorisation has to be ensured. Unauthorised changes would lead to flaws in meeting the requirements and the user needs. A request form should be maintained to include at least the following details.
- Name of the person who has initiated the request
 - Department to which he belongs
 - Reason for the change
 - Detail note on the change while mentioning the module to which it relates
 - Approval of the change by an authorised person

The auditor should review

- Method for initiation and approval of the changes and ensure that the request for change is made through request form
- Priorities assigned for changes to be made
- An estimated time for completion of the changes
- Cost estimation before any changes.

Audit of software change management

Part 1

Pre-audit: General understanding

Audit: Documents and policies

Change initiation and approval

Part 2

Audit - Modification

Testing and acceptance

Implementation

Compliance testing

Security

Post audit

Part 3

Testing environment

Answer: [a] Request for change is made through request form

Module:7

Reference No:M7079

Question: _____ is hiding of certain details of an object from another class.

[a] Encapsulation

[b] Abstraction

- [c] Inheritance
- [d] Polymorphism

Module 7- Object Oriented Analysis - Part 2

An object oriented model makes use of objects, where the program instructs the object on "what" to do. However it does not instruct "how" to do. The features of OOA are abstraction, encapsulation, polymorphism and inheritance.

Abstraction: Analysts have defined abstraction in various ways. Some have defined it as a separation of behaviour from implementation. Behaviour would include data type and implementation as the representation of the object. According to the others, it is trying to isolate certain aspects of a data. It means including the essential features of data and excluding the boundary or other non-essential details to describe the data.

Abstraction is deciding on what an object is and what it will do. The use of abstraction by a system analyst will help him understand a problem before making any changes. When abstraction is used, the attributes of the objects can be easily modified.

Encapsulation: Encapsulation is hiding certain details of one object from other objects. With the use of encapsulation in system development there would be minimum impact on the other objects as a result of change in one object. It should be used especially when the system is being developed or is evolving.

Advantages of encapsulation

- Isolating knowledge: It isolates tasks that are performed by an object from other objects.
- Protects the system when changes are being made. The changes that are made in one object will have little influence or effect on the other objects.

Inheritance: Inheritance helps in defining the parent-child relationship between the classes. A sub class inherits all the attributes from the super class. There are two types of inheritance - interface inheritance and implementation inheritance.

- Interface inheritance: It is the classification of objects based on some common external interface. The class will possess attributes from its super class and may also have its own attributes. The inheritance of the attributes from a single class is called single inheritance and inheritance from multiple classes i.e. inheriting attributes from various classes is called multiple inheritance.
- Implementation inheritance: When the classes share implementation it is called as implementation inheritance.

Inheritance increases reusability of programs.

Polymorphism: Polymorphism reduces the effort required to extend the existing system.

It is the ability of an object to take several forms. An object, which is denoted by a name assigned to it, will be able to do a specific set of operations when it is called for. There are two types of polymorphism - inclusion and operation polymorphism.

- Inclusion polymorphism: This allows an object to belong to more than one class at a time. An object that belongs to one class can also belong to another, provided that the first object has a subclass relationship with the other object.
- Operation polymorphism: Different objects can use an operation with the same name though they have no relationship between them.

Answer: [a] Encapsulation

Module:7

Reference No:M7080

Question: The auditor while conducting the audit of software change management should ensure that changes are

- [a] Tested, accepted by the users and implemented
- [b] Accepted by the users
- [c] Accepted by the users and implemented
- [d] None of the above

Module 7- Audit of Software Change Management - Part 2

This is the second of a three part series on audit of software change management. The earlier article covered the pre-audit phase, review of documents and policies, change initiation and approval steps of audit phase. This article deals with other steps of audit phase and post audit phase.

1. **Modification:** Modification of the code should take place in a controlled environment. The modification stage should be separated from the production environment and quality assurance. The auditor should review
 - Procedure of communication to the programmer of the changes required
 - Control over the version change
 - Changes to the software are not made in the production environment, testing environment or the quality assurance environment
 - Library records to ensure that all the codes are maintained. The records should give a complete list of all the software that are available in the library along with the version numbers.
2. **Testing and acceptance:** Changes should be tested before being implemented. The testing process can be automated since the software is commercially available in the market. (This aspect is dealt in detail in Part III of the article).
3. **Implementation:** No change should be implemented unless the user is satisfied with the change and accepted it. Only authorised changes should be implemented. The auditor should verify that
 - Procedure exists to move only authorised codes to the production environment.
 - Responsible person is designated for authorising the changes.
 - Process exists for reconciling changes and by authorised persons only.
4. **Compliance Testing:** Compliance testing is done to ensure that only authorised changes have moved to production and the procedure designed by the management for system changes have been followed. Compliance testing can be divided into two - for non-emergency situations and emergency situations.

Non-emergency situations: The auditor should examine the non-emergency situations by selecting a sample from the population of non-emergency situations. After selecting the sample, the auditor should conduct a detail review of the entire process beginning with initiation, documentation and approval by a responsible authority. The documents should state that the code after making changes has moved to the testing environment and that it was subsequently approved by the quality assurance department before being implemented.

Emergency situations: During an emergency, the normal procedure for making changes may not be followed. Chances of unauthorised changes in such situations are more.. The auditor should ensure that

- Management has defined what situations will be considered as emergency.
- Procedure exists for making changes in an emergency situation.
- Emergency ids have enable and disable option. All the emergency ids are disabled after usage.
- An audit trail exists for all emergency ids which are reviewed by a responsible person
- All the changes made are properly documented
- Back up procedures exist

The auditor should take a sample of emergency changes and review whether the situation is properly classified as an emergency situation, whether proper procedure was followed and the changes have been properly documented. He should also review whether the number of emergency changes made during the period under review is appropriate to the volume of emergency change requests.

5. **Security:** The access to the change management library should be restricted. The auditor should review the security to the library to ensure that the access has been restricted.

Post audit: The auditor should ensure that the suggestions made by him have been implemented. If the suggestions are not implemented then the management must satisfy the auditor about the reasons for non-implementation of the suggestions.

Audit of software change management

Part 1

Pre-audit: General understanding

Audit: Documents and policies

Change initiation and approval

Part 2

Audit - Modification

Testing and acceptance

Implementation

Compliance testing

Security

Post audit

Part 3

Testing environment

Answer: [a] Tested, accepted by the users and implemented

Module:7

Reference No:M7081

Question: Request for proposal should be drafted by

[a] Top management

[b] Project team

- [c] Vendor
- [d] IT steering committee

Module 7- Request for Proposal

Request for Proposal (RFP) is one of the most important documents when a company wants to license or purchase software from vendors. It contains a draft of the company's software requirement and needs. It is on the basis of this proposal that the company identifies the vendor from whom it would like to purchase the software.

Unless a company plans its requirements, it cannot buy the appropriate software. A good RFP will clearly outline the needs of both the management and vendor. The criteria for a good RFP are as under:

- A project team along with participation from technical staff and the users should be created for drafting the RFP.
- An analysis of the needs of the company should be done. The needs analysis should state
 - o The purpose of acquiring the software.
 - o The functions it will perform.
- The requirement should be defined in a clear and detailed manner.
- It should be a questionnaire, which does not require a detailed answer from the vendor.

The RFP should be the same for all vendors. It should be framed in a way that allows for easy comparison between different proposals of the vendors.

Consultant:

Consultants are usually appointed when the company has no idea of the availability of the products in the market or if it is not in a position to define its needs. The company before it appoints a consultant must ensure that the consultant has a good knowledge of the market and is not biased towards a particular product. The role of the consultant would be to

- Help the company in defining its needs
- Preparation of the RFP
- Distribution of the same to the vendors
- Analysing the proposals of different vendors
- Selection of the vendor and finalising the contract

Copyright:

It is always advisable for the company to get its RFP copyrighted. This prohibits the vendors from distributing the company's RFP to other vendors. Copyrighting would also prevent the vendors from showing the company's plans and its requirements to the competitors.

Components of contract with the vendor:

- Description of the deliverable
- Cost structure
- Date of deliverables
- Support that will be provided by the vendor
- Maintenance agreement
- Installation support that will be provided by the vendor
- Testing of the product before the installation
- Warranty period (if any)

- Ownership of the property

The RFP should be appended to the contract. This ensures that the vendor will not make any contradictory statements later.

Customised software: When a company is interested in customised software, it buys the vapourware software i.e. the software with no pre-determined programs and functions. The company should not purchase the software just on the basis of demo of screens appearing on the original software. A demo does not give a good idea about the response time of the software (from the database) or the flexibility in the software. The company should ensure that the response to RFP from the vendor includes detailed information of the dates on which the targets will be met. This apart, the financial credibility of the company must also be considered.

Answer: [b] Project team

Module:7

Reference No:M7082

Question: Which of the following statements is true with regard to an IT budget?

- [a] Expenses related to disaster recovery need not be considered
- [b] Network management expenses include troubleshooting costs
- [c] Training costs are not part of IT budget
- [d] None of the above

Module 7- IT budgeting -Part 2

This is the second article in our series on IT budgeting. In this article, we have described the various direct labour costs that need to be included in an IT budget.

IT management expenses

These include the labor expenses or outsourcing fees for network, system, and storage management. Expenses are calculated as follows:

No of people managing a particular task * rate per person.

Network management

These include manpower expenses for optimal maintenance of network components. They include access media, network and communication, information sharing and printing.

The following categories of expenses are normally included

- a. Manpower costs for troubleshooting and maintenance. Failure identification and fault management expenses also fall under this category.
- b. Network traffic management expenses
- c. Network performance managements expenses
- d. User management expenses. These include adding, deleting modifying users etc.
- e. Operating system management expenses
- f. Routine maintenance expenses like maintenance of passwords etc.

- g. Advance support maintenance -support personnel for this function is involved only in cases where problems cannot be solved using standardised solutions and require an in-depth analysis.

Systems Management

The routine maintenance expenses of physical computers are a part of systems management.

Types of expenses included are

- a. Costs involved in infrastructure planning like identifying needs and researching options. The infrastructure involved here includes servers, client networks and off-the-shelf applications.
- b. Manpower costs for procurement support, and testing of the products.
- c. Manpower costs involved in software deployment, up gradation etc.
- d. Manpower costs involved in asset management and tracking changes reconciliation etc.
- e. Labor expenses for application management and access management.
- f. Manpower costs of security personnel if any
- g. Labor costs involved in hard re-configurations, system upgrades, topology changes or other changes related to hardware settings. However, software up gradation costs is not included here.

Storage Management

The expenses involved in this category are

- a. Labor costs involved in disk and file management. For instance, maintenance of hard disks, directory trees etc.
- b. Annual expenses for storage capacity management
- c. Data access management expenses including file access management and remote server access
- d. Annual expenses of back up management and archiving staff members
- e. Expenses of staff involved in Disaster recovery management
- f. Repository management
- g. Support costs

Labor costs

- a. Administration,
- b. General IS management
- c. Learning costs- includes casual training or formal training experts from outside the organisation, in-house course management, costs involved in delivering the courses, and the cost of time spent attending courses.
- d. Vendor management costs.
- e. IT related traveling costs
- f. Other miscellaneous operation costs.

Fees and contracts

This includes fees paid to outside faculty for training, maintenance contract costs, support contracts for IT etc.

This is an activity based costing, however it can be modified to head count basis also.

Article 1	Introduction -direct costs-hardware and software
Article 2	Direct costs-direct labor costs, support costs
Article 3	Support costs-indirect costs

Answer: [b] Network management expenses include troubleshooting costs

Module:7

Reference No:M7083

Question: One of the methods that can be adopted to mitigate the risk of uncontrolled requirements from users in a product development life cycle is to have

- [a] Longer delivery cycles
- [b] Shorter delivery cycles
- [c] Project end delivery
- [d] None of the above

Module 7- Software Development- Issues and Risks

Software development is becoming increasingly complex as projects are increasing in size. As a result, the number of potential problems and demands from businesses are increasing by the day.

In this article, we have discussed the risks and issues associated with software development-

Development Issues

Some of the common issues involved in software development are

Cost-schedule-Avoiding cost and time delays

Compatibility-Ensuring that the product is compatible with the intended environment

Performance-Ensuring that the product meets the required specifications.

Fail -safe and fault tolerant- Ensuring that the system copes with certain influences like hardware failure, power failure etc.

Scalability -Ensuring that product can cope with changing environments such as operating systems etc.

Risk Assessment

Few years ago the IT team reduced risks by clinging to a six-week change cycle, now they have to cope with short notices like a 6 day change cycle or 6 hour change cycle. Hence, it is highly recommended that risk management should be taken seriously and be incorporated into the entire decision making processes. Risk management now is applicable to all segments of IT operations.

Some risks associated with the software cycle include

1. Changing user requirements
2. Lack of quality
3. An unachievable development schedule
4. High turnover among users or in the development team
5. Friction between developers and customers.
6. Business risks- the failure of a software project, may lower the credibility of a brand, reduce productivity, and revenue, and increase liability. These are much more critical in case of e-commerce projects

One method to tackle such issues is to develop a risk management plan. The plan should include an automatic escalation process in case things get out of hand. The risk plan should also consider the cost impact of the whole process.

Sample plan

A sample risk management plan has been given below. This model prescribes a four-stepped methodology to tackle each risk and issue that is identified by the developers.

The steps involved in the risk management plan are

Identification: The first step in the risk management plan is to identify risks. There are various sources of risks in a project. For instance, users could be a source of risk. Users could be constantly adding/modifying requirements. This could delay the delivery date of the project and thereby escalate the costs.

Risks analysis: in this step, an analysis of the risk needs to be done. The analysis should include a plan for mitigating risks and risk contingency plans. In the above example, one of the control measures for the above risks is to have a good requirements collection in the initial phases of the project. Risk should be escalated to a higher level after a certain benchmark. For instance: Inform higher authorities, if

1. The users have not accepted the prototype within a specified time.
2. Users make changes to the requirements after 30 days of trial.
3. User requirement changes that are more than 10% of the original accepted requirements.

Remedial measure: The next step is to plan the actual implementations of risk. For the above-mentioned cases, you can follow the approach given below to incorporate the risk mitigant factor into the product development life cycle. For instance, it may be decided to use a user-based interface prototype at the beginning of the projects to ascertain requirements and maintain effective change control over user requirements. In such a case, keep the delivery cycles shorter in order to minimise inter-stage changes etc.

Risk management: This involves deciding on support issues for implementation like staffing of the project team. Entrusting the complete responsibility to a particular member for a particular project including risk management, deciding on the delivery schedules of the various stages of the project and the costs considerations.

Answer: [b] Shorter delivery cycles

Question: ----- is a risk which when handled inadequately may lead to an insecure ERP implementation.

- [a] Lack of management intervention.
- [b] Lack of adequate access rights
- [c] Lack of auditability
- [d] All of the above

Module 7- Enterprise Resource Planning: Implementation Issues

Enterprise Resource Planning or ERP as it is popularly known is a tool that was developed to integrate various business processes into a single synchronised entity. The idea behind ERP was to conserve valuable resources and reduce the transaction processing times to the bare minimum. However, when one looks at the various implementations in organisations, the scene is quite the opposite. In certain cases, the cycle time for small activities has increased several times, going against the original objective of why ERPs came into being in the first place.

Observations on the reasons behind the failure of various such implementations indicate that the problem is not with the product or technology. The basic idea of process integration is a perfectly justifiable idea. The problem however, lies with the implementation methodology, and our approach to the product and technology. The solution lies in logically re-thinking and carefully planning the implementation. The management has to clearly identify the control points of each business process and the integrated solutions devised must be configured to include the control objectives.

Issues

Some of the risks associated with an ERP implementation have been listed below. These have been classified into 3 categories- business, product and resource issues.

Business issues

There are 2 types of business issues that need to be decided prior to an ERP implementation.

Management policies: ERP implementation brings about a change in the way the business is being conducted until now. Since the basic idea is the integration of various processes, departmental barriers need to be removed. This can mean resistance from staff who are used to a particular kind of business operation. Hence, this issue needs to be clarified before any ERP implementation is started.

Management control: One of the basic principles of ERP is that data is captured only once. The original data is then manipulated, modified and used by various business processes. Therefore, the management's intervention for control is not required while the data passes through different sections. The management can now shift its focus to making business decisions based on the data, than concentrating on the control of data. Hence, it is important that managements are prepared for this change.

Product Issues

There are 2 product issues that need to be clarified for an ERP implementation

Data Ownership: Unlike the original business model, the same data is now available to all parts of business (that is finance, accounting purchase etc) due to the integrated processing of the data. Hence, access rights need to be clearly defined during implementation. The principles of security need to be built at the designing and testing phase to ensure a secure business process.

Auditing: The system to be implemented needs to be auditable and should allow an independent reviewer to easily verify its activities. Evidence that the system is functioning as per the specifications, is adequately controlled and confirming to standard practices, should be made available. This will prevent designing an insecure system with poorly designed controls.

Resource Issues

Two resource issues need to be tackled for an implementation

Skilled resources: Since ERP implementation is a specialised function, the organisation needs to pool required skilled resources for an implementation.

Cost and time overruns: ERP implementations are among the largest IT projects that are usually undertaken by organisations. So, they need to be treated like any other software development project with inbuilt project management controls to avoid delays and overruns.

Finally, all these efforts should lead to a completed system, which has a high level of integrity.

Answer: [d] All of the above

Module:7

Reference No:M7085

Question: Which of the following statements is true with regard to IT budgeting?

- [a] It includes only direct development costs.
- [b] Productivity loss (of an end-user) that occurs during IT training is a relevant cost for the budget.
- [c] Indirect costs of the budget include training costs and productivity losses.
- [d] All of the above

Module 7- Information Technology -Budgeting

Most organisations do not have a good tracking mechanism for their IT budgets. Most of the time, indirect costs like training costs that are borne by users are not accounted for in the budgeting analysis. Besides, these costs may sometimes be a major part of the total IT department costs, and could constitute 50 % of the total cost. Though hard to quantify, efforts must be made to track these costs-

Given below is the framework of a budget for an IT project /department. It includes the following components:

- Acquisition costs
- Installation costs
- Maintenance costs
- Networks costs and
- Application costs

This budget is intended to provide the IT professional a clear idea of the total costs involved in the development of an IT component.

The above components can be grouped into 2 basic categories.

Direct costs- These are costs, which can be directly attributed to the IS cost centre. They include hardware costs, software costs, direct labour, operations staff cost, development costs and communication fees.

Indirect costs- These are costs, which cannot be directly attributed to the IS project. These include training costs, support costs, and loss of revenue during down time.

Each of these costs have been described in detail below

Direct Costs

I. Hardware and software costs

1. Hardware

Initial costs- These include the acquisition fee for computers, such as servers, workstation and the like. This includes the cost incurred for computers, memory, storage media and application software. Acquisition fees may be amortised over a period of three years using the straight-line method. (Assumption: Computer assets have a life of three years.)

Annual up gradations- These include the costs incurred for upgrading of:

- a. Computer memory
- b. Storage media like hard disks, network storage devices
- c. Peripheral devices like new CD-ROM drives, multimedia accessories or printers
- d. Network components like cabling, new network cards, new ports and the like
- e. Other miscellaneous items like spares

2. Software

The following expenses have to be considered for both new software and up gradations:

- a. Client server software
- b. Operating system licenses
- c. Applications like word processors, spreadsheets, financial packages, accounting packages, vertical applications packages, business software
- d. Utility software like network management software, virus protection tools, programming packages, screen savers, back up tools, performance tuning tools, test tools, configuration management tools, documentation tools and the like
- e. Messaging software and remote connectivity.

3. Monthly costs

These include the monthly financial expenses for leased hardware, software and supplies, as well as costs incurred for toner cartridges, diskettes, tapes and other consumables.

	software
Article 2	Direct costs-direct labour costs,support costs
Article 3	Support costs-indirect costs

Answer: [c] Indirect costs of the budget include training costs and productivity losses.

Module:7

Reference No:M7086

Question: System designer is responsible for _____.

- [a] Ensuring the correctness of the system design.
- [b] Examining the internal interfaces
- [c] Resolving and answering queries from customers
- [d] Designing and creating a high-level system architecture

Module 7- System engineering roles - I

The concept of "systems engineering" can be clearly understood by defining the twelve roles of system engineering. This classification gives an overview of system engineering and helps to define its organisation charter. The following are the six roles of system engineering. Remaining six roles are defined in the next article.

1. Requirement manager: Requirement manager is also known as specifications writer or functional architecture developer. Requirement manager clearly writes what the customer requires. This helps to design and architect the system and sub-systems. He has to ensure that the right requirements of the customer are captured by functional architecture. Requirement manager needs to assess the impact of potential changes on the system. Thereafter he has to modify the specific requirements according to the changes.

2. System designer: System designer is also known as chief engineer, system architect or design architecture developer. His role starts after the requirement manager performs his functions. But in many cases, they proceed simultaneously. He is responsible for designing and creating high-level system architecture, integration and verification processes. He deliberates on different ways of building the system as per the specifications and then selects the final system design.

3. System Analyst: System analyst is also referred as performance modeller, system modeller or a simulator. System analyst is responsible for ensuring the correctness of the system design. He analyses the weight, power, input, output and memory of the system, to ensure that the proposed system is according to the user's specifications. Modeling the critical parts of the system and explaining the system's functioning to the users is also the duty of the system analyst. The level of modelling depends on the level of accessible simulation tools. Complex and risky program demand an extensive analysis than a simple program.

4. Validation and verification engineer: Validation and verification engineer is also known as test planner and the system test programmer. . Validation and verification engineer is responsible for testing the designed and developed system to check whether it will meet the specific requirements. He implements the system verification programme, tests the plans and procedures. He identifies the irregularities and conveys the same to the experts.

5. Logistics and Operations manager: He also performs maintenance and disposal functions.

Resolving and answering the queries from customers in the later stages of program is generally the primary responsibility of the logistics manager. At the same time, he has to incorporate the maintenance, operation, logistics and disposal functions into the primary and implementation phases of system design. They create user manuals and have full knowledge of design and operational aspects of the system.

6. Glue role: System engineer performing the glue role is also called as risk identifier, system integrator or the owner of the internal interfaces. He is responsible for identifying and preventing the problems at interfaces. For this he has to examine the internal and subsystem-to-subsystem interfaces.

System designers ensure the functioning of subsystems and Glue systems engineers make sure that they do not interfere with each other. System engineer should have adequate knowledge and experience to perform Glue role and must regularly update them.

Answer: [d] Designing and creating a high-level system architecture

Module:7

Reference No:M7087

Question: Which of the following is the function of customer interface role?

- [a] Interacting with customers to understand the customer requirements.
- [b] Data and process asset management
- [c] Resolve the conflicts between system engineers
- [d] Managing the complex and pervasive information systems

Module 7- System engineering roles - II

Six roles of system engineering were discussed in the earlier article. Next six roles are being explained in the present article.

7. Customer Interface role: Customer advocate or surrogate is the name of the system engineer performing the customer interface role. Developing the system from the customer's perspective is the main objective of the system engineer. Therefore, in a customer interface role, he has to interact with customers for a clear understanding of the customer requirements. His role is limited to build a customer specific product and does not include the marketing process of the organisation. Different organisations perceive the customer interface role differently.

- Organisation, which does not recognise the customer interface as a system-engineering role: Such organisations don't allow customers to discuss with system engineers. They fear that customers may derive more benefits from the system engineers without providing any additional funding.
- Organisation that maintain customer interface throughout the system design: Technical staff' of the customer are regularly informed of the status on design and other issues. System engineers respond to the change requests of the technical personnel.
- Organisations that link the customer interface role with the requirements manager and system designers: This is the role played by the system engineers in the new business development area. Their responsibility is to discuss with requirements manager and system designer and evaluate the cost effectiveness of different options.

8. Technical Manager: Technical manager is also called as Technical planner, technical scheduler or project manager. Technical management is a part of program management function. Program systems engineering manager or the engineers involved in delivering customer specific product may be given the responsibility of technical management function.

A product manager or an engineer similar to systems engineer may be created as the system engineering is extended to commercial companies. He is more responsible for marketing and cost aspects rather than a technical aspect.

9. Information Manager: Information managers perform the functions of configuration management and data management. Organisations, which give importance to "program management", consider the configuration management as a role of system engineer. But they have to consider the complete information requirements of the system and business to deal with complex and pervasive information systems. Hence, data management and process asset management are included in the functions of information managers.

10. Process Engineer: Process engineer is also referred to as business analyst, business process-reengineer or the owner of system engineering process. He is responsible for documenting, following and improving the project and system engineering processes. He has to identify the systems engineering metrics.

11. Coordinator: He coordinates different disciplines and is head of the integrated product teams. His duty is to resolve the conflicts after consultation with systems engineers. They try to bring coordination between engineers. Coordinators should possess team leadership skills. They should motivate the groups to build leadership and working norms skills.

12. Others: This include all other skills expected of a system engineer viz. shell scripting, performance analysis, SQL and network integration. Such a role of a system engineer is inclined more towards computer systems.

Answer: [a] Interacting with customers to understand the customer requirements

Module:7

Reference No:M7088

Question: Which of the following is not essential to consider while designing the effective user interface?

- [a] Ergonomics
- [b] Ergonomics
- [c] Interface technology
- [d] Evaluating vendors

Module 7- System design - User interface, input and output design

Development of an efficient, reliable and maintainable system is the main objective of a system design phase. The main elements in the system design phase are user interface, input design and output design.

User interface design

Users can communicate with the computer system through User interface system. The following are the principles for designing a user-interface:

- Understanding the underlying business functions thoroughly and maximising the graphical effectiveness
- Identify the users of the system, and develop the system from their perspective
- Designing a comprehensive interface and use of prototyping
- Feedback enabled
- Proper documentation of interface design.

The following guidelines help to design a good user interface: The design, which considers ergonomics, aesthetics and interface technology, can be an effective user interface design.

1. **Ergonomics:** It describes the working, learning, and interacting process with computers.
2. **Aesthetics:** Aesthetics relate to developing an attractive and easy user interface
3. **Interface technology:** The organisational structure necessary to achieve design objectives is described in interface technology.

Controls: Menu bars, toolbars, dialog boxes, scroll bars, check boxes, command buttons, spin bars and the like act as control features.

Input design

The quality of the output is based on the quality of input. A good input design system should enable a timely and accurate input of data into information system. Batch input, online input and tradeoffs are different methods of input and data entry. Input of the necessary data by avoiding constant data input will minimise the input volume. If the data is available in other system files, it should not be fed again.

Designing data entry screens

Forms: Form filling is an effective online data entry method. A blank form on the screen is filled with the data. An effective, accurate, simple and consistent input forms ensure the quality of the output. The following techniques must be followed for form filling:

- Proper flow must be maintained in the forms
- Information must be grouped into heading, body and comments
- Captions will guide people while filling the form.

Encourage users to furnish complete data in order to reduce errors. An attractive form by using different font sizes can attract the users to fill the forms completely.

Screens: The screen design must be simple, attractive and consistent. The user must be capable of moving between the screens. The screen can be divided into heading, body and comment to make the screen simple. The information can be grouped logically to make screen consistent.

Blinking cursors, pictorial icons, different colour combination and different font sizes can be used to make the screen attractive.

Input errors: The quality of the data is improved when input errors are minimised. Avoiding unnecessary data entry will reduce input errors to a certain extent. On the other hand, a data validation check, verifies the data at input stage itself so as to accept only those, which satisfy specific conditions. Sequence, existence, data type, range, reasonableness, validity and combination

checks and batch controls are different types of checks before the data is passed.

Input controls: Audit trail, data security, record retention policy and encryption ensure the correctness and completeness of the input data.

Output design

The system analyst should enquire the output needs, the required quantity, format, place and time of requirement and output method before designing the output. Print, screen, audio and electronic output are the different forms of output. The speed, cost flexibility and storage differ in each output technology.

An analyst should interact with the users before designing the output. He should understand the possible sources of bias in output and inform the users about the same. Training should be provided to the users to verify the accuracy by using different type of outputs.

Printed output: Special layout forms are used to design printed reports. Detail, exception and summary reports are the different types of printed reports. Decision makers extensively use these reports. Hence its format and design must be approved by the users.

Controls: Several output control methods are used to protect the integrity and security of output and to avoid theft or unauthorised access.

Answer: [d] Evaluating vendors

Module:7

Reference No:M7089

Question: Which of the following is essential in the process of system migration?

- [a] A comprehensive strategy for reengineering project
- [b] Monitoring the system engineering contractors
- [c] Existence of configuration management
- [d] All the above

Module 7- Audit of System Migration

In a business environment, the only constant thing is change. Therefore systems must be continuously modified so as to be in line with the new environment. The existing systems' life is extended by adopting new technical infrastructure. Such a process is referred to as System Migration. Organisations have to consider the objective behind the system migration for a smart selection of technical infrastructure and to execute the reengineering process efficiently.

Step: 1: Examine whether a comprehensive strategy for reengineering project has been developed:

All reengineering projects have a clearly spelt out long-range strategy with a focus on right problems and deliverables. The strategy should pay attention to even minor details and all assumptions should be tested thoroughly. While deciding the reengineering process, emphasis should be on inputs like strategic, programmatic, technical and economic issues.

A detailed migration strategy should consider the development of contingency plan and availability

of testing facilities. The appropriateness of the software integration process has to be verified. Migration should be considered as a separate project and must be managed efficiently.

Step 2: Carefully examine and monitor the role of outside systems engineering services:

Technical expertise and ability to employ skilled personnel enables contractors to offer better engineering services to their clients. But, lack of proper policies to monitor the contractors may result in the project failure. Their role should be clearly defined.

Contracting organisation should maintain sufficient control over the project. It should select the contractors, who have suitable experience and adequate resources to deal with the project. Qualified people should handle the task. Businesses should look into the contractor's advices carefully. The cost-benefit trade-off of outside contracts has to be examined.

Step 3: Check whether sufficient training is provided to the technical staff to deal with new technology:

In a reengineering effort, new technology and programming concepts are adopted and hardware is changed and updated. This demands provision of adequate training to the existing staff or replace them with skilled staff. Training proves successful in developing required skills for the new technology but it is difficult to motivate the employees to accept change. Organisations should educate the employees on the potential benefits from change. Therefore, technology and organisational aspects should be covered in training programme. Another essential thing is that the skills required for the new technology must be clearly mentioned in the contract.

Step 4: Ensure the existence of configuration management:

For a systematic implementation of migration process, configuration management is essential. It should cover system documentation, all change requests with priority assigned, the impact of such changes and the like. In addition it is important to have information on cost of maintenance and project management capabilities to for smooth maintenance operation.

Ensure that adequate documentation of legacy systems, change control processes and historical measurements are available. It helps to know the present system, manage the future and to identify the controls exercised over the system. Change control processes include methodology to handle change requests. Historical measurements record the changes made, problems encountered and cost incurred at that time. All these details serve as a baseline to deal the change with available time and resources. Absence of data delays the system release.

Step 5: Examine the documentation of requirements definition and its authentication:

If the requirements for the reengineering effort are not properly described and verified it may result in system failure. Requirements relating to functional, non-functional, users and customers, hardware, software and architecture are to be mentioned. But is not an easy process to specify the requirements for such a diversified list.

Absence of baseline requirements or flaws in them complicates the process further. Quite often people mistake that the existing requirements are sufficient but many times it is not so. They may not correspond to the system functionality. Therefore, it is necessary to check whether:

- "Concept of operations" is developed for the intended system according to the user's requirement and ensure its documentation

- The end-to-end operational scenarios and quality attributes are specified and validated. Ensure its accuracy and appropriateness to the proposed system
- Requirements implications are understood thoroughly

User scenarios, rapid prototyping and storyboards development are the practices in operation to make the process efficient.

Answer: [d] All the above

Module:7

Reference No:M7090

Question: Which of the following should the management consider in System Migration?

- [a] Cost schedule and capacity trade-off
- [b] Impact of changed elements
- [c] Present development and future maintenance costs
- [d] All the above

Module 7- Audit of System Migration - II

Part I of Audit of System Migration focussed on the five steps of System Migration Audit. This article deals with remaining five steps for system migration audit.

Step 6: Architecture should be the primary concern in reengineering effort:

Systems software architecture includes software components and the relationship with its visible properties. The primary consideration in the reengineering effort should be the systematic evaluation of existing software and the intended system's architecture. Evaluating the existing architecture helps to know whether it can be taken as a base for reengineering project or to start afresh, ignoring the existing architecture.

The architecture guidelines include the following:

- A framework for integrating separately conceived systems with overall system is developed
- Subsystems are upgraded and checked whether they fit properly in the larger system.
- All stakeholders must have a common understanding about the architecture
- Past performance must be evaluated if architecture is acquired from vendors.
- Architecture evaluation is done at an early stage of system development, say in the design phase itself.
- The core system and operating environment are understood
- Security measures and logistics are evaluated

Step 7: Ensure the existence of distinctive reengineering process:

Defining the life cycle process is not sufficient to understand reengineering process. A detailed guideline for system development process and its integration with work products must exist. A distinct reengineering process is to be prepared. Stakeholders are to be engaged in formulation process and process results have to be linked to goals and objectives.

Quality people, technology and resources might be there, but without quality process in place, these resources may not produce quality products. Major reengineering concepts like operational system

migration strategy and software architecture have to be defined first. This helps in the evaluation of the organisation's ability to carry out the reengineering tasks efficiently. Then the low-level task of reengineering and the software applications have to be considered. In case, outside contractors are involved, their ability in the software development process and past experience has to be considered.

Step 8: Ensure the reengineering plan is prepared and followed:

Project team consisting of engineers and software reengineering experts play an important role in solving the global issues involved in the migration approach. They can do so by understanding the missions, goals, objectives and systems thoroughly.

A reengineering plan has to be prepared and followed carefully. A planning group must be formed with a leader. Stakeholders must approve the plan. Ensure that proper feedback is provided to top management about the implementation of plan. Give the responsibility of both planning and execution to the same team to ensure the efficient execution of the plan.

Step 9: Evaluate the commitment of the management:

All large-scale projects, which contain strategic, business and information technology planning, managing resources, organising and evaluating projects, demand management's attention. But their concentration on the reengineering effort is much more important, because correction of the missteps is very difficult in this process.

Assign the responsibility of completing the project to a competent person. Core personnel should assist the responsible manager. For the success, the project leader and the team should stay on the project with no other major responsibilities thrust on them.

Step 10: - Ensure that management decisions are based on technical grounds

Stakeholders that include line managers, project team, experts may often have to take decisions under constraints of time and resource. However, technical details should not be ignored. Management must provide technical advice on cost, schedule and capability trade offs to ensure successful completion of reengineering project. Technical advice must be provided after analysing various parameters like system, historic data and knowledge of skilled people.

Auditor has to ensure that management has considered the

- Cost schedule and capability trade-off
- Impact of changed element (whether cost, schedule or function) on other elements
- Present development and future maintenance costs

Answer: [d] All the above

+Module:7

Reference No:M7091

Question: Which of the following would minimise the test failures?

- [a] Properly documented requirements
- [b] Early detection of defects

- [c] Automated input selection
- [d] All the above

Module 7- Test Automation Framework

Introduction

Testing is a major element in 'system development and maintenance' costs. Hence its failure results in heavy loss to the enterprise and also delays the implementation of software. Defects in specifying the requirement (Requirement defects) is the major contributing factor for test failures. Identifying the problem in the early phase of development process can avoid unnecessary expenses. Model-based automated test is an approach, which effectively identifies and corrects the requirement defects in the initial stages. Test automation framework is the name given to the approach. It merges with several test generation tools and helps in defect prevention. It reduces cost and manual effort.

The following is the detailed explanation of how model based testing effectively minimises the defects and reduces the costs:

1. Modeling requirements: Well-documented requirements, equip the developer with a disciplined and structured approach. Usually several persons are involved in the process of developing and maintaining the requirements. Incomplete and inconsistent requirement specification results in chaotic presentation. Informal documentation of the requirements is another aspect, which makes defect identification difficult. Human effort may not permit rigorous inspection to reduce inconsistencies.

A disciplined and a well-structured modelling process helps in formalising the requirements. It serves as an efficient tool to have a complete requirement specification and automated test generation.

2. Defect detection: The "requirements defects" are identified and corrected in the defect detection process. Early detection prevents percolation of defects. Mistakes when identified in the later stages of development increase cost and also lead to enormous rework. On the other hand, if they are detected in the early stage, rectification cost can be minimised.

3. Requirement validation: Users and stakeholders must specify and validate the requirements according to their needs and functionality. Automated test model assist users to evaluate and understand the requirements thoroughly.

4. Test Design effort: Manual selection of test inputs and outputs may give rise to errors. It is also a time consuming activity to have such a manual procedure for all tests. Automated test design process can produce an effective testing effort. The requirement analysis models can be leveraged to perform automatic test design activities.

Application of Model in the organisation

A typical organisation, involved in development process, will comprise requirement engineer, architecture designer and test engineer. The documented requirements are sent to the designers and testers under System Requirement Specifications (SRS), function lists, or change request form. This is very essential for test planning and development.

Developing verification tools is an important function of designers and testers. Tools are essential to validate and verify the requirements of system development. These tools use the verification

models developed by testers to detect the defects automatically. The test failure reports are automatically generated in the test execution process. The reports are linked to the requirements to make the defect detection process simple.

The requirements are generated in a modeling tool by a requirement engineer. Then the test specification is produced by applying a consortium model translator. TAF should support the modeling tool used by requirements engineer. As a second step, the test vector generator is applied to the test specification to develop a group of test vectors. The system input values and the projected output value is enclosed in each test vector.

Then the test engineer writes the test driver schema. It contains details regarding inputs to be fed and outputs to be recovered from the system. Once the test vectors are developed and test driver schema is prepared, they have to be linked to the test driver generator. It transfers the input information contained in the vectors to the template available in the schema. The final test driver runs all the tests and stores the results.

The consistency of system behaviour with the model can be confirmed through effective tests developed by the model. The accuracy system produced by the designers is evaluated to ensure that the system is as per the requirements. Running the tests against the system does it.

Answer: [d] All the above

Module:7

Reference No:M7092

Question: The primary objective of controlling the IT funding is to

- [a] To increase revenue from IT services
- [b] To reduce costs of IT functions
- [c] Ensure adequate funding for the IT functions
- [d] All of the above

Module 2 – Control objectives for planning block

IT funding

Introduction

As in any functional area, IT also requires adequate funding for its operation. Such an activity must be accompanied by adequate control objectives. However, one specific issue concerning IT funding is that most organisations do not have system in place to track indirect costs of IT. Similarly, organisations do not have a system to track the costs involved in end-users time being spent in maintenance of their individual systems and training. It is important that the organisation establishes a comprehensive budget, which takes into consideration the total costs involved in ownership of IT infrastructure.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources

To ensure adequate funding to the IT functions	To ensure effectiveness and efficiency in the performance of the IT function	1. Establishment of total cost of ownership 2. Operational budget establishment and ownership 3. Cost and benefit analysis 4. Control over actual expenditure 5. Funding avenues 6. Technology life cycles 7. Agreement of the budget with business objectives 8. Information asset management.	• Technology • Support • The human factor

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and for IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **Operational budget:** The management should establish a budgeting process for the IT functions. The budget should be structured to satisfy the requirements of the long term and short terms plans developed by the management. Various funding avenues have to be explored to ensure that the operations of the IT are conducted in a smooth manner.
- **Cost and benefit analysis:** The management should put in place a mechanism to analyse that the costs incurred for IT activities are justified and are in tandem with the industry standards. A similar mechanism should be put in place for analysing the revenues generated by the organisation.
- **Cost and benefit review and observation:** The management should put in place a process to control the costs that are being incurred and benefits that accrue from the IT services. The process should consist of a mechanism to compare the actual costs and revenues with the budgeted figures. The variance between the same should be analysed and the cause and the remedy for the same has to be decided. The source for the actual cost should be the accounting records of the organisation. The process defined by the management should routinely record and report the costs and benefits accrued. For analysing benefits, key performance standards can be established and the actual benefits can be compared to the standards established.

II. Operational Controls

Not applicable for this activity.

Answer: [c] Ensure adequate funding for the IT functions

module:7

Reference No:M7093

Question: The overall objective of keeping an inventory of all IT components is to

- [a] Prevent any unauthorised alteration to the components
- [b] Provide for physical verification of the components
- [c] Provide a record of the changes made to the components
- [d] All of the above

Module 2 – Control objectives for implementation block

Configuration management

Introductionw2

The organisation maintains a record of all assets. This maintenance should also extend to the IT assets including software. This recording facilitates detection of any unauthorised changes to the software, control over altering the assets, their purchase, disposal and physical verification.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To provide for an effective control over the IT assets.	To ensure effective use of IT assets. Also to ensure that the assets are available for IT functions and they are reliable.	1. Inventory of assets 2. Change management process 3. Software license 4. Storage library	• Technology • Support

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and for IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **Configuration inventory:** The management should develop proper procedure for identifying and maintaining a record of all the configuration items. The record should be updated when there is an acquisition, disposal, sale or change in the configuration. The record should show the correct location at any given time. The record should contain the history of all changes.
- **Baseline:** A baseline should be identified to act as a checkpoint to return to, after the changes have been made.
- **Verification:** The procedure should incorporate physical verification. This ensures that the inventory is as per the existing items and that any discrepancies are resolved.
- **Licensed software:** The software policy of the organisation usually provides for the use of licensed software. A procedure should be defined to ensure that only authorised software is being used in the organisation. The IT managers should make use of virus detection and remedy software. A periodical check should be done to ensure compliance with the software policy, license agreements and the use of anti-virus software.
- **Storage library:** A storage library area should be defined for storage of all software under development in each stage of system development life cycle.
- **Future demands:** A procedure should exist for analysing all the future demands. This analysis should be considered when acquiring new IT assets.
- **Audit trails:** All the changes made should be properly recorded. To facilitate this process automated tools such as library management software may be used. The record should contain details of the version number, the date of creation of the software and the like.

II. Operational Controls

Not applicable for this activity.

Answer: [d] All of the above

Module:7

Reference No:M7094

Question: Which of the statements is true with regard to conversion plan for new system deployment?

- [a] It does not include system conversion
- [b] During migration, old master files need not be updated
- [c] Output of old systems are to be compared with new system output.
- [d] All of the above

Module 7 – Control objectives for implementation block

Installation of acquired/ developed system

Introduction

The installation process requires a comprehensive, formal installation plan, which must include the details of installation, migration, conversion and acceptance details.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
The solution	To ensure effectiveness of	1. Testing	• Data

satisfies the user's requirements.	the information system, ensure integrity and availability of the information system.	environment and procedures. 2. Acceptance criteria 3. Capacity and throughput analysis 4. Data conversion 5. Business continuity plans 6. Training 7. Quality plans 8. Post implementation review	• Technology • Human factor • Support

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **Implementation plans:** The implementation should contain the components of equipment installation, training, software installation and conversion procedures. All affected parties should approve it.
- **Conversion:** The conversion plan should consist of following components
 1. **System conversion**
 2. **Data conversion plans:** This should include-data collection and verifying methods, comparison of original and converted files and the master files, updating of both old master and new master during the conversion and implementation period, Verification of initial processing of the new system. The responsibility of the conversion lies with system owners.
- **Testing:** A comprehensive testing strategy should be prepared and approved by management. The testing should be conducted in an independent test environment, which is representative of the future environments. Back up plans also need to be prepared. The testing strategies should include parallel or pilot testing criterions and be performed as per them. The test should include all components and the user departments and IT functions should approve the final test results. The procedures should state that the users accept the security level and the residual risk. This should be based on the roles and responsibilities of the various IT personnel. Before migration, the user should test the operation under production environment similar to that of the new systems.
- **Training:** The operations group and the user staff should be adequately trained in the new system.

- **Performance optimisation:** Software performance optimisation plans should be developed to forecast the future resource requirements for new software.
- **Promotion to production:** The plan established for migration procedures should ensure that system owner authorisation is obtained, and the new system has been successfully operated through all production cycles. The respective environments should be properly segregated.
- **Post-implementation review:** A post implementation review of the new system should be conducted and analysed for its effectiveness within the budgetary limits.
- **Final Evaluation:** The post implementation review of the new system should also include evaluation of the system for compliance with user's requirements.

II. Operational Controls

Not applicable for this activity.

Answer: [c] Output of old systems are to be compared with new system output.

Module:7

Reference No:M7095

Question: The main objective behind variance analysis with regard to costing is

- [a] To increase revenue
- [b] To monitor costs
- [c] To increase efficiency
- [d] All of the above

Module 7 – Control objectives for implementation block

Cost Management

Introduction

Costing assumes considerable significance in the IT function framework. A process needs to be put in place to ensure that all IT costs are recorded and allocated to the appropriate IT service in the required level of detail.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To realise an accurate costing picture of the IT services in sufficient detail	To ensure efficiency in the utilisation of the IT resources.	1. Resources identification and measurement 2. Charging rules and regulations 3. Rates-charging and charge back 4. Cost reporting mechanism	• Data • Technology • Human factor • Support

		5. Revenue analysis 6. Benchmarking procedures	

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **Identification of chargeable items:** The IT management needs to establish procedures to identify those items that are chargeable are identified and measured. The IT management should obtain the guidance from the senior management in this regard. A process needs to be put in place to ensure that users are able to track and control the use of IT services and billing details.
- **Costing procedures:** A costing procedure needs to be established to provide an accurate picture of the costs and revenue information of the IT services. The procedures should contain the following components:
 1. Recording procedures
 2. Allocation procedures
 3. Definition of forecasts
 4. Comparison between actual and forecasts
 5. Variance analysis
 6. Evaluation of the costs effectiveness of the IT services

The management should periodically evaluate the results of the IT costing services with regard to other financial measurement systems adopted in the organisation.

- **Revenue billing and charge back procedures:** The management defines and establishes a user billing procedure. The billing procedure should include the following components:
 1. Billing rates
 2. Charge back rates

The rates being charged should be reflective of the costs involved in the services.

The procedure adopted by the management should encourage a fair usage of the IT resources.

II. Operational Controls

Not applicable for this activity.

Answer: [b] To monitor costs

Module:7**Reference No:M7096****Question: All system designs need to be approved by**

- [a] Only the senior management
- [b] Both senior management and users
- [c] Only the user department
- [d] None of the above

Module 7 - Control objectives for implementation block**Develop/acquire and maintain application software****Introduction**

The system development life cycle process adopted by the organisation should result in an automated solution, which satisfies the requirements of users, as well as be in line with the overall objectives of the business. The control objectives involved in this activity has been dealt in a two part series. The first part deals with management controls whereas the second part deals with operation. This is the first in the series.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
The application software, developed/acquired support the processes of business	To ensure effective and efficient use of IT resources. To ensure the integrity of the information generated by the IT solution developed and to ensure compliance with legal requirements if any.	1. The organisation's information architecture 2. SDLC methodology adopted by the organisation 3. Life cycle of the application software 4. Controls and security measures in the application software 5. Interface between user and machine 6. Software documentation 7. Testing and acceptance of developed/acquired software 8. Customisation of packages for an acquired	• Technology

		application softwares	

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

- **System design:** The SDLC methodology adopted by the management should incorporate adequate tools and techniques, which provides for user's involvement in creation of designs for any new project. It also ensures that procedure exists to ensure compliance of the design with the user's requirements.
- **Management approval:** It should be ensured that all system designs are approved by the management and the users department
- **Changes to existing system:** It should be ensured all the control objectives relevant for new system development are also observed for those projects wherein the existing systems are being modified.

Definition and documentation of file requirement: The SDLC methodology adopted by the management should ensure that a defined procedure exists for developing the file formats and maintaining related documents. Such procedure should ensure that corporate data dictionary rules are met.

- **Programming:** A detail programming specifications should be included in the SDLC approach adopted by the management. The detail specifications should comply with the system design specifications.
- **Software testing:** SDLC methodology should provide for a testing plan. The testing plan should prescribe unit, application, integration, system, load and stress testing to be performed for every system development. Testing standards should be prescribed and it should be ensured that tests performed should comply with them.
- **Consideration of Availability in application software:** The SDLC approach adopted by the management should ensure the criterion of availability has been complied with during design phase or at the earliest possible phase.
- **Re-assessment:** SDLC approach should provide for re-assessment of design whenever there is significant discrepancy occurring in the development of the systems.

Answer: [b] Both senior management and users

Module:7

Reference No:M7097

Question: The ----- provides the go-ahead approval for the projects

- [a] The project head
- [b] The user department head
- [c] The senior management
- [d] All of the above

Module 7 – Control objectives for planning block

Project management

Introduction

Every organisation needs to set up a project management mechanism to identify and maintain those projects, which satisfies the objectives of the operation plans of the organisation.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To achieve the deliverance of the project requirements in time and within budget.	To ensure effective utilisation of IT resources.	1. Involvement of management for funding and supervision of the project 2. User involvement 3. Break down of tasks, definition of milestones 4. Tracking the progress of the project with regard to milestones 5. People and cost operational budget 6. Quality assurance mechanisms 7. Risk assessment procedure 8. Personnel management 9. The level of project management capabilities in the organisation	• Technology • Support • Human factor

Specific control objectives

The specific control objectives have been categorised into management controls and operational

controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

1. **Project management structure:** A project management framework should be made mandatory for every project undertaken. The framework should at least contain the following:
 - The breakdown of the project into different tasks
 - Time and operational budget
 - Allocation of responsibilities
 - Milestones
 - Approvals
2. **Project scope definition:** Every project should have a clear-cut definition of the scope and must contain a clear-cut statement on the nature of the project.
3. **Involvements of senior management:** The senior management should study the feasibilities studies and approve the project based on its review.
4. **Involvement of users:** The project management structure should provide for the involvement of users in definition and implementation of the project.
5. **The human factor:** The structure should provide a basis for allocating responsibilities to team members and define the roles and responsibilities of each team member.
6. **Master plan:** A master plan should be prepared for each project. The plan should contain the details of scope, resource details, time frame, costing details and provide permission for measurement of progress. It should provide a basis for the control of the project for all aspects, through its life cycle.
7. **Quality assurance tasks:** The preparation of a quality plan should be made an integral part of all new systems. This should be agreed by all the parties and formally reviewed.
8. **Risk management:** All project management framework should include a risk management methodology.
9. **Testing:** A test plan should be developed for each implementation
10. **Training:** A training plan should accompany each implementation
11. **Post implementation review:** Post-implementation review should be carried out for each implementation to ascertain if the desired objectives have been met.

II. Operational Controls

Not applicable for this activity

Answer: [c] Senior Management

Module:7

Reference No:M7098

Question: The security and the control features of the application should be assessed at the time of

- [a] Programming phase
- [b] Conceptual design phase
- [c] Testing phase
- [d] Implementation phase

Module 7 – Control objectives for implementation block

Develop/acquire and maintain application software-Operational controls

Introduction

The system development life cycle process adopted by the organisation should result in an automated solution, which satisfies the requirements of users, as well as be in line with the overall objectives of the business. The control objectives involved in this activity has been dealt in a two part series. The first part deals with management controls whereas the second part deals with operation. This is the second in the series.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
The application software, developed/acquired support the processes of business	To ensure effective and efficient use of IT resources. To ensure the integrity of the information generated by the IT solution developed and to ensure compliance with legal requirements if any.	1. The organisation's information architecture 2. SDLC methodology adopted by the organisation 3. Life cycle of the application software 4. Controls and security measures in the application software 5. Interface between user and machine 6. Software documentation 7. Testing and acceptance of developed/acquired software 8. Customisation of packages for an acquired application softwares	• Technology

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

II. Operational controls

1. **Data source:** The SDLC approach adopted by the management should require that an adequate mechanism for data collection be prescribed in the system design.
2. **Input requirements:** The SDLC approach should provide for adequate inputs requirements design and documentation of the same.
3. **Interfaces-external and user machine:** The SDLC approach should provide design of all interfaces -internal and external. Adequate documentation should also be maintained for these specifications. It also should ensure that interface mechanism between the user and the system is easy and convenient.
4. **Processing requirements:** The SDLC approach should provide for adequate processing requirements, design and documentation.
5. **Output requirements:** The SDLC approach should provide for adequate output requirements design and documentation.
6. **Application software control features:** The internal control and the security features design should be made a part of the initial system design phase only. Further, the application controls should ensure the accuracy, completeness, timeliness and authorisation of the input, processing and outputs.
7. **Reference and support documentation:** Adequate reference and support manuals should be made available to users to ensure accurate operation of the systems.

Answer: [b] Conceptual design phase

Module:7

Reference No:M7099

Question: With regard to auditing project management in IT implementation, to ensure that project has delivered the required benefits the auditor should verify if

- [a] Post implementation process is part of the project management
- [b] If quality assurance plan is developed for each project
- [c] There is involvement of all categories of users
- [d] All of the above

Module 7- Audit working guideline

Project Management

Table of applicability

For IT task	Control objectives

	Management controls	Operational controls
Project management	1. Project management structure 2. Project scope definition 3. Involvement of senior management 4. Involvement of users 5. The human factor 6. Master plan 7. Quality assurance tasks 8. Risk management 9. Testing 10. Training 11. Post implementation review	Not applicable for this activity

Audit Process

The Audit process has been covered in two parts. In the first part, the preliminary understanding and analysis have been covered. In the second part, the test of controls and substantive testing have been dealt with. This article is first in the two-part series.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. Quality head 2. Project quality head 3. Organisation's quality assurance department representative 4. IT function's quality assurance department representative 5. Security management representative 6. Steering committee members 7. IT function representative 8. Project Leader 9. Project financing committee	1. Policies and procedures of • SDLC methodology • SDLC framework • Quality assurance plans and procedures 2. Project plan 3. Project quality assurance plan 4. Status reports 5. Minutes of IT steering committee meetings 6. Quality reports

Preliminary analysis

The next step is analyse the effectiveness of the control measures adopted and the degree of reliability that can be placed on the control measures. This can be done through ensuring

1. Selection and recruitment of the personnel is based on a defined criteria
2. Qualifications for new recruits are based on the requirements laid down by the relevant professional bodies.
3. Job specifications are acceptable to the management and the personnel
4. Training provided to personnel is in accordance with the defined training programme
5. Management is interested in providing the training and educating the personnel
6. Appropriate steps are taken to identify gaps between technical and management skill and to eliminate them
7. Vital IT functions have continuous cross training and back up of personnel
8. Personnel are encouraged to take leaves
9. Security policies are adequate
10. Evaluation of the personnel based on the job specifications are done at regular intervals
11. Resources are safeguarded in case of change of jobs and terminations
12. HR policies and procedures comply with the laws and regulations applicable to the organisation

Answer: [d] All of the above

Module:7

Reference No:M7100

Question: Which of the following statements is false, with regard to the audit guideline on IT funding?

- [a] The auditor should interview the project team leader
- [b] IT budgets should be based on the organisation's budgets and long term and short term plans
- [c] The auditor should test computation of variance
- [d] The auditor should identify the failures in identifying and recording actual costs

Module 7- Audit working guideline

IT funding

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
IT Funding	1. Operational budget 2. Cost and benefit analysis 3. Cost and benefit review and observation	Not applicable for this activity

Audit Process

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. CFO 2. CIO 3. IT steering committee member 4. IT management	1. Costing and budget policies and procedures 2. IT budget 3. IT Short term and long term plans 4. Roles and responsibilities 5. Business objectives 6. Reports of variance 7. Reports and minutes of steering committee meetings

Preliminary analysis

The next step is analyse the effectiveness of the control measures adopted and the degree of reliability that can be placed on the control measures. This can be done through ensuring that

1. IT budgets are based on the organisation's budgets and long term and short term plans
2. Heads of major IT units participate in the preparation of the budgets
3. The policies and procedures provide for review of actual cost and computation of variance between the actual and budgeted cost
4. IT functions provide cost justified services and are in accordance with the standard cost of the industry

Tests of controls

A clear picture of the functioning of the controls can be gained by

- Obtaining evidences
- Reviewing the deliverables

Tests: The following tests have to be done, before an opinion is formed on the functioning of IT tasks in the organisation. The following should be tested

1. IT budget is proportionate to the IT activity plan
2. Classification of IT costs are appropriate
3. Recording, processing and reporting of the IT costs are adequate
4. Computation of variance
5. Cost benefit analysis of IT functions
6. Effectiveness of cost monitoring tools

These tests ensure that control measures identified in the preliminary analysis section are in place.

Substantive testing

This step is undertaken so as to substantiate the auditor's view of controls objectives either not being met or not existing. The control weaknesses observed and its impact will have to be documented. In order to further substantiate the viewpoint

1. Comparative benchmarks, from similar organisation, industries can be identified.
2. Previous budgets, variances and the actions taken to rectify the variances must be reviewed

Identification of shortfalls

The auditor should identify:

- Inconsistency between the IT budgets and organisational budgets and long term and short term plans
- Failure to identify and record actual costs

Answer: [a] The auditor should interview the project team leader

Module:7

Reference No:M7102

Question: Before accepting the end product of contract, the ----- test should be conducted.

- [a] Integrity testing
 [b] Stress testing
 [c] User acceptance testing
 [d] All of the above

Module 7 - Control objectives for implementation block**Develop/ acquire and maintain system software****Introduction**

An established project management procedure is necessary for the appropriate technological solution. In order to identify the right solution an objective analysis of the various alternatives will have to be done. This has been dealt in two articles. This is the second article.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To provide a clear objective approach to enable the organisation to choose the right technological solution	To ensure effective and efficient way to choose the right solutions	1. Acquisition and implementation plans and procedures 2. User involvement 3. Compliance with organisation and IT objectives 4. Compliance with information framework of the organisation 5. Feasibility studies 6. Information, functional, operational requirements 7. Sustainability requirements 8. Cost analysis 9. Security and control considerations	• Technology • Human Factor • Support

		10. Vendor evaluations and responsibilities	

Specific control objectives

The specific control objectives have been categorised into management controls and operational controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls-Contd

8. **Risk assessment results:** For every technological implementation/project, risk assessment should be made a mandatory requirement before implementation. The possible security threats, vulnerabilities and its impact should be determined so as to evolve a framework of the risk assessment.
9. **Security and control considerations:** A cost benefit analysis of the security features is required to ensure that costs do not exceed benefits. Security features should be determined at the initial requirements phase itself and approved by the management and the users. Business continuity plans should also be made a part of the entire project for the continuous functioning of the selected system.
10. **Audit considerations:** The technological solution selected should provide mechanisms for adequate audit trails in order to protect sensitive data.
11. **Procurement of the selected software:** A standard procedure must be followed for procurement of selected technology, its related hardware and software.
12. **Facilities specification:** The contract with the technology vendor or the third party service provider should specify the details of the facilities to be provided. The same must be verified with tests.
13. **Acceptance of the software:** An acceptance plan should be provided and agreed upon with the vendor. The procedures should include the acceptance tests that are to be conducted and the inspections that are to be carried out.
14. **Contract Programming:** All the procedures that are applicable for in-house development should be made applicable for contract programming also. The end services should be adequately tested before being accepted and implemented by the organisation. The testing procedures should ensure compliance with the organisation's IT and quality standards. It should include all components of testing like stress testing, procedure testing, component testing, load testing, tuning and performance testing, regression testing and user acceptance testing and pilot testing.

Answer: [d] All of the above

Module:7

Reference No:M7103

Question: What is the overall objective while acquiring/developing system software?

- [a] To strike a right balance between costs and benefits
- [b] To provide a efficient and effective way to choose solutions
- [c] To satisfy user's requirement
- [d] All of the above

Module 7 – Control objectives for implementation block

Develop/ acquire and maintain system software

Introduction

An established project management procedure is necessary for the appropriate technological solution. In order to identify the right solution an objective analysis of the various alternatives will have to be done. This topic has been dealt in two articles. This is the first article.

Table of Applicability

Overall objective	Why	How	
		Operations/documentation	Resources
To provide a clear objective approach to enable the organisation to choose the right technological solution	To ensure effective and efficient way to choose the right solutions	1. Acquisition and implementation plans and procedures 2. User involvement 3. Compliance with organisation and IT objectives 4. Compliance with information framework of the organisation 5. Feasibility studies 6. Information, functional, operational requirements 7. Sustainability requirements 8. Cost analysis 9. Security and control considerations 10. Vendor evaluations and responsibilities	• Technology • Human Factor • Support

Specific control objectives

The specific control objectives have been categorised into management controls and operational

controls. Management controls include those IT activities wherein it is the responsibility of the management in defining and procedurising that activity. Management controls are also general controls applicable across the organisation and IT. Operational controls include those activities wherein the control framework defined by the management is mainly conducted through the functioning of the systems and deployment of IT resources.

I. Management Controls

1. **Selection of the system software:** The organisation should construct a standard framework to identify the system software that will satisfy the functional and organisational requirements.
2. **Information requirements:** The acquisition procedure adopted by the company should ensure that requirements for new or modified solution have been clearly and completely defined. The requirements statements should clearly specify all the functional and operational requirements, as also the security compatibility and reliability features.
3. **Identification of various alternatives:** Various alternatives should be identified, followed by an analysis of relevant parameters that is cost/benefit, technical, economical and the like.
4. **Devising an acquisition strategy:** Keeping in line with the organisational objectives and user requirements, various alternatives have to be analysed to identify the best strategy to acquire technology. The alternatives are in-house development, acquisition from external vendor, modification of existing system or the combinations of all these.
5. **Third party service considerations:** In case of third party services, it should be ascertained that their services satisfy the requirements of the organisation and should be evaluated for their effectiveness. Before accepting the software license from a third party, should be ascertained for its integrity rights.
6. **Feasibility studies**
 - Technological: Each alternative should be analysed for its technological feasibility prior to selection of the technological solution.
 - Economical: Each of the alternatives proposed should be analysed for its costs and benefits with regards to the requirements of the organisation.
 - Information architecture: The alternative or the solution selected should be in line with information architecture of the organisation. It should comply with the data model of the organisation.
7. **Information architecture:** The alternative or the solution selected should be in line with information architecture of the organisation. It should comply with the data model of the organisation.

Answer: [b] To provide a efficient and effective way to choose solutions

Module:7

Reference No:M7104

Question: Which of the following is not a problem in Groupware implementation?

- [a] Difficulty in expressing requirements
- [b] Requirements are not subject to change
- [c] Informal work practices
- [d] Specifications for systems will change even after the system's installation

Module 7 – Groupware implementation

Groupware refers to computer systems and applications such as video conferencing systems, collaborative authoring systems and group decision support systems, which support collaborative work. Implementation of Groupware systems is difficult because: -

- Its requirements are difficult to express.
- Requirements are subject to change during project implementation.
- Groupware systems aim to support work practices. Unlike work processes, which describe the methodology to work, work practices don't have any formal framework. They are based on general practices followed to complete the work. Hence, the system requirements to support these work practices cannot be defined until they are installed and tested in the real work conditions.
- Users may find new methods of system usage after the successful implementation of groupware system with their increased reference frame. Thus, system requirements are subject to change even after installation.

An evolutionary implementation approach of system design may not guarantee the correctness of the system but helps solve the above problems to some extent. In an evolutionary implementation method, organisational environment, software design issues and an approach to link the organisation and design need to be considered.

1. **Organisational Issues:** - In order to identify the impact of software design on organisation environment, the process of adaptation should be clearly understood. Adaptive Structuration Theory (AST) makes the theoretical framework of the adaptation process clear. The theory focuses on a groups' interaction with information technology. It explains how user groups adapt technological changes. . It also helps identify the key factors essential for monitoring the process.

While developing a model for monitoring the adaptation process the AST model can be linked with the following:

- *Features of technology implementation:* These refer to the size and type of the technology and the time and budget required for implementation
 - *Method of technology implementation:* It refers to the type of participation required (active or passive), tools and techniques for the project as also the size and structure of the project team.
 - *Consequences of technology implementation:* This has a reference to the effect of implementation on the company and staff and also the changes in personnel.
2. **Software design issues:** - an appropriate software design, in which a system can be decomposed into different modules, is essential to make the redesigning process flexible. Such a design is difficult to find. However, system decomposition can be done with regard to functional design.
 3. **Aligning software design:** - Software design can be easily associated with the organisational environment through the theoretical background provided by the AST approach and identifying the key variables. However, before aligning:
 - Adopt a scenario-based approach rather than a formal modelling approach.
 - Identify a technique with the available tools to effectively trace the requirements

- Develop an appropriate method to monitor and explain the changes taking place in requirements.

Answer: [b] Requirements are not subject to change

Module:7

Reference No:M7105

Question: Which of the following people should be interviewed to get the right information, while auditing the acquisition/development of application software?

- [a] Software vendors
- [b] Project staff
- [c] IT management
- [d] All of the above

Module 7- Audit working guideline

Develop/ acquire and maintain application software-1

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Develop/ acquire and maintain application software	1. System design 2. Management approval 3. Changes to existing system 4. Definition and documentation of file requirement 5. Programming 6. Software testing 7. Consideration of availability in application software 8. Re-assessment	1. Data source 2. Input requirements 3. Interfaces-external and user -machine 4. Processing requirements 5. Output requirements 6. Application software control features 7. Reference and support documentation

Audit Process

The audit process has been covered in three parts. This article is the first part, and deals with the preliminary understanding.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
1. Security management head 2. IT function head 3. Project financiers/owners 4. Chief Information Officer 5. Project owner	1. Policies and procedures of • SDLC methodology • SDLC framework 2. IT objectives 3. IT long term and short term plans 4. Detailed project documentation which includes details of each project stage, feasibility studies reports, costing reports and testing and acceptance plans

Preliminary analysis

The next step is to analyse the effectiveness of control measures adopted and their reliability. This can be done by ensuring that the following are in place

1. The SDLC approach and framework is followed while working on new projects and modifying existing systems
2. Users are involved in the requirements and design phase
3. All design specifications are approved by the senior management and the affected user department
4. The process and procedures adopted by the management comprises :
 - Definition and documentation of file-formats
 - Programme specifications for information development, which should match design specifications.
 - Data entry details correlate with data collection details
 - Definition and documentation of input requirements
 - Interface between user and the system development
 - Internal and external interface development
 - Processing requirements
 - Out put requirements
 - Control and security requirements including application controls in the initial design phase itself
 - Logical and application specifications
 - Availability, maintainability and reliability of the systems
 - Verification measures for routine tasks
 - Project testing plan and approval by user before implementation
 - Security checks for access controls or depersonalisation of old data(for sensitive information)
 - Adequate user manuals
 - Re-assessment procedure, if there is occurrence of any significant discrepancies
 - Sensitivity assessment

The next article will focus on the test of controls and substantive testing.

Reference No:M7106

Question: Which one of the following does not serve as a Minimum Acceptable Tolerance criteria for selecting software?

- [a] The basic objective of the application
- [b] Operational errors
- [c] Risk element
- [d] Management Information System Reports

Module 7- Minimum Acceptable Tolerance for Software

No company would want to purchase software that is sub-optimal in quality, but this is often the case with many companies that acquire software even from top vendors. This results in a decrease in the profits, as the subsequent costs are not added to the assets in final accounts, but are deducted from the profits.

The following criteria serve as the minimum acceptable tolerance limits for acquiring software, beyond which companies should reject the software: -

1. Give importance to the basic objective of the application: The primary objective of the application should not be sacrificed at the cost of other services because of the initial enthusiasm at the time of making the purchase. Later when the absence of the primary feature is discovered, it may cost more than the other free services provided. For instance, it may be quite obvious that an exporter may not verify the existence of an important feature - (like the feature which includes automatic checking of commission and discount on foreign bills) in the flurry of purchasing an export-specific software that is linked to export needs.
2. Don't tolerate operational errors: Errors in the operational reports may be the cause of great loss to the organisation. One way to avoid such losses is to undertake a software audit. The expenses of a software audit are far less than the costs incurred in operational errors. For instance, in a certain company, penal interests on late instalment receipts were not calculated in spite of having a parameter file in the system for the particular action. It was identified by a routine audit after two years. The reason was non-activation of the instruction logic. Hence it is essential to test that the logic and the operational reports should not be sacrificed in order to save time and labour investment.
3. Management Information System reports should be up to the mark: Often organisations do not pay much attention to errors in the Management Information Systems report, considering it as a least important. In reality it is not so. Since crucial decisions are taken by the management on the basis of MIS reports, they play an important role in the survival of a company.
4. Multiple platforms are beyond tolerance: Efficiency will be at detriment if multiple platforms are involved. Software input and output that is digitally different will not be able to effectively match the time, labour and accuracy of the software. For example, if the information produced using sophisticated software in one department is channelled to a low-end database in another department, it may result in frequent disorders. This is because the low-end software may not be able to incorporate the changes that the advanced software undertakes.

Minimum Acceptance Tolerance limits need not focus on the complete perfection of the software. Practically this cannot be achieved. They should enable companies to avoid the selection of software of a sub-standard quality and minimise the hidden cost involved.

Answer: [c] Risk Element

Reference No:M7107

Question: Which of the following statements is true with regard to auditing the acquisition/development of application software?

- [a] Data entry and data collection should tally
- [b] Data entry and data collection need not tally
- [c] Data entry and input processing details should match
- [d] None of the above

Module 7- Audit working guideline

Develop/ acquire and maintain application software-2

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Develop/ acquire and maintain application software	1. System design 2. Management approval 3. Changes to existing system 4. Definition and documentation of file requirement 5. Programming 6. Software testing 7. Consideration of availability in application software 8. Re-assessment	1. Data source 2. Input requirements 3. Interfaces-external and user -machine 4. Processing requirements 5. Output requirements 6. Application software control features 7. Reference and support documentation

Audit Process

The audit process has been covered in three parts. The first part covered a preliminary understanding and analysis of the process. This article is the second part, and focuses on the test of controls.

Tests of controls

A clear picture of the functioning of controls can be gained by:

- Obtaining evidence
- Reviewing the deliverables

Tests: Before the auditor takes a stand on the functioning of IT tasks in the organisation, he should check

1. The involvement of users in the requirement phase and design phase.
2. The procedures to ensure that all issues of the current phase are resolved before moving to the next phase.
3. All significant modification to existing systems are implemented using the SDLC approach for new projects
4. All design specifications are approved by the senior management and the affected user department before beginning the project
5. The design specification include definition and documentation of file-formats in accordance with the standards
6. Programme specifications for information development, are in agreement with design specifications.
7. Data entry and data collection details match.
8. A easy to use interface exists between the user and the system
9. Design and documentation of internal and external interface development
10. Existence of processing requirements
11. Existence of output requirements are existing
12. The design of control and Security requirements . This should be included in the conceptual phase itself.
13. Involvement of the security officer in the design phase and development phase
14. Applications should have provision for automatic verification of the tasks performed.
15. The design of mechanisms to provide availability, maintainability and reliability of the systems
16. Existence of a Project testing plan approved by the user
17. Existence of user support manuals
18. Existence of the help desk function to assist users
19. Updation of user documents
20. Re-assessments are conducted in case of significant deviations.

Answer: [a] Data entry and data collection should tally

Reference No:M7108

Question: Which of the following does the auditor have to review(during acquisition / development) to ensure the availability of application software?

- [a] System design of projects
- [b] User requirement statements
- [c] Specifications statement
- [d] All of the above

Module 7- Audit working guideline

Develop/ acquire and maintain application software-3

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Develop/ acquire and maintain application software	1. System design 2. Management approval 3. Changes to existing system 4. Definition and documentation of file requirement 5. Programming 6. Software testing 7. Consideration of availability in application software 8. Re-assessment	1. Data source 2. Input requirements 3. Interfaces-external and user -machine 4. Processing requirements 5. Output requirements 6. Application software control features 7. Reference and support documentation

Audit Process

The audit process has been covered in three parts. The first and second parts deal with the preliminary understanding, analysis, and test of controls. This concluding article focuses on substantive testing.

Substantive testing

This step is undertaken to substantiate the auditor's viewpoint that control objectives are either not being met, or do not exist. The shortcomings in controls and its consequences also should be documented. He can also:

1. Identify benchmarks from similar organisations/ industries
2. Use industry best practises or international standards to review the adequacy of the system development approach.
3. Perform a detailed review of:
 - The system design documentation to evaluate the adequacy of the same
 - Approval from management and relevant user departments
 - Software documentation to ensure that a organised file documentation exists and is structured in accordance with user and system requirements.
 - New system implementation projects, to ensure that all system programmes, interfaces, input, output, processing, data collection mechanisms are as per approved design.
 - The projects to check for any technical discrepancies
 - The projects to ensure the adequacy of internal control and system designs
 - Data integrity verification is conducted by the application
 - User reference materialsto verify if they are being updated .
 - The effectiveness of the programme with regard to - input, processing, interface specification process, and output specification process and the testing standards and its compliance.

Identifying shortcomings

The auditor should identify

- Deficiencies in SDLC methodologies
- Designs that do not meet user requirements
- File requirements that do not meet the requirements of data dictionary rules
- Poorly designed file, input, output, interface and processing specifications.
- Projects wherein availability has not been considered.
- Projects wherein the data integrity verification routines have not been incorporated into the applications.
- Deficient organisation standards
- Inadequate user and support manuals

- ☐ Significant discrepancies that did not result in re-assessments of projects.

Answer: [d] All of the above

Reference No:M7112

Question: With regard to auditing the process of acquisition/development of system software, an erroneous technological feasibility study may lead to

- [a] Difficulties in the implementation of the originally designed solution
- [b] Selection of alternative solutions which are expensive
- [c] Selection of alternative solutions which are highly risky
- [d] All of the above

Module 7- Audit working guideline

Develop/ acquire and maintain system software-4

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Develop/ acquire and maintain system software	1. Selection of system software 2. Information requirements 3. Identification of various alternatives 4. Formulation of an acquisition strategy 5. Third party service considerations 6. Feasibility study: technological and economical 7. Risk assessment results 8. Security and control considerations 9. Audit considerations 10. Procurement of the selected software 11. Facilities specification	Not applicable for this activity

	12. Acceptance of the software	
	13. Contract programming	

Audit Process

The audit process has been covered in four parts. The first three parts covered the preliminary understanding, preliminary analysis and test of controls. This article is the fourth part, and focuses on substantive testing.

Substantive testing

This step is undertaken to substantiate the auditor's viewpoint that control objectives are either not being met, or do not exist. The shortcomings in controls and its consequences also should be documented. He can also consider the following points:

1. Comparative benchmarks from similar organisations, and industries can be identified.
2. Industries' best practises or international standards can be utilised to review the adequacy of the risk assessment approach.
3. The auditor needs to perform a detailed review of the-
 - Security, internal control and audit trails of the systems
 - The selection of the software and implementation of the same
 - Compliance with the organisation's procurement policies and procedures
 - Third party service management
 - Monitoring of contract programming
 - The facilities acceptance process to ensure that environments and accommodation tests are conducted

Identifying shortcomings

The auditor should identify

- Deficiencies in SDLC methodologies
- Projects that do not meet user's requirements
- Expensive alternatives selected
- Highly time consuming projects
- Erroneous economic/technical feasibility studies
- Inadequate Risk assessments
- Improper/inadequate control features and audit trails

- ☐ Absence of user-friendly designs
- ☐ Non-compliance with the organisation's policies and procedures for vendor selection and management
- ☐ Non-compliance with the third party services agreement
- ☐ Non-compliance with contract programming terms and conditions
- ☐ Products which were accepted without adequate facilities testing, system testing, and accommodation testing
- ☐ Products which were accepted without technology and functionality testing and work load trails
- ☐ System failure
- ☐ Non-compliance with the contract terms and conditions

Answer:[a] Difficulties in the implementation of the originally designed solution

Reference No:M7113

Question: Which of the following resources need not be considered as a cost to be charged to users?

- [a] Hardware
- [b] Development of applications
- [c] Communication channels
- [d] All of the above

Module 7 – Audit working guideline

Cost management Part 1

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Cost management	1. Identification of chargeable items 2. Costing procedures 3. Revenue billing and charge back procedures	Not applicable for this activity

Audit Process

The audit process has been covered in two parts. This article is the first part, and deals with a preliminary understanding and analysis of the process.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
IT cost team Users	1. Policies and procedures with respect to ▪ Resources identification and measurement ▪ Charging rules and regulations ▪ Rates- charging and charge back ▪ Cost reporting mechanism 2. Organisation policies and procedures relating to budgets 3. Documents - IT functions ▪ Budgets - present and the previous year ▪ Allocation of resources ▪ Data used ▪ Method of allocating cost ▪ Any other relevant reports 4. Documents - users ▪ Budgets - present and previous years ▪ Current IT plans 5. Allocation of resource for IT functions , including functions that are charged back and absorbed

Preliminary analysis

The next step is to analyse the effectiveness of the control measures adopted, and their reliability. This can be done by ensuring that:

- The management has defined and established a user billing procedure for the IT functions.
- The management has developed procedures for
 - o Developing yearly plans, criteria for prioritisation of activities and maintenance of plans.
 - o Creating budgets for different IT resources and ensuring that the budgets comply with overall organisation budgets.
 - o Allocating costs of the user department.

- o Communicating to users the components of revenue bills.
- o Approval of budgets by the users and periodicity of delivering reports .
- The use of IT resources to be charged should include usage of
 - o Hardware
 - o Development of applications
 - o Communication channels
 - o Peripherals
 Beside the above other indirect cost that can be included are administrative cost, help desk facility, maintenance cost, vendor service cost and any other relevant costs.
- Users are provided with reports on the performance of cost centres, assessment of organisation cost with the industry standards and t changes in the cost components.
- Cost allocation method are in line with the changing requirements of the business
- Opportunities for reducing charge backs have been identified

The next article focuses on the second part - the test of controls and substantive testing.

Answer: [d] All of the above

Reference No:M7114

Question: Which of the following should the auditor check out to decide on the costing method of the organisation?

- [a] The process of allocating cost and its acceptance by the management
- [b] The process of charging rates in keeping the costs involved in providing the services
- [c] The process of allocating costs to external users only and not to internal users
- [d] All of the above

Module 7 – Audit working guideline

Cost management Part 2

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Cost management	1. Identification of chargeable items 2. Costing procedures 3. Revenue billing and charge back procedures	Not applicable for this activity

Audit Process

The audit process has been covered in two parts. The first part covered a preliminary understanding and analysis of the process. This article is the second part, and focuses on the test of controls and substantive testing.

Tests of controls

A clear picture of the functioning of controls can be gained by:

- Obtaining evidence
- Reviewing the deliverables

Tests: Before the auditor takes a stand on the functioning of IT tasks in the organisation, he should check

- Method for allocation of cost and its acceptance by the users
- Existence of cost improvement techniques
- Performance of the IT resources
- Delivery of reports and ensure effective and efficient utilisation of IT resources
- Allocation of resources to the user department
- The rates being charged- is in line with the costs involved in providing the services.

Tests should be performed to ensure that control measures identified in the preliminary analysis are functioning as desired.

Substantive testing

This step is undertaken to substantiate the auditor's viewpoint that control objectives are either not being met, or do not exist. The shortcomings in controls and its consequences also should be documented. He can also:

1. Identify comparative benchmarks from similar organisation and industries.
2. Confirm the charge back, by calculating from raw data to the final figures in the report
3. Ensure that the performance reports reflect the usage of CPU and peripherals, lines of code program written and printed, changes made in the programs, the number of enquiries at the help desk, number of transmissions and the like
4. Check if charge backs are tested regularly to ensure that the calculations are correct
5. Verify consistency between the charge backs of different users
6. Review distribution process of reports

7. Assess user satisfaction with regard to charge backs and the budgeted figures, progress of development plans and charge backs, benchmarking of charge backs against different alternatives and the like

Identifying shortcomings

The auditor should identify:

- ☐ Opportunities to improve the effectiveness and efficiency in the cost methodology and use of resources
- ☐ Non-inclusion of certain cost items in the charge back
- ☐ Alterations (if any)made to the cost allocation methodology
- ☐ Allocation of cost between equipment and applications
- ☐ Inappropriate allocation of cost among different users
- ☐ Prospect of using IT resources to meet the business needs of the users
- ☐ Prospects of improving the performance by enhancing the efficiency in the process of collecting, gathering, allocating, communicating and reporting on costs
- ☐ Cost variances
- ☐ Profitability of IT functions in delivering services to both internal and external users ,and in the light of the budget

Answer: [b] The process of charging rates in keeping the costs involved in providing the services

Reference No:M7115

Question: Which of the following documents is not relevant for an auditor for obtaining an understanding on the configuration management?

- [a] Configuration inventory
- [b] Offsite storage inventory
- [c] Policies and procedures for acquisition, maintenance and disposal of equipments
- [d] Development of applications

Module 7 – Audit working guideline

Configuration management Part 1

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls

Configuration management	1.	Configuration inventory	Not applicable for this activity
	2.	Baseline	
	3.	Verification	
	4.	Licensed software	
	5.	Storage library	
	6.	Future demands	
	7.	Audit trails	

Audit Process

The audit process has been covered in two parts. This article is the first part, and deals with a preliminary understanding and analysis of the process.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel		Document	
1.	Operations team	1.	IT policies and procedures related to
2.	Application development team	▪	Configuration acquisition, maintenance and their disposal
3.	Support and facilities team	▪	Quality assurance
4.	Software vendors employees	▪	Change control
5.	Asset management team	2.	Organisation policies and procedures with respect to
6.	Quality assurance team	▪	Purchase, rent or lease of equipment and software
		▪	Acquisition, maintenance and disposal of equipments and software
		▪	Use of licensed software
		3.	Inventory of configuration both onsite and offsite related to
		□	System software
		□	Application software
		□	Hardware
		□	Facilities
		□	Data
		4.	Configuration baseline information

	5. Documents related to □ Inventory of fixed assets □ Equipments on lease □ Changes to configuration of the systems 6. Inventory of library resources - test, development and production results 7. Offsite storage inventory □ Equipments □ Data □ Manuals and the like
7.	8.

Preliminary analysis

The next step is to analyse the effectiveness of the control measures adopted, and their reliability. With respect to configuration it is necessary to ensure that

- A process exists for creating and maintaining the baselines for configuration
- A configuration procedure is in place and provides for maintaining the integrity of the configuration
- There is a proper authorisation system for making the required changes
- Process exists for determining whether the procedures for documenting the configuration is adequate
- Personnel have the required skills and expertise
- Access to software baselines are reviewed periodically and appropriate actions taken to rectify errors, if any
- Accounting records are reconciled with the actual inventory on a periodical basis
- Changes are recorded and maintained
- Configuration reports reflect the applications migrating from development to testing environment and from testing to production environment

Answer: [d] Development of applications

Reference No:M7116

Question: Library management software helps in which of the following?

- [a] Documenting the changes that are made to program
- [b] Controlling the version numbers of the programs

[c] Generating the reports on changes made to programs

[d] All of the above

Module 7 - Audit working guideline - Configuration management Part 2

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Configuration management	1. Configuration inventory 2. Baseline 3. Verification 4. Licensed software 5. Storage library 6. Future demands 7. Audit trails	Not applicable for this activity

Audit Process

The audit process has been covered in three parts. This article is the second part, and deals with a preliminary understanding and analysis of the process.

Preliminary analysis (contd..)

The next step is to analyse the effectiveness of the control measures adopted, and their reliability. This can be done by ensuring that the following are in place

- All the software must be labelled and an inventory maintained of them
- With respect to software change controls, procedures must exist for
 - o Maintaining a library of application programs
 - o Restricting the access to the library
 - o Determining the dependability and integrity of software inventory. This is to ensure the use of licensed software only.
 - o Detecting the use of unauthorised software, if any. The management must be informed for appropriate action.
- As regards the software storage, the following are necessary
 - o Storage of all the software
 - o Separate storage library for different stages of development of software
 - o A separate area to store sources that are moving to production environment
 - o Owner for each software
 - o Clearly defined access controls
 - o An established audit trail
 - o Detection procedures for instances of violation prescribed code. The same must be

- documented and reported to the management
- o Assessment of appropriate action undertaken to rectify the violation
- Library management entails use of appropriate software. It should be considered whether the library management software is used for
 - o Documenting the changes that are made to the program
 - o Controlling the version numbers of the programs
 - o Generating the reports on changes made to programs

Besides the above there are certain general analysis that the auditor should carry. These pertain to

- Processes for maintaining the status on the resources that are purchased and leased.
- Configuration baseline reflects the changes that are made to the applications, quality and operations.

The successive articles focus on test of controls and substantive testing.

Answer: [d] All of the above

Reference No:M7117

Question: On which of the following should the auditor perform substantive testing with regard to configuration management?

- [a] Review of the configuration records
- [b] Review of incidents reported to senior management
- [c] Review of the training manuals
- [d] All of the above

Module 7 – Audit working guideline – Configuration management Part 3

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Configuration management	1. Configuration inventory 2. Baseline 3. Verification 4. Licensed software 5. Storage library 6. Future demands 7. Audit trails	Not applicable for this activity

Audit Process

Audit process has been covered in two parts. The first part deals with the preliminary understanding and preliminary analysis. Preliminary analysis is dealt in detail in the second part. The concluding part deals with the test of controls and substantive testing.

Tests of controls

A clear picture of the functioning of the controls can be gained by

- Obtaining evidences
- Reviewing the deliverables

Tests: The following tests have to be done, before an opinion is formed on the functioning of IT tasks in the organisation. Such tests pertain to various aspects viz., baseline configuration, unauthorised software, software storage and reporting.

- In baseline configuration, it must be ensured that Baseline configuration is defined
- Procedures for recording, changing and approval of the same by the management are defined
- Actual status on the configuration of the assets is reflected in configuration records
- Records are reviewed by the management at appropriate intervals
- Policies and procedures are defined for configuration reporting
- Standards for the performance of maintenance of configuration and reporting are complied with
- Configuration baseline is compared at regular intervals with the inventory records of the equipment and resources

As regards unauthorised software it must be ensured that

- Policies and procedures exist for detection of use of unauthorised software
- Personnel understand the significance of authorised software and that appropriate training is provided.
- Personnel have signed the forms for compliance with the procedures
- Software are centrally controlled
- Software are reviewed on a continuous basis, violations are reported and appropriate actions are taken

For software storage it must be ensured that

- Storage libraries are defined

- Storage of programs and source code for all the programs are defined during their development

Reporting entails

- Collecting and processing information for reporting

Tests should be performed to ensure that the identified control measures in the preliminary analysis section are functioning as desired.

Substantive testing

This step is undertaken so as to substantiate the auditor's view of controls objectives either not being met or not existing. The control weaknesses observed and its impact will have to be documented. In order to further substantiate the viewpoint

- Review of the frequency at which the configuration records are reviewed by the management and reconciliation of the various records
- Examination of the libraries using a software to duplicate software, missing object codes and deleting the data, files and programs that are not required

Identification of shortfalls

The auditor should identify:

- Lack of awareness among the personnel on configuration baseline
- Ineffectiveness and inefficiencies in baseline configuration procedures
- Inappropriate reflection of the changes made by the vendors in configuration records

Answer: [a] Review of the configuration records

Reference No:M7118

Question: Which of the following should a company look into prior to reengineering a product?

- [a] Compliance with ethical issues
- [b] Infringements that might occur in the high-risk area of the product
- [c] Patent owner's awareness of reverse engineers' intention
- [d] All of the above

Module 7 – Ethical and legal issues involved in Reverse engineering:

Introduction:

'Reverse engineering' is a widespread practice in software engineering that involves disassembling, inspection and study of a product to identify its underlying strengths and weaknesses, so as to make

a replica of it or to enhance the existing system. In general, reverse engineering is adopted for building similar products with enhanced performance and productivity (in terms of cost of manufacture and maintenance).

Normally, to buy a product and study its intricacies for developing a similar product albeit with improved features is considered as legal and ethical. However, the reverse engineering processes should conform to the clauses that govern the patent rights of a company.

Some of the legal and ethical issues involved in reverse engineering and their solutions are discussed below:

- *Does purchasing a product from one manufacturer and sending it to another for reverse engineering violate legal strictures?*

Buying a product from one manufacturer and giving it to another manufacturer for the purpose of reengineering does not violate any legal strictures. However, such an act could amount to being unethical. The correct way is to directly buy the product from the manufacturer for reengineering without involving a mediator for this purpose. In other words, the supplier interested in reengineering a product should buy it from its manufacturer, revealing his intention behind the purchase prior to reengineering. Further, legal issues will arise if protected data is being replicated or being processed without prior consent.

- *Is it legally acceptable to buy a product from a manufacturer who has imitated its patented version and may be violating the copyrights?*

By and large, purchasing contracts tend to protect the buyer. However, it is better to avoid buying a product, which infringes the copyrights of the original manufacturer (i.e. a deliberated purchase of an infringing product may pull the buyer into legal complications and there is every chance of him being legally sued)

- *Does such an act conform to the values of the company?*

The reverse engineering process, should comply with the values of the company. In other words, when it is the turn of the company (that reengineers the legacy system), it should be able to handle infringements of its patent (the reengineered one), since every competitive product in an open market becomes an inspiration for reengineers.

How to go about it then? Considering the above legal and ethical issues, if the company decides to reverse engineer a product, then it is advisable to acquire the consent of the owner. This can be done by an out-and-out purchase of the product in the open market. A second option would be to arrive at an understanding with the patent owner prior to the reverse engineering process, so that the latter is well aware of the intention behind such purchase. Further, during the course of the reverse engineering process, the company should be watchful about imitating or disassembling a protected part of the product, which is also known as the high-risk area.

Answer: [d] All of the above

Reference No:M7119

Question: A reengineering project may fail due to ?

- [a] Lack of proper observation and assumptions
- [b] Lack of training for the workforce
- [c] Inadequate documentation of requirements of the target system
- [d] All of the above

Module 7 – Shortcomings in a reengineering process- Part I:

What is reverse engineering or reengineering?

Reverse engineering or reengineering involves separating the components of a system and observe it's working with an intention of creating its replica or improving upon the original product. For example, in the refrigerator industry, a manufacturer may buy a product from his competitor; disband it to examine its make for enhancing the original refrigerator with similar parts.

Risks involved in reverse engineering:

Reengineering brings with it the benefits of revealing the strengths and weaknesses of a product so as to develop a better product. But at the same time it can prove unsafe if the risks involved in it aren't evaluated and acted upon.

Following risks in reengineering may lead to failure of a project:

1. *Incomplete or fallible reverse engineering approach:* Strategies in reengineering may be faulty due to lack of in-depth observation and poor assumptions. Lack of proper attention may lead to concentrating on a wrong problem. This in turn leads to a flaw in the reengineering strategy. E.g. company may be uncertain about replacing a part of the parent product or renovating it. This hampers architectural decisions at the subordinate level, eventually affecting the overall reverse engineering process. In other words, the end product will head for a failure if the steps are not taken at the initial stage of the process.
2. *Employing inappropriate consultants outside the firm:* Usually outside contactors and consultants are employed for proper understanding and technical know-how of the product. The consultant should be hired based upon the experience and technical expertise. It is also necessary for the consultants to have similar views and interests on various issues, say for example cost cutting. Thus, it is always prudent on the company's part, not to give complete control to a single outside contractor. Also, the company should remain alert for any problem.
3. *Insufficient training programs:* By and large, reengineering processes fail due to lack of proper training for the reverse engineering personnel. The work force must be well aware of the frequent updates in the hardware and addition of new programming syntax. Understanding new technologies and programming methodologies becomes difficult for a person who hasn't been upgrading his skills.

Ideally, a training programme should:

- ☐ Identify the needs of the trainee
 - ☐ Check expenditure and time involved in the training
 - ☐ Check whether the trained members are competent enough to lead a team.
4. *Lack of proper control over the parent (legacy) system:* Lack of proper knowledge about the parent system (or the legacy system) leads to inadequate understanding of system maintenance costs, cost incurred in changes, defects in the legacy system and long-term project planning. Lack of control is caused due to inadequate documentation, change control processes and track records for changes. It is important to maintain the record of all kinds of changes made, costs incurred in making the changes and the impact caused by the changes, without which long-term projections are highly unfeasible. As a result, the release of the end-product (or the final product) is delayed.
5. *Lack of validation of requirements:* Generally, there is very little or no substantiation for the concept of the target system (i.e. the derived one). Consequently, a well-documented requirement list (which includes hardware and software requirements, architecture requirements, maintenance and cost requirements and so on) for the target system is absent. The prime reason for this is taking the requirements of the legacy system for granted (and not planning it all over again for the target system). Some more issues have been discussed in Shortcomings in a reengineering process-part I.

Answer: [d] All of the above

Reference No:M7120

Question: A complicated legacy system cannot be taken as a model for the target system because

- [a] Inadequate understanding of the concept will lead to inadequate documentation
- [b] Inadequate knowledge would mean incurring expenditure to train the workforce
- [c] Understanding and enhancing a complicated legacy system is not viable
- [d] The management will lose control over the reengineering process

Module 7 – Shortcomings in a reengineering process- Part II:

What is reverse engineering or reengineering?

Reverse engineering or reengineering refers to disassembling a product and observe it's working with an intention of creating its replica or improving upon the original product. For example, in the refrigerator industry, a manufacturer may buy a product from his competitor; disband it to examine its make for enhancing the original refrigerator with similar parts.

The previous part discusses issues related to the following:

- Incomplete or fallible reverse engineering approach
- Employing inappropriate consultants outside the firm
- Insufficient training programs
- Lack of proper control over the parent (legacy) system
- Lack of validation of requirements

The remaining issues discussed in this article that are as follows:

1. *Improbable software architecture of the legacy system:* At times, the architectural structure of the legacy system that is taken as model (check) for enhancement is too complicated or not viable. In such cases, the technical design of target system doesn't comply with that of the parent system, eventually leading to improper understanding of the end product. Unless the legacy system is well conceived, implementing the target system is not possible. It is very essential that the basic building blocks of the legacy system are comprehensible.
2. *Absence of a specific and distinct perception of an ideal reverse engineering process:* The evolution of the legacy system, to a large extent influences the reengineering process. By and large, a proper documentation of the legacy system is mistaken for substantiation for a reverse engineering process. On the contrary, a well-documented legacy system can only be an inspiration for the outcome of a reverse engineering process, not implementation as a whole. In fact a proper set of processes/steps is to be planned before reengineering process of a product is taken up, in the absence of which the reengineering process fails. Apart from the technology used, quality people employed and the resources on hand, a proper quality process also has to be followed to complete the reengineering process.
3. *Improper planning to overcome the shortcomings in a reengineering process:* One of the major requisite for reengineering is project planning. Often in the presence of the legacy system, the intermediate level is neglected and attention is given only to the low level (i.e. coding part). This creates confusion in the vision of the target system to be developed.
4. *Lack of continuing dedication from the management:* Only, dedicated effort at the management's end in keeping the whole process in control can see a reengineering process through completion. Errors in initial stages (i.e. during the designing of the building blocks of a software), often leads to a complete failure. When the management lacks dedication, the whole workforce loses focus, thereby leading to deterioration of the project. If the management delegates full responsibility to the lower level managers, they tend to divert the project from the focussed objective of the reengineering process, resulting in a devastating outcome.
5. *Preset technical specifications for the target system:* A set of fixed directive or mandates preset or predetermined by the management establishing constraints on technical approach, cost, schedule and performance, without taking into consideration the opinion from the workforce at the lower levels often causes a reengineering process to fail. On one hand when a well-documented form is soul of the reverse engineering process, on the other hand it is equally risky to rely on a document that doesn't consider the approval of the team in setting goals for the project.

Answer: [c] Understanding and enhancing a legacy system is not viable

Question: Which of the following steps is not involved component based software development?

- [a] System evolution
- [b] Component qualification
- [c] User requirement analysis
- [d] Component adaptation

Module 7 – Component Based Software Development (CBSD):

Introduction

Component-based software development refers to the process of developing large software systems by putting together, the components of already-existing software. This is done to make the software system more flexible and easy to maintain. This technique cuts down the development and maintenance costs. Further, assembling upgrading and supporting the system become less cumbersome. While building the basic building blocks of the software system, it is assumed that some parts of large systems are often recurrent. Hence, such parts should be coded (or written) only once, so as to reuse and reassemble the code instead of writing it all over again. Component-based systems include both COTS (Commercial off-the-shelf) products and the components of non-developmental products.

COTS (Commercial off-the-shelf) refers to readymade things that can be bought from a manufacturer's virtual shelf. Thus an already developed component can be integrated for developing the new system, at a cheaper rate. Such availability makes integration in large software systems easier and faster.

Why CBSD is becoming popular? The availability of a diverse range of COTS makes development of component-based systems viable. Further, the improved quality of COTS, high costs of system development & maintenance, and the growing reusability of already-existing software components in the industry, has paved way for the rise in the use of CBSD.

CBSD lays foremost emphasis on *composing software* rather than developing software.

Steps in CBSD:

Four major steps in component-based software development are discussed below:

□ **Component Qualification:** Component qualification, also known as *suitability testing* involves examining whether an already-developed product can be employed for developing a new system. Selection of the appropriate product (component) is done after taking all the competing products available in the market into consideration. Further Component qualification also ensures that the algorithms (employed in CBSD) have been validated. *Component qualification* is a two-staged process, namely- *discovery* and *evaluation*. In the *discovery* stage, the characteristic features of the component such as its interface, reusability, dependability on the product, functionality and so on, are identified. This is not a well-defined process and is often thwarted by complexities in identifying the intricate information about the component prior to its integration with the new system. To standardise the component qualification study, *evaluation*, which is a more refined approach, is adopted. Internationally accepted standards (prescribed by the ISO) for product evaluation guide the evaluation process. *Evaluation* process, involves paper-based studies of

the various components. It takes into consideration, the opinion of the users of the component before developing a prototype.

□ Component adaptation: Component adaptation refers to acclimatising the component to the new system. Every component is designed and developed to meet different needs. Hence, it is very important to ensure these components get along well with the new system. The three different approaches employed in *component adaptation* are *white box*, *grey box* and *black box*. These approaches differ from each other in the extent to which they make the internal code of a component accessible. E.g. a white box approach allows accessing and rewriting the internal code of the component so as to make it compatible with the new system. A black box approach makes the internal code inaccessible, limiting the use of the code only to execution. Since white box approach allows modification of codes, it leads to increase in developing and maintaining costs.

□ Component assembling: Individual components are integrated using a definite and distinct architecture. Various examples of infrastructure employed for assembling are database (that controls all the operational data centrally), message bus (that has separate data stores to notify changes in the components) and so on.

□ System evolution: System evolution involves repairing the errors in the component, updating them, and transforming them into reusable units. Further, any additional functionality that may be required is incorporated in a new component and added in the system.

Answer: [c] user requirement analysis

Reference No:M7122

Question: Which of the following processes is the same for both RAD and SDLC?

- [a] Concept definition
- [b] User requirement definition
- [c] Rapid prototyping
- [d] Iterative approach

Module 7 - How RAD surpasses traditional approach of Software development:

Introduction

The changing needs of a business, calls for a faster approach of software development. With the expansion of the market, the information requirements also change rapidly, thereby inducing the need for faster changes and updates in the information systems. The traditional approach i.e. the SDLC (System Development Life Cycle), also known as the waterfall approach, falls short of coping with the rapid changes in system requirements. Such limitations in SDLC has paved way for Rapid Application Development (RAD). RAD reduces development costs and time.

A Comparative assessment of SDLC and RAD

□ *Developmental phases of the two approaches:*

SDLC (System Development Life Cycle)	RAD (Rapid Application Development)
Concept definition (feasibility analysis)	Concept definition (feasibility analysis)

User requirement definition	Implementation of a skeletal system
System design	User evaluation and concept refinement
Implementation	Implementation of refined requirements
Integration and testing	User evaluation and concept definition
Acceptance installation	
Maintenance	

□ *Underlying concept of the two approaches:* SDLC starts off with user requirement specification prior to any other step, i.e. in SDLC the requirement specification is done much before the commencement of the project. This leaves less or no scope for changes in requirement analysis, during the course of system development. While on the other hand, RAD initially, develops a prototype / model of the system to be designed and it provides adequate room for improvising the requirement specification (which can be evidently seen in the second, fourth and fifth steps of RAD)

Further, in SDLC, the system design phase (which establishes the features and functions in detail using process diagrams and pseudocode) is rigid, while in RAD prior to system design, re-evaluation of end user's requirement is carried out thereby ensuring that the project does not deviate from the primary objective.

□ *Merits and demerits of RAD and SDLC:* Due to the shortcomings in the SDLC approach, RAD was sought for as a replacement.

Unlike the SDLC, RAD offers a faster approach to software development with better quality.

- SDLC is a slower process when implemented. On the contrary RAD is fast in developing a system, since it uses iterative prototyping (i.e. uses tools like Object oriented System design - OOSD, Joint application development-JAD, and Computer Aided Software Development-CASE). These tools allow reusability of code, and faster software modelling.
- SDLC is too extensive and leads to high costs of developing and maintenance, therefore is incompetent in developing medium scale systems with low budget. On the contrary, RAD cuts development and maintenance costs.
- SDLC assumes that the user requirement can be ascertained at the very beginning of the project and it remains unchanged during the course of project, which is not the case. User requirements keep changing and often need to be modified. RAD involves the user in various workshops and end-user meetings in order to re-evaluate the requirements, thus is flexible to changes.
- However, RAD requires dedicated team effort as a major part of a RAD process rests on informal evaluation and there is no rigid set of rules defining each phase. Thus, RAD would not be feasible for a large system. On the contrary, SDLC is reliable in developing extensive systems as the processes followed in SDLC are comprehensive and exhaustive, larger systems can be developed with greater accuracy.

Answer: [a] Concept definition

Explanation: Both RAD and SDLC start off with feasibility. RAD proceeds by implementing an informal model (a skeletal model) while, an SDLC progresses in refining user requirements and then goes for implementation.

Question: Which of the following is "TRUE" with respect to audit of software licensing?

- [a] Management need not have a license to run the software
- [b] All the employees of the company should be entitled to use the software
- [c] Procedure should exist for identifying which software is obsolete
- [d] There should be no restriction on using the software

Module 7 – Audit of Software Licensing

Software refers to various kinds of programs that are required to operate the computer and related devices. The management must ensure that the software used by the company are either licensed or are free software. In this article we focus on audit of licensed software. (Refer our article on software policy)

We shall categorise the audit of software licensing into three phases - pre-audit, audit and post audit.

Pre-audit

Inventory of the software: The auditor should obtain a list of all authorised software that is used in the organisation from the management. It should include the details regarding the

- Software, its version number and the platform on which it can run
- Number of persons entitled to use the software at a time or number of copies purchased
- Date of purchase
- Any updates done and the date on which they were done or modifications
- Proof of licence - The evidence should be substantial enough for the management to be something which the management can prove that they have a right to use of using the software
- Details of the systems on which the software is used
- Restriction on using the software, if any
- Maintenance agreement

Policies and procedures: Policies and procedures related to the software acquisition should be obtained to gather information on the management's guidelines on using personal software or other software that can be downloaded from the Internet and the like. He should also obtain the results of management's test on compliance with the policies and procedures, circumstances where there was non-compliance, the actions taken and the like.

Audit

Risks and their measurement: With respect to risk and their measurement the auditor should review whether

- Software purchase, its distribution , and control include an element of risk. If yes, whether a risk assessment has been made
- Risk factors that are identified by the management are appropriate
- Results of cost/benefit analysis

Compliance: The auditor must ensure that policies and procedures defined by the management are adhered to. He should ensure that

- Techniques are implemented for monitoring the compliance with the policies and procedures
- Actions taken in case of non-compliance where appropriate
- Actions taken where documented and distributed to the required users
- Where required, the non-compliance was escalated to senior management
- Instances, where the management has not implemented any techniques to ensure compliance, the auditor should conduct the compliance test

Security: The authorised software should be adequately secured by implementing both physical and logical security. The security should also extend to copyrights, license and the like. The auditor should determine the adequacy of the security methods that are implemented.

Obsolete software: The software that is no longer required or is not in use can be disposed off. Depending on the agreement with the licensor the organisation can sell, transfer or dispose of the software. The sale or transfer should include transfer of all media on which software is stored, license, and manuals. It should also be ensured that software is deleted from the computer systems and back ups. The following should be ensured with respect to obsolete software

- Process of identifying which software is obsolete
- Person responsible for identifying it
- Method of disposal
- Review of records of disposal

For the conduct of audit the auditor can use the commercial software that are available.

Post-audit: The auditor should ensure that his findings and recommendations are considered by the management and implemented where appropriate.

Answer: [c] Procedure should exist for identifying which software is obsolete

Reference No:M7124

Question: Which of the following is not security issue related to the offshore development?

- [a] Loss of adequate control
- [b] Difference of opinions between the client and the offshore developer
- [c] Increase in the complexity of the network
- [d] Increase in the revenue of the vendor

Module 7 – Offshore development and the related security issues

There has been a tremendous growth in the Indian software market. The main reason behind this is Offshore Development projects undertaken by the Indian software companies or Offshore development centres (ODC) as they are called by the outsourcers of the software. Many developed countries outsource their development activity to Asian countries owing to low development costs, availability of trained personnel and the like.

ODC may develop software for various companies or may cater to the needs of single company. The analyst of the client states the system specifications and requirements. The programs and codes are generated by the ODC. ODC can be connected to the client either through the Internet, a leased line or virtual private network. This leaves scope for vulnerabilities to creep in. Vulnerabilities could range from viruses, intrusions or unauthorised access into sensitive information of the client and the like.

Security risks related to Offshore Development

Every company is required to assess their threats and take counter measures to overcome them. The threats could be from outside the company like denial of service, networking intrusions or could be inside the company like fraud, sabotage by disgruntled employees and the like. However it may not be possible to take measures to prevent all the risks. The company should assess the estimated loss of each risk and decide on the level of risk it can tolerate. The investment in security should be proportionate to the risks.

Some of the main risks associated with the offshore development are

- Inadequate control: When a company out sources the development of software it has very less control about the conditions in which the software is developed. Also the company needs a regular communication with the ODC. This creates hardships for the security personnel, as he will find it difficult to authenticate the users from ODC.
- Complexity of the network: Complexity of the network and its continuous expansion has made its management more difficult. The access of the ODC adds more to this difficulty specially when the ODC serves many clients and is not dedicated to a single client.
- Difference of opinions: It is not necessary that the approach of the ODC and the client regarding the measures to be taken against known vulnerabilities should be the same. These could create differences and create vulnerabilities for both the ODC and his client.
- Intellectual property: When the company goes in for offshore development it has to give information about its trade secrets, data related to customers and other financial information. A company would suffer severe damages if the intellectual property were misused, as the dispute would be subject to international laws.
- Other legal issues: Data related to the customers is subject to privacy policy of the company and privacy law of the country. It is difficult for a company to ensure that the privacy policy and law are abided to by the offshore developer.

Answer: [d] Increase in the revenue of the vendor

Reference No:M7125

Question: Which of the following statements is not true about Kiviatic charts?

- [a] Kiviatic chart is a performance index
- [b] Kiviatic chart gives a comprehensive diagrammatic representation of system utilisation

- [c] The center or the hub of a Kiviati chart represents an idle processor
- [d] Accuracy in interpretation of Kiviati chart depends on user's experience and knowledge

Module 7 – Performance evaluation using Kiviati Diagrams

Introduction

In order to monitor and evaluate the performance of a system, the numeric values (or quantitative measures) should be converted to their equivalent qualitative values, i.e. for ensuring infallible performance evaluation the qualitative throughput of a system has to be accurately assessed. Performance measures can be represented by employing various charts like Gant chart, Kiviati chart, benchmark test etc.

Performance index is maintained to represent the equivalent numerical values for qualitative measures of a system. A *performance index* is a descriptor used for representing the performance level of a system (taking into consideration some of the aspects of the system). These indices are carefully defined so as to measure each and every aspect of performance of a system. E.g. 'Productivity' can be taken as a performance index class having production rate, data processing rate, maximum throughput etc as its indices. Or for example, for turnaround time, reaction time and the like can be indices of a performance index class named '*responsiveness*'.

The Kiviati graph

A Kiviati chart is a display adapted from many other related graphs that are used in performance evaluation. It gives a geometric representation for every individual performance index's (like say productivity, responsiveness etc) utilisation.

A Kiviati chart incorporates all the data required to evaluate the qualitative performance of a system, in a single chart. Thus, a Kiviati chart gives the evaluator a summary of the complete system utilisation.

How to draw a Kiviati chart

- A system comprises of a number of processors, each functioning in its own way with varying performance levels. Hence, for a comprehensive performance evaluation, an in-depth measure of qualitative utilisation of each processor has to be done. Thus, prior to drawing a Kiviati chart, each processor is represented by a spoke of wheel. Any arbitrary point on the spoke determines the recent most average fractional utilisation of each processor. The centre of the wheel is taken as 'zero' (i.e. the processor is in idle state) and outer rim of the wheel is taken as 'one' (i.e. the processor is completely busy).
- A polygon is drawn taking the points of all the processors as vertices. Since it is assumed that the center is zero and rim of the wheel is one, it can be very easily deduced that concentration of the polygon near the center indicates 'Low utilisation' and a 'High utilisation' is indicated if the polygon is towards the rim of the wheel. Thus, a good system (a balanced one) has a star like picture in a Kiviati chart.
- A strongly skewed or asymmetric polygon will show a poor load balance. Moreover, slightest change in the load balance is quite evident in the Kiviati diagram.

- 'Current utilisation' (i.e. if the processor is at the given particular instant of time) is indicated using dark shading in the graph.

A sample Kiviati chart

The following diagram illustrates how a Kiviati chart looks like. The rim of the wheel indicates that the processor is in busy state and the centre indicates that the processor is idle. Difference of opinions: It is not necessary that the approach of the ODC and the client regarding the measures to be taken against known vulnerabilities should be the same. These could create differences and create vulnerabilities for both the ODC and his client.

Merits of using a Kiviati representation

- Since, a Kiviati diagram puts down the utilisation of every processor in a system, it becomes easier for the observer to comprehend the performance of the system.
- Any problem that might be present with the working of any processor can be identified at one glance.
- Moreover, since the choice of the quantitative measures (of each processor) is arbitrary, an unbiased judgement can be formed on the performance of the system as a whole.

Limitations of Kiviati charts

- All the axes of the Kiviati diagram are taken to be of equal length, which may not be the case in practical implementation (since the measure of quality cannot be standardised).
- Extreme values i.e. the values at the rim of the wheel are always considered to be better, but a higher value of quality measure does not prove desirable always.
- Moreover, Kiviati representation is an art (since it does not have any standard or generalised interpretation) that improves with practice and continuing observation. Hence, a successful conception of a Kiviati graph totally lies in the knowledge and discretion of the user.

Answer: [a] Kiviati chart is a performance index

Reference No:M7126

Question: Which of the following must be considered before entering into software maintenance agreement?

- [a] Provisions in the agreement
- [b] Date of purchase
- [c] List price of the software
- [d] None of the above

Module 7 – IT budget

At times companies are forced to cut down their IT budgets and control their Information system purchases. This necessitates software maintenance agreement, an essential step in minimising the

IT budget.

Software licensing, maintenance and technical support are the three general things that are considered in determining the price of the software at the time of purchase. Software maintenance agreement enables an IT organisation to incorporate all the modifications to the software according to the recent changes.

The cost of maintenance ranges from 10% to 90% of the cost of software depending on the type of application and vendors. Hence it is essential to negotiate well before entering into software maintenance agreements.

The following are some guidelines for software maintenance agreements that help IT organisations to minimise the cost:

1. **Provisions in the agreement:** The maintenance provisions must be clearly known before entering into an agreement. For example, an agreement may contain a provision for modifications or upgradation for Microsoft windows but may not provide the advancements like new versions of Microsoft windows.
2. **Date of commencement:** Negotiate and determine the installation date for the software in the agreement instead of installing immediately after the purchase.
3. **Price negotiation:** The price of the maintenance agreement must be determined on the basis of proper negotiation between the parties. Organisations should take care that it is not based on the list price. Further the contract must be thoroughly reviewed to evaluate its compliance with the vendor's invoice.
4. **Flexibility:** Restrictions in the agreement minimise the flexibility to change. Especially in case of mergers, vendors do not permit companies to merge their licenses and terms. Ensure that the agreement does not contain any provisions that restrict the expanding options.

Finally the benefits derived out of the maintenance agreement must be recorded by counting the number of bugs addressed by the vendor.

Organisations even have other options to minimise the expenditure rather than squeezing IT budget. Restructuring the expenditure for instance. An IT department may have to spend huge amount of resources on certain aspects, which are unavoidable. Thus, secure private networks, encryption, virtual private networks and security are the main concerns in this context. Ignoring these or cutting the investment in security aspects may expose the business to risk.

On the other hand it is essential to cut costs to release financial resources. Undertaking a cross-departmental strategy that leverage the IT investment in saving the cost of other departments will benefit the organisation as a whole. For example, a collaborative workgroup software tool implemented in the organisation will increase the cost of IT department. At the same time it reduces the travelling expenses of other departments and improves the long run productivity of the company.

Answer: [a] Provisions in the agreement

Reference No:M7127

Question: Which of the following accounting issues may cause problems while implementing accounting software?

- [a] Adequate controls to ensure the integrity of accounting data
- [b] Altering the accounting procedures whenever software is altered
- [c] Ignoring policies and procedures by employees
- [d] None of the above

Module 7 – Accounting Software

Accounting software package must improve the accounting performance of an organisation. Thus it becomes essential to analyse the accounting needs and integrate them with the software performance. Several factors need to be considered before undertaking new software. The following are some of the accounting issues that may present problems while dealing with the software.

I. Lack of controls: Without existence of proper controls any amount of investment in new software will go waste. Hence proper checks and balances must be established to ensure the integrity of accounting data.

The following are some of the controls that an organisation can incorporate while using the software

- Group the source documents into manageable size and verify the totals of these groups after posting.
- In batch processing, review all the items like dates, period and amounts before posting.
- Recheck the calculations and processed data by an alternative method if possible.
- Check the numbers at regular intervals by reconciling related things like cashbook and bank statement.

Frequent reconciliation and testing of transactions ensures the accounting data integrity.

II. Lack of appropriate procedures: Organisations usually face problems when they use the same old controls in the new accounting package. The accounting procedures must be duly altered whenever there is an alteration in the accounting software.

III. Ignoring accounting procedures: Quite often employees ignore policies and procedures designed to prevent accounting errors. Supervisors must ensure that employees follow these procedures. Proper training and encouragement must be given to employees in the usage of such procedures. They must be made readily accessible to the users.

Organisations may also consider the following issues related to software:

1. ***Optimum utilisation of the software:*** The existing software must be utilised to its fullest. It is not feasible to install new software for a single additional feature, which can actually be added by upgrading the old software or understanding the existing software.

Further an active software support agreement with the vendors and adequate training to employees ensures appropriate use of software.
2. ***Thorough understanding of software working:*** A thorough understanding of working of the software will avert problems. Monitor the defaults regularly and modify the software according to the requirements.

3. ***Discontent with the system's speed:*** Software speed is another issue. However, this can be resolved through utilities available in the packages. These utilities control the size of the files and enhance the speed of the software. Hardware aspects like operating systems and network configuration will also affect the system speed. Therefore, upgrading the hardware and monitoring the network configuration will resolve the hardware related speed problems.
4. ***Discontent with reporting capabilities:*** Many accounting packages contain built-in standard reporting formats. But organisations may find it difficult to capture the required data. Even if the data is captured, they may not be able to get it in the required format. Organisations, in such a case, need not go for new software. Redesigning the existing system can help organisations in generating useful reports.

Finally, provide continuous training on software and incorporate any upgrades to the software. Possible ways for optimum software utilisation must be identified.

Answer: [c] Ignoring policies and procedures by employees

Reference No:M7129

Question: Which of the following is not a risk factor associated with a DSS?

- [a] Simplification of models
- [b] Misuse
- [c] Confusion between theory and reality
- [d] Improper field testing

Module 7 – Decision Support Systems (DSS)-Risks

Introduction

The class of systems that aid the decision making process are termed as Decision Support Systems (DSS). Decision support systems have given ample opportunities for organisations and their decision makers to arrive at intelligent and rational decisions. DSS fits into the top level and higher middle level of an organisation as they cater to structured & unstructured information. Success of DSS depends on its proper usage and implementation. This because, DSS is being incorporated in many of the systems inherent in an organisation like file drawer systems, data analysis, accounting systems, representational systems, optimisation systems and suggestion models. An extensive utilisation exposes it to a number of risks.

Factors responsible for poor adoption of DSS

Some of the reasons for improper functioning of the DSS in organisations could be attributed to the following:

- Improper definition of the target group and clients
- Unclear collection of inputs from the end users or target group before devising a DSS
- Mismatch of DSS with the decision making style of the organisation/its managers
- Managers are not given a proper reason for adapting a DSS and thus results in resistance to change
- Lack of proper field testing

- Lack of technical support in the form of training or orientation

Apart from these, a number of other constraints like poor marketing, knowledge transfer or dissemination, lack of training in hardware and software, short shelf life of DSS software, poor user interface and operational constraints come in the way of a successful DSS.

Risks

A DSS should be analysed for a number of risks, more so in the implementation model stage. Some of the typical risks include misuse, simplification leading to misleading outputs and confusion between model and reality.

Misuse: The decision makers could probably fall under the weight of the system by itself. That is, they could make the system responsible for any of their actions or decisions. So, it gives an alibi for the decision makers to exploit the system for their personal agenda as they could easily address the failure of any decisions to the system.

Simplification of models: A simplified model of DSS could result in giving a wrong picture of the intended outputs or results. This aspect is more important in the making of the model itself as the purpose for devising a support system must hold good for everyone in the organisation. A model aimed at economic benefits may not necessarily keep the client or end users benefit in mind.

Confusion between model and reality: The users may not be aware of the assumptions and limitations of the model underlying the making of a particular decision making system. They end up having big expectations about the software and hardware capabilities of the system. This arises due to the huge gap that exists between theory and practice.

Answer: [d] Improper field testing

Reference No:M7130

Question: Which of the following is an advantage of an automated software-testing tool?

- [a] Minimises cost and increases effectiveness
- [b] Replaces the manual testing process
- [c] Modifies the manual testing process
- [d] Develops a standalone testing environment

Module 7 - Automated software testing process

An automated software testing process is an essential requirement for software testing in today's market. It minimises the cost and increases the effectiveness of the testing process. Several automated tools are available for mainframe and GUI based applications. But companies find it difficult to implement these tools. Many are faced with problems like increased working time and difficulty in understanding. The two part series of the article provides an overview on the successful implementation of an automated testing tool.

Automated testing

Automated testing refers to mechanising the manual testing process. The essential criterion to

implement the automated tools is the existence of prescribed manual testing process in the organisation. An effective manual process should have: -

1. Detailed test cases
2. A standalone testing environment

The basic purpose of automating the testing process is to minimise the work in case of repeatable tests. Repeatable tests are run to determine the unintended consequences while altering an application. Therefore, a database showing the detailed test cases must exist.

Costs and benefits

Automated testing is performed in addition to the normal manual testing. Basically, automated testing involves high cost and time if an ineffective method is used. For example, if record/playback (a feature included in many tools) method is used for testing, it takes more time than the manual testing. Therefore, a little thinking before applying the tool to the process makes it effective.

1. Select the tool, which is consistent with the organisational testing requirements.
2. The tests that are subject to repeated operation must be automated and not the one-time tests.
3. Avoid costly and ineffective methods like record/playback testing.
4. Automating the complex test process may prove to be a costly affair because of the problems involved. Hence, simple and straightforward processes are best suited for automation.
5. Finally, data-driven automated testing method must be selected. Data-driven methodology helps in building generic test scripts. Functional decomposition method and key word driven method are the two types of data-driven methods.

The purchasing blunder

The reason for the failure of most automated tools is blunders made at the time of purchase. For example, consider record/playback method. If this tool is selected for testing, a user may face the following problems:

- Immeasurable and unaccepted level of costs.
- The entire test has to be re-recorded in case an error is made while entering data.
- The tests also have to be re-recorded if there is any change in the application
- Unreliable scripts used
- Scripts have to be changed in case of any change in the application

In such cases an automated testing methodology is an appropriate method to ensure proper and effective testing. The following article deals with such methodologies.

Answer: [a] Minimises cost and increases effectiveness

Reference No:M7131

Question: Which of the following is an advantage of functional decomposition method of automated software testing process?

- [a] Requires less technical knowledge
- [b] Use of multiple data files for particular test case
- [c] Scripts can be aligned with higher level test script
- [d] Scripts done in spreadsheet format can be used a number of times

Module 7 – Automated software testing process – II

The first part of the article on automated software testing process dealt with the introduction and cost/benefits analysis of an automated testing method. Present article will focus on two types of data-driven automated software testing methods and the requirements for its successful implementation.

I. Functional Decomposition method:

This method is superior to record/playback method. Under this method, the test cases are minimised to their basic tasks. Such tasks are performed independently with the help of user defined, business function and utility scripts. The process includes four steps:

1. Navigation
2. Specific function
3. Data verification
4. Return navigation

Merits

- Minimises duplication of effort in developing scripts by using modular design
- Scripts can be aligned with higher-level test script easily
- Expected results, utilised for verification, are stored in simple test records

Demerits

- Requires high-level technical knowledge
- Data has to be re-entered continuously in various files
- Due care must be taken for data file format
- Usage of multiple data files for particular test case

II. Keyword driven method

It is also referred to as Test plan method. It is totally data driven method and superior to functional decomposition method. Key words are used to perform specific functions by processing input parameters. Template for a test case is developed through spreadsheet program. Copying this template can perform additional test cases.

Merits

- Scripts do not have to be written again once done in spreadsheet format
- Scope for reusing the generic utility tests
- Translation of any existing format into spreadsheet is not difficult

Demerits

- Requires knowledge of scripting language for customised function development
- In case of more number of functions, more keywords have to be learnt by testers. It consumes time.

Change management

While adopting an automated testing tool, an enterprise may face resistance to change from tester. This is because tester involvement is less in tool selection. Therefore, management should have a definite approach to manage these changes. For instance the following are some of the fears of testers and the solutions to tackle those:

- 1. Complete replacement:** Testers fear that if an automated tool is implemented manual requirement will be reduced. However it is a helpful tool for testers. It saves their time and effort.
- 2. Training:** Training on the new tool involves much time. But in reality it is not so. For example, test-plan method requires only minimal learning on spreadsheet usage.
- 3. Difficulty in usage:** Testers in fact do not use it. A test tool specialist appointed specifically for the purpose uses it.

Staff selection

A senior level programmer is an appropriate person for the position of test tool specialist. However, it is not specifically required. The following are his functions:

- Establishing automated scripts
- Establishing procedures and standards
- Framing procedures for managing change
- Establishing required infrastructure
- Managing and executing the test scripts
- Test running and furnishing results to testers

Answer: [c] Scripts can be aligned with higher-level test script

Reference No:M7132

Question: Which of the following is not expected of an RFP (Request for Proposal)?

- [a] Specifications
- [b] Time saving
- [c] Sending to prospective vendors
- [d] Sending outside for budget planning

Module 7 – Request for proposal

What is a RFP?

A Request For Proposal (RFP) is a formal procedure followed by companies to notify vendors or service providers that they intend to purchase goods and/or services and invite proposals. Large organisations invest huge amounts of money to purchase good and services from vendors.

Purpose

RFP's are developed and implemented in order to:

- Ensure that vendors deliver the product or service as per the customers' requirements.
- Institute and standardise the vendor's proposal for the purpose of easy understanding, analysis, interpretation and comparison.
- Notify the vendors that the purchase is bid competitively.

Instructions

A typical RFP contains instructions to the vendor on the following aspects:

Specifications: RFPs must furnish detailed information on the specifications of the product or service the buyer is seeking.

Proposal Content: This contains specific instructions on how the response (a proposal) should be crafted or prepared.

Timing: Some questions like "when does the business expect the proposals?" are to be addressed here. More precisely, it is known as the RFP close date. This allows the company issuing the RFP to plan and schedule their decision-making process.

Benefits

Product Purchase Satisfaction: The buyer is able to set criteria to evaluate proposals by using an RFP. It makes it clear to vendors that proposals not living up to the requirements mentioned in the RFP will not be entertained. If not for RFP's, buyers would end up buying things what ever comes their way. This would result in customer dissatisfaction due to improper communication about the product.

Product Price Satisfaction: With the help of an RFP all the vendors know that many others are bidding for the purchase. This shall give the vendor an incentive for a best price on the first proposal.

Vendor Product Comparison: Once the RFP has expired and the buyer has proposals, comparisons are possible because the vendor has responded to a common set or requirements.

Time Savings: Though the time taken to devise an RFP is more, the time spent preparing an RFP is relatively more when compared to the time devoted on explaining the requirements to every vendor

and making the best price quote. Buyers are in no way bound to waste time with vendors who are not in a position to deliver the product or services they require.

Distribution of the RFP

The RFP's are to be sent eight to ten weeks before the requested submission date. This is because, writing a detailed proposal takes time, and there should be enough time provided for potential vendors to think about and respond to the RFP's.

- ☐ The RFPs are to be distributed to the vendors who have been identified as being able to produce the materials that the buyer wants
- ☐ RFP's are not to be sent to organisations with which the buyer has no intention to work
- ☐ An in-house project should not be sent to an outside party for project planning
- ☐ RFP's should not to be sent outside for planning the budget

Answer: [d] Sending outside for budget planning

Reference No:M7133

Question: The internal logic of the program is tested by which one of the following test: -

- [a] Black box
- [b] white box
- [c] Unit test
- [d] Integration test

Module 7 – Comparison between Black box testing and White box testing

Testing

Testing is one of the most important elements of software quality assurance. Testing is executing the software application intended to check for as many errors as possible, before the software is delivered to the customer.

There are basically two types of testing: -

1. White box testing
2. Black box testing

White box testing is performed at early stage of the testing process while black box testing is performed at the later stage. This is due to the reason that black box testing deliberately neglects the control structures and the focus is shifted towards information domain.

White box testing

Also called glass box testing, it is conducted on code component of the software by analysing the internal working of a software product. Different tests are performed to ensure that all the internal processes and functions are carried out according to specifications. White box testing can be done only by close examination of procedural details. Hence specific programming knowledge is required to determine the output.

White box testing helps in ascertaining that:

- All the independent paths in a program are executed at least once.
- All logical decisions are taken as intended.
- All the loops in a program are started and terminated as desired.
- Internal data structure has been checked for their validity.
- Internal interfaces are verified for reliability.

Pros and cons of white box testing

Pros

- Developers can verify the functionality of their components at the time of software development cycle.
- Quality assurance time is reduced as the assembled product has fewer bugs.

Cons

- It is very expensive
- Not suitable for large applications
- It is time consuming process

Black box testing

It is also called behavioral testing. It is done by understanding the specific function (s) that the software product is designed to perform. A series of tests are conducted to know that all the functions are being carried out accordingly, inputs are being properly accepted and desired outputs are delivered. Simultaneously, black box tests find errors in each function. Black box testing is no alternative to white box testing but it is an integral approach which covers different set of errors than that of white box testing. Black box testing is done to: -

- Identify incorrect and unnoticed functions
- Identify all external interface errors
- Check errors in data structure
- Identify problems in database access
- Check behavioral and performance errors
- Validate the capability of system hardware and software to recover the loss due to external or environmental threats.

Pros and cons of black box testing

Pros

- Black box testing is done from end user perspective
- Tester need not to know about internal working of the program
- One can even test the environment in which the program is executed

- The resources and effort used for testing can be used multiple times.

Cons

- Requirements should be clear and unambiguous otherwise difficulty in test cases is possible
- All properties of a software product cannot be tested
- The reason behind the failure of any functionality cannot be identified.

Answer: [b] White box

Reference No:M7106

Question: Which one of the following does not serve as a Minimum Acceptable Tolerance criteria for selecting software?

- [a] The basic objective of the application
- [b] Operational errors
- [c] Risk element
- [d] Management Information System Reports

Module 7- Minimum Acceptable Tolerance for Software

No company would want to purchase software that is sub-optimal in quality, but this is often the case with many companies that acquire software even from top vendors. This results in a decrease in the profits, as the subsequent costs are not added to the assets in final accounts, but are deducted from the profits.

The following criteria serve as the minimum acceptable tolerance limits for acquiring software, beyond which companies should reject the software: -

5. Give importance to the basic objective of the application: The primary objective of the application should not be sacrificed at the cost of other services because of the initial enthusiasm at the time of making the purchase. Later when the absence of the primary feature is discovered, it may cost more than the other free services provided. For instance, it may be quite obvious that an exporter may not verify the existence of an important feature - (like the feature which includes automatic checking of commission and discount on foreign bills) in the flurry of purchasing an export-specific software that is linked to export needs.
6. Don't tolerate operational errors: Errors in the operational reports may be the cause of great loss to the organisation. One way to avoid such losses is to undertake a software audit. The expenses of a software audit are far less than the costs incurred in operational errors. For instance, in a certain company, penal interests on late instalment receipts were not calculated in spite of having a parameter file in the system for the particular action. It was identified by a routine audit after two years. The reason was non-activation of the instruction logic. Hence it is essential to test that the logic and the operational reports should not be sacrificed in order to save time and labour investment.

7. Management Information System reports should be up to the mark: Often organisations do not pay much attention to errors in the Management Information Systems report, considering it as a least important. In reality it is not so. Since crucial decisions are taken by the management on the basis of MIS reports, they play an important role in the survival of a company.
8. Multiple platforms are beyond tolerance: Efficiency will be at detriment if multiple platforms are involved. Software input and output that is digitally different will not be able to effectively match the time, labour and accuracy of the software. For example, if the information produced using sophisticated software in one department is channelled to a low-end database in another department, it may result in frequent disorders. This is because the low-end software may not be able to incorporate the changes that the advanced software undertakes.

Minimum Acceptance Tolerance limits need not focus on the complete perfection of the software. Practically this cannot be achieved. They should enable companies to avoid the selection of software of a sub-standard quality and minimise the hidden cost involved.

Answer: [c] Risk Element

Reference No:M7107

Question: Which of the following statements is true with regard to auditing the acquisition/development of application software?

- [a] Data entry and data collection should tally
- [b] Data entry and data collection need not tally
- [c] Data entry and input processing details should match
- [d] None of the above

Module 7- Audit working guideline

Develop/ acquire and maintain application software-2

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Develop/ acquire and maintain application software	9. System design	8. Data source
	10. Management approval	9. Input requirements
	11. Changes to existing system	10. Interfaces-external and user -machine
	12. Definition and	

	documentation of file requirement	11. Processing requirements
13.	Programming	12. Output requirements
14.	Software testing	13. Application software control features
15.	Consideration of availability in application software	14. Reference and support documentation
16.	Re-assessment	

Audit Process

The audit process has been covered in three parts. The first part covered a preliminary understanding and analysis of the process. This article is the second part, and focuses on the test of controls.

Tests of controls

A clear picture of the functioning of controls can be gained by:

- Obtaining evidence
- Reviewing the deliverables

Tests: Before the auditor takes a stand on the functioning of IT tasks in the organisation, he should check

21. The involvement of users in the requirement phase and design phase.
22. The procedures to ensure that all issues of the current phase are resolved before moving to the next phase.
23. All significant modification to existing systems are implemented using the SDLC approach for new projects
24. All design specifications are approved by the senior management and the affected user department before beginning the project
25. The design specification include definition and documentation of file-formats in accordance with the standards
26. Programme specifications for information development, are in agreement with design specifications.
27. Data entry and data collection details match.
28. A easy to use interface exists between the user and the system
29. Design and documentation of internal and external interface development
30. Existence of processing requirements

31. Existence of output requirements are existing
32. The design of control and Security requirements . This should be included in the conceptual phase itself.
33. Involvement of the security officer in the design phase and development phase
34. Applications should have provision for automatic verification of the tasks performed.
35. The design of mechanisms to provide availability, maintainability and reliability of the systems
36. Existence of a Project testing plan approved by the user
37. Existence of user support manuals
38. Existence of the help desk function to assist users
39. Updation of user documents
40. Re-assessments are conducted in case of significant deviations.

Answer: [a] Data entry and data collection should tally

Reference No:M7108

Question: Which of the following does the auditor have to review(during acquisition / development) to ensure the availability of application software?

- [a] System design of projects
- [b] User requirement statements
- [c] Specifications statement
- [d] All of the above

Module 7- Audit working guideline

Develop/ acquire and maintain application software-3

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Develop/ acquire and maintain application software	9. System design	8. Data source
	10. Management approval	9. Input requirements
	11. Changes to existing system	10. Interfaces-external and user -machine

	12. Definition and documentation of file requirement	11. Processing requirements
	13. Programming	12. Output requirements
	14. Software testing	13. Application software control features
	15. Consideration of availability in application software	14. Reference and support documentation
	16. Re-assessment	

Audit Process

The audit process has been covered in three parts. The first and second parts deal with the preliminary understanding, analysis, and test of controls. This concluding article focuses on substantive testing.

Substantive testing

This step is undertaken to substantiate the auditor's viewpoint that control objectives are either not being met, or do not exist. The shortcomings in controls and its consequences also should be documented. He can also:

4. Identify benchmarks from similar organisations/ industries
5. Use industry best practises or international standards to review the adequacy of the system development approach.
6. Perform a detailed review of:
 - The system design documentation to evaluate the adequacy of the same
 - Approval from management and relevant user departments
 - Software documentation to ensure that a organised file documentation exists and is structured in accordance with user and system requirements.
 - New system implementation projects, to ensure that all system programmes, interfaces, input, output, processing, data collection mechanisms are as per approved design.
 - The projects to check for any technical discrepancies
 - The projects to ensure the adequacy of internal control and system designs
 - Data integrity verification is conducted by the application
 - User reference materialsto verify if they are being updated .
 - The effectiveness of the programme with regard to - input, processing, interface specification process, and output specification process and the testing standards and its compliance.

Identifying shortcomings
The auditor should identify

- ☐ Deficiencies in SDLC methodologies
- ☐ Designs that do not meet user requirements
- ☐ File requirements that do not meet the requirements of data dictionary rules
- ☐ Poorly designed file, input, output, interface and processing specifications.
- ☐ Projects wherein availability has not been considered.
- ☐ Projects wherein the data integrity verification routines have not been incorporated into the applications.
- ☐ Deficient organisation standards
- ☐ Inadequate user and support manuals
- ☐ Significant discrepancies that did not result in re-assessments of projects.

Answer: [d] All of the above

Reference No:M7112

Question: With regard to auditing the process of acquisition/development of system software, an erroneous technological feasibility study may lead to

- [a] Difficulties in the implementation of the originally designed solution
- [b] Selection of alternative solutions which are expensive
- [c] Selection of alternative solutions which are highly risky
- [d] All of the above

Module 7- Audit working guideline

Develop/ acquire and maintain system software-4

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Develop/ acquire and maintain system software	14. Selection of system software	Not applicable for this activity
	15. Information requirements	

	16.	Identification of various alternatives	
	17.	Formulation of an acquisition strategy	
	18.	Third party service considerations	
	19.	Feasibility study: technological and economical	
	20.	Risk assessment results	
	21.	Security and control considerations	
	22.	Audit considerations	
	23.	Procurement of the selected software	
	24.	Facilities specification	
	25.	Acceptance of the software	
	26.	Contract programming	

Audit Process

The audit process has been covered in four parts. The first three parts covered the preliminary understanding, preliminary analysis and test of controls. This article is the fourth part, and focuses on substantive testing.

Substantive testing

This step is undertaken to substantiate the auditor's viewpoint that control objectives are either not being met, or do not exist. The shortcomings in controls and its consequences also should be documented. He can also consider the following points:

4. Comparative benchmarks from similar organisations, and industries can be identified.
5. Industries' best practises or international standards can be utilised to review the adequacy of the risk assessment approach.
6. The auditor needs to perform a detailed review of the-
 - Security, internal control and audit trails of the systems
 - The selection of the software and implementation of the same
 - Compliance with the organisation's procurement policies and procedures

- Third party service management
- Monitoring of contract programming
- The facilities acceptance process to ensure that environments and accommodation tests are conducted

Identifying shortcomings

The auditor should identify

- Deficiencies in SDLC methodologies
- Projects that do not meet user's requirements
- Expensive alternatives selected
- Highly time consuming projects
- Erroneous economic/technical feasibility studies
- Inadequate Risk assessments
- Improper/inadequate control features and audit trails
- Absence of user-friendly designs
- Non-compliance with the organisation's policies and procedures for vendor selection and management
- Non-compliance with the third party services agreement
- Non-compliance with contract programming terms and conditions
- Products which were accepted without adequate facilities testing, system testing, and accommodation testing
- Products which were accepted without technology and functionality testing and work load trails
- System failure
- Non-compliance with the contract terms and conditions

Answer:[a] Difficulties in the implementation of the originally designed solution

Reference No:M7113

Question: Which of the following resources need not be considered as a cost to be charged to users?

- [a] Hardware
- [b] Development of applications
- [c] Communication channels
- [d] All of the above

Module 7 – Audit working guideline

Cost management Part 1

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Cost management	4. Identification of chargeable items 5. Costing procedures 6. Revenue billing and charge back procedures	Not applicable for this activity

Audit Process

The audit process has been covered in two parts. This article is the first part, and deals with a preliminary understanding and analysis of the process.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
IT cost team Users	6. Policies and procedures with respect to - Resources identification and measurement - Charging rules and regulations - Rates- charging and charge back - Cost reporting mechanism 7. Organisation policies and procedures relating to budgets 8. Documents - IT functions - Budgets - present and the previous year - Allocation of resources - Data used

	▪ Method of allocating cost ▪ Any other relevant reports
	9. Documents - users ▪ Budgets - present and previous years ▪ Current IT plans
	10. Allocation of resource for IT functions , including functions that are charged back and absorbed

Preliminary analysis

The next step is to analyse the effectiveness of the control measures adopted, and their reliability. This can be done by ensuring that:

- The management has defined and established a user billing procedure for the IT functions.
- The management has developed procedures for
 - o Developing yearly plans, criteria for prioritisation of activities and maintenance of plans.
 - o Creating budgets for different IT resources and ensuring that the budgets comply with overall organisation budgets.
 - o Allocating costs of the user department.
 - o Communicating to users the components of revenue bills.
 - o Approval of budgets by the users and periodicity of delivering reports .
- The use of IT resources to be charged should include usage of
 - o Hardware
 - o Development of applications
 - o Communication channels
 - o Peripherals
 Beside the above other indirect cost that can be included are administrative cost, help desk facility, maintenance cost, vendor service cost and any other relevant costs.
- Users are provided with reports on the performance of cost centres, assessment of organisation cost with the industry standards and t changes in the cost components.
- Cost allocation method are in line with the changing requirements of the business
- Opportunities for reducing charge backs have been identified

The next article focuses on the second part - the test of controls and substantive testing.

Answer: [d] All of the above

Reference No:M7114

Question: Which of the following should the auditor check out to decide on the costing method of the organisation?

- [a] The process of allocating cost and its acceptance by the management
- [b] The process of charging rates in keeping the costs involved in providing the services
- [c] The process of allocating costs to external users only and not to internal users
- [d] All of the above

Module 7 – Audit working guideline

Cost management Part 2

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Cost management	4. Identification of chargeable items 5. Costing procedures 6. Revenue billing and charge back procedures	Not applicable for this activity

1.

Audit Process

The audit process has been covered in two parts. The first part covered a preliminary understanding and analysis of the process. This article is the second part, and focuses on the test of controls and substantive testing.

Tests of controls

A clear picture of the functioning of controls can be gained by:

- Obtaining evidence
- Reviewing the deliverables

Tests: Before the auditor takes a stand on the functioning of IT tasks in the organisation, he should check

- Method for allocation of cost and its acceptance by the users
- Existence of cost improvement techniques
- Performance of the IT resources
- Delivery of reports and ensure effective and efficient utilisation of IT resources
- Allocation of resources to the user department
- The rates being charged- is in line with the costs involved in providing the services.

Tests should be performed to ensure that control measures identified in the preliminary analysis are functioning as desired.

Substantive testing

This step is undertaken to substantiate the auditor's viewpoint that control objectives are either not being met, or do not exist. The shortcomings in controls and its consequences also should be documented. He can also:

8. Identify comparative benchmarks from similar organisation and industries.
9. Confirm the charge back, by calculating from raw data to the final figures in the report
10. Ensure that the performance reports reflect the usage of CPU and peripherals, lines of code program written and printed, changes made in the programs, the number of enquiries at the help desk, number of transmissions and the like
11. Check if charge backs are tested regularly to ensure that the calculations are correct
12. Verify consistency between the charge backs of different users
13. Review distribution process of reports
14. Assess user satisfaction with regard to charge backs and the budgeted figures, progress of development plans and charge backs, benchmarking of charge backs against different alternatives and the like

Identifying shortcomings

The auditor should identify:

- Opportunities to improve the effectiveness and efficiency in the cost methodology and use of resources
- Non-inclusion of certain cost items in the charge back
- Alterations (if any)made to the cost allocation methodology
- Allocation of cost between equipment and applications
- Inappropriate allocation of cost among different users
- Prospect of using IT resources to meet the business needs of the users
- Prospects of improving the performance by enhancing the efficiency in the process of collecting, gathering, allocating, communicating and reporting on costs
- Cost variances
- Profitability of IT functions in delivering services to both internal and external users ,and in the light of the budget

Answer: [b] The process of charging rates in keeping the costs involved in providing the services

Reference No:M7115

Question: Which of the following documents is not relevant for an auditor for obtaining an understanding on the configuration management?

- [a] Configuration inventory
- [b] Offsite storage inventory
- [c] Policies and procedures for acquisition, maintenance and disposal of equipments
- [d] Development of applications

Module 7 – Audit working guideline

Configuration management Part 1

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Configuration management	8. Configuration inventory	Not applicable for this activity
	9. Baseline	
	10. Verification	
	11. Licensed software	
	12. Storage library	
	13. Future demands	
	14. Audit trails	

Audit Process

The audit process has been covered in two parts. This article is the first part, and deals with a preliminary understanding and analysis of the process.

Preliminary understanding

First, an understanding of the IT activity defined, its business requirements and related organisational issues is essential. An understanding of the control measures adopted for the activity is also required. This can be done by interviewing the concerned staff and going through related documents. The relevant personnel and the documents are given below:

Personnel	Document
8. Operations team	9. IT policies and procedures related to ▪ Configuration acquisition, maintenance and their disposal ▪ Quality assurance
9. Application development team	

10.	Support and facilities team	▪ Change control
11.	Software vendors employees	10. Organisation policies and procedures with respect to ▪ Purchase, rent or lease of equipment and software ▪ Acquisition, maintenance and disposal of equipments and software ▪ Use of licensed software
12.	Asset management team	11. Inventory of configuration both onsite and offsite related to □ System software □ Application software □ Hardware □ Facilities □ Data
13.	Quality assurance team	12. Configuration baseline information
		13. Documents related to □ Inventory of fixed assets □ Equipments on lease □ Changes to configuration of the systems
		14. Inventory of library resources - test, development and production results
		15. Offsite storage inventory □ Equipments □ Data □ Manuals and the like
14.		16.

Preliminary analysis

The next step is to analyse the effectiveness of the control measures adopted, and their reliability. With respect to configuration it is necessary to ensure that

- A process exists for creating and maintaining the baselines for configuration
- A configuration procedure is in place and provides for maintaining the integrity of the configuration
- There is a proper authorisation system for making the required changes
- Process exists for determining whether the procedures for documenting the configuration is adequate

- Personnel have the required skills and expertise
- Access to software baselines are reviewed periodically and appropriate actions taken to rectify errors, if any
- Accounting records are reconciled with the actual inventory on a periodical basis
- Changes are recorded and maintained
- Configuration reports reflect the applications migrating from development to testing environment and from testing to production environment

Answer: [d] Development of applications

Reference No:M7116

Question: Library management software helps in which of the following?

- [a] Documenting the changes that are made to program
- [b] Controlling the version numbers of the programs
- [c] Generating the reports on changes made to programs
- [d] All of the above

Module 7 - Audit working guideline - Configuration management Part 2

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Configuration management	8. Configuration inventory	Not applicable for this activity
	9. Baseline	
	10. Verification	
	11. Licensed software	
	12. Storage library	
	13. Future demands	
	14. Audit trails	

Audit Process

The audit process has been covered in three parts. This article is the second part, and deals with a preliminary understanding and analysis of the process.

Preliminary analysis (contd..)

The next step is to analyse the effectiveness of the control measures adopted, and their reliability. This can be done by ensuring that the following are in place

- All the software must be labelled and an inventory maintained of them
- With respect to software change controls, procedures must exist for
 - o Maintaining a library of application programs
 - o Restricting the access to the library
 - o Determining the dependability and integrity of software inventory. This is to ensure the use of licensed software only.
 - o Detecting the use of unauthorised software, if any. The management must be informed for appropriate action.
- As regards the software storage, the following are necessary
 - o Storage of all the software
 - o Separate storage library for different stages of development of software
 - o A separate area to store sources that are moving to production environment
 - o Owner for each software
 - o Clearly defined access controls
 - o An established audit trail
 - o Detection procedures for instances of violation prescribed code. The same must be documented and reported to the management
 - o Assessment of appropriate action undertaken to rectify the violation
- Library management entails use of appropriate software. It should be considered whether the library management software is used for
 - o Documenting the changes that are made to the program
 - o Controlling the version numbers of the programs
 - o Generating the reports on changes made to programs

Besides the above there are certain general analysis that the auditor should carry. These pertain to

- Processes for maintaining the status on the resources that are purchased and leased.
- Configuration baseline reflects the changes that are made to the applications, quality and operations.

The successive articles focus on test of controls and substantive testing.

Answer: [d] All of the above

Reference No:M7117

Question: On which of the following should the auditor perform substantive testing with regard to configuration management?

- [a] Review of the configuration records
- [b] Review of incidents reported to senior management
- [c] Review of the training manuals
- [d] All of the above

Module 7 – Audit working guideline – Configuration management Part 3

Table of applicability

For IT task	Control objectives	
	Management controls	Operational controls
Configuration management	8. Configuration inventory 9. Baseline 10. Verification 11. Licensed software 12. Storage library 13. Future demands 14. Audit trails	Not applicable for this activity

Audit Process

Audit process has been covered in two parts. The first part deals with the preliminary understanding and preliminary analysis. Preliminary analysis is dealt in detail in the second part. The concluding part deals with the test of controls and substantive testing.

Tests of controls

A clear picture of the functioning of the controls can be gained by

- Obtaining evidences
- Reviewing the deliverables

Tests: The following tests have to be done, before an opinion is formed on the functioning of IT tasks in the organisation. Such tests pertain to various aspects viz., baseline configuration, unauthorised software, software storage and reporting.

- In baseline configuration, it must be ensured that Baseline configuration is defined
- Procedures for recording, changing and approval of the same by the management are defined
- Actual status on the configuration of the assets is reflected in configuration records
- Records are reviewed by the management at appropriate intervals
- Policies and procedures are defined for configuration reporting
- Standards for the performance of maintenance of configuration and reporting are complied with
- Configuration baseline is compared at regular intervals with the inventory records of the equipment and resources

As regards unauthorised software it must be ensured that

- Policies and procedures exist for detection of use of unauthorised software
- Personnel understand the significance of authorised software and that appropriate training is provided.
- Personnel have signed the forms for compliance with the procedures
- Software are centrally controlled
- Software are reviewed on a continuous basis, violations are reported and appropriate actions are taken

For software storage it must be ensured that

- Storage libraries are defined
- Storage of programs and source code for all the programs are defined during their development

Reporting entails

- Collecting and processing information for reporting

Tests should be performed to ensure that the identified control measures in the preliminary analysis section are functioning as desired.

Substantive testing

This step is undertaken so as to substantiate the auditor's view of controls objectives either not being met or not existing. The control weaknesses observed and its impact will have to be documented. In order to further substantiate the viewpoint

- Review of the frequency at which the configuration records are reviewed by the management and reconciliation of the various records
- Examination of the libraries using a software to duplicate software, missing object codes and deleting the data, files and programs that are not required

Identification of shortfalls

The auditor should identify:

- Lack of awareness among the personnel on configuration baseline
- Ineffectiveness and inefficiencies in baseline configuration procedures
- Inappropriate reflection of the changes made by the vendors in configuration records

Answer: [a] Review of the configuration records

Reference No:M7118

Question: Which of the following should a company look into prior to reengineering a product?

- [a] Compliance with ethical issues
- [b] Infringements that might occur in the high-risk area of the product
- [c] Patent owner's awareness of reverse engineers' intention
- [d] All of the above

Module 7 – Ethical and legal issues involved in Reverse engineering:

Introduction:

'Reverse engineering' is a widespread practice in software engineering that involves disassembling, inspection and study of a product to identify its underlying strengths and weaknesses, so as to make a replica of it or to enhance the existing system. In general, reverse engineering is adopted for building similar products with enhanced performance and productivity (in terms of cost of manufacture and maintenance).

Normally, to buy a product and study its intricacies for developing a similar product albeit with improved features is considered as legal and ethical. However, the reverse engineering processes should conform to the clauses that govern the patent rights of a company.

Some of the legal and ethical issues involved in reverse engineering and their solutions are discussed below:

- *Does purchasing a product from one manufacturer and sending it to another for reverse engineering violate legal strictures?*

Buying a product from one manufacturer and giving it to another manufacturer for the purpose of reengineering does not violate any legal strictures. However, such an act could amount to being unethical. The correct way is to directly buy the product from the manufacturer for reengineering without involving a mediator for this purpose. In other words, the supplier interested in reengineering a product should buy it from its manufacturer, revealing his intention behind the purchase prior to reengineering. Further, legal issues will arise if protected data is being replicated or being processed without prior consent.

- *Is it legally acceptable to buy a product from a manufacturer who has imitated its patented version and may be violating the copyrights?*

By and large, purchasing contracts tend to protect the buyer. However, it is better to avoid buying a product, which infringes the copyrights of the original manufacturer (i.e. a deliberated purchase of an infringing product may pull the buyer into legal complications and there is every chance of him being legally sued)

- *Does such an act conform to the values of the company?*

The reverse engineering process, should comply with the values of the company. In other words, when it is the turn of the company (that reengineers the legacy

system), it should be able to handle infringements of its patent (the reengineered one), since every competitive product in an open market becomes an inspiration for reengineers.

How to go about it then? Considering the above legal and ethical issues, if the company decides to reverse engineer a product, then it is advisable to acquire the consent of the owner. This can be done by an out-and-out purchase of the product in the open market. A second option would be to arrive at an understanding with the patent owner prior to the reverse engineering process, so that the latter is well aware of the intention behind such purchase. Further, during the course of the reverse engineering process, the company should be watchful about imitating or disassembling a protected part of the product, which is also known as the high-risk area.

Answer: [d] All of the above

Reference No:M7119

Question: A reengineering project may fail due to ?

- [a] Lack of proper observation and assumptions
- [b] Lack of training for the workforce
- [c] Inadequate documentation of requirements of the target system
- [d] All of the above

Module 7 – Shortcomings in a reengineering process- Part I:

What is reverse engineering or reengineering?

Reverse engineering or reengineering involves separating the components of a system and observe it's working with an intention of creating its replica or improving upon the original product. For example, in the refrigerator industry, a manufacturer may buy a product from his competitor; disband it to examine its make for enhancing the original refrigerator with similar parts.

Risks involved in reverse engineering:

Reengineering brings with it the benefits of revealing the strengths and weaknesses of a product so as to develop a better product. But at the same time it can prove unsafe if the risks involved in it aren't evaluated and acted upon.

Following risks in reengineering may lead to failure of a project:

6. *Incomplete or fallible reverse engineering approach:* Strategies in reengineering may be faulty due to lack of in-depth observation and poor assumptions. Lack of proper attention may lead to concentrating on a wrong problem. This in turn leads to a flaw in the reengineering strategy. E.g. company may be uncertain about replacing a part of the parent product or renovating it. This hampers architectural decisions at the subordinate level, eventually affecting the overall reverse engineering process. In other words, the end product will head for a failure if the steps are not taken at the initial stage of the process.
7. *Employing inappropriate consultants outside the firm:* Usually outside contactors and consultants are employed for proper understanding and technical know-how of the product. The consultant should be hired based upon the experience and technical expertise. It is also

necessary for the consultants to have similar views and interests on various issues, say for example cost cutting. Thus, it is always prudent on the company's part, not to give complete control to a single outside contractor. Also, the company should remain alert for any problem.

8. *Insufficient training programs:* By and large, reengineering processes fail due to lack of proper training for the reverse engineering personnel. The work force must be well aware of the frequent updates in the hardware and addition of new programming syntax. Understanding new technologies and programming methodologies becomes difficult for a person who hasn't been upgrading his skills.

Ideally, a training programme should:

- ☐ Identify the needs of the trainee
- ☐ Check expenditure and time involved in the training
- ☐ Check whether the trained members are competent enough to lead a team.

9. *Lack of proper control over the parent (legacy) system:* Lack of proper knowledge about the parent system (or the legacy system) leads to inadequate understanding of system maintenance costs, cost incurred in changes, defects in the legacy system and long-term project planning. Lack of control is caused due to inadequate documentation, change control processes and track records for changes. It is important to maintain the record of all kinds of changes made, costs incurred in making the changes and the impact caused by the changes, without which long-term projections are highly unfeasible. As a result, the release of the end-product (or the final product) is delayed.
10. *Lack of validation of requirements:* Generally, there is very little or no substantiation for the concept of the target system (i.e. the derived one). Consequently, a well-documented requirement list (which includes hardware and software requirements, architecture requirements, maintenance and cost requirements and so on) for the target system is absent. The prime reason for this is taking the requirements of the legacy system for granted (and not planning it all over again for the target system)
Some more issues have been discussed in Shortcomings in a reengineering process-part I.

Answer: [d] All of the above

Reference No:M7120

Question: A complicated legacy system cannot be taken as a model for the target system because

- [a] Inadequate understanding of the concept will lead to inadequate documentation
- [b] Inadequate knowledge would mean incurring expenditure to train the workforce
- [c] Understanding and enhancing a complicated legacy system is not viable
- [d] The management will lose control over the reengineering process

Module 7 – Shortcomings in a reengineering process- Part II:

What is reverse engineering or reengineering?

Reverse engineering or reengineering refers to disassembling a product and observe it's working with an intention of creating its replica or improving upon the original product. For example, in the refrigerator industry, a manufacturer may buy a product from his competitor; disband it to examine its make for enhancing the original refrigerator with similar parts.

The previous part discusses issues related to the following:

- Incomplete or fallible reverse engineering approach
- Employing inappropriate consultants outside the firm
- Insufficient training programs
- Lack of proper control over the parent (legacy) system
- Lack of validation of requirements

The remaining issues discussed in this article that are as follows:

6. *Improbable software architecture of the legacy system:* At times, the architectural structure of the legacy system that is taken as model (check) for enhancement is too complicated or not viable. In such cases, the technical design of target system doesn't comply with that of the parent system, eventually leading to improper understanding of the end product. Unless the legacy system is well conceived, implementing the target system is not possible. It is very essential that the basic building blocks of the legacy system are comprehensible.
7. *Absence of a specific and distinct perception of an ideal reverse engineering process:* The evolution of the legacy system, to a large extent influences the reengineering process. By and large, a proper documentation of the legacy system is mistaken for substantiation for a reverse engineering process. On the contrary, a well-documented legacy system can only be an inspiration for the outcome of a reverse engineering process, not implementation as a whole. In fact a proper set of processes/steps is to be planned before reengineering process of a product is taken up, in the absence of which the reengineering process fails. Apart from the technology used, quality people employed and the resources on hand, a proper quality process also has to be followed to complete the reengineering process.
8. *Improper planning to overcome the shortcomings in a reengineering process:* One of the major requisite for reengineering is project planning. Often in the presence of the legacy system, the intermediate level is neglected and attention is given only to the low level (i.e. coding part). This creates confusion in the vision of the target system to be developed.
9. *Lack of continuing dedication from the management:* Only, dedicated effort at the management's end in keeping the whole process in control can see a reengineering process through completion. Errors in initial stages (i.e. during the designing of the building blocks of a software), often leads to a complete failure. When the management lacks dedication, the whole workforce loses focus, thereby leading to deterioration of the project. If the management delegates full responsibility to the lower level managers, they tend to divert

the project from the focussed objective of the reengineering process, resulting in a devastating outcome.

10. *Preset technical specifications for the target system:* A set of fixed directive or mandates preset or predetermined by the management establishing constraints on technical approach, cost, schedule and performance, without taking into consideration the opinion from the workforce at the lower levels often causes a reengineering process to fail. On one hand when a well-documented form is soul of the reverse engineering process, on the other hand it is equally risky to rely on a document that doesn't consider the approval of the team in setting goals for the project.

Answer: [c] Understanding and enhancing a legacy system is not viable

Reference No:M7121

Question: Which of the following steps is not involved component based software development?

- [a] System evolution
- [b] Component qualification
- [c] User requirement analysis
- [d] Component adaptation

Module 7 – Component Based Software Development (CBSD):

Introduction

Component- based software development refers to the process of developing large software systems by putting together, the components of already-existing software. This is done to make the software system more flexible and easy to maintain. This technique cuts down the development and maintenance costs. Further, assembling upgrading and supporting the system become less cumbersome. While building the basic building blocks of the software system, it is assumed that some parts of large systems are often recurrent. Hence, such parts should be coded (or written) only once, so as to reuse and reassemble the code instead of writing it all over again. Component-based systems include both COTS (Commercial off-the-shelf) products and the components of non-developmental products.

COTS (Commercial off-the-shelf) refers to *readymade* things that can be bought from a manufacturer's virtual shelf. Thus an already developed component can be integrated for developing the new system, at a cheaper rate. Such availability makes integration in large software systems easier and faster.

Why CBSD is becoming popular? The availability of a diverse range of COTS makes development of component-based systems viable. Further, the improved quality of COTS, high costs of system development & maintenance, and the growing reusability of already-existing software components in the industry, has paved way for the rise in the use of CBSD.

CBSD lays foremost emphasis on *composing software* rather than developing software.

Steps in CBSD:

Four major steps in component-based software development are discussed below:

- *Component Qualification:* Component qualification, also known as *suitability testing* involves examining whether an already-developed product can be employed for developing a new

system. Selection of the appropriate product (component) is done after taking all the competing products available in the market into consideration. Further Component qualification also ensures that the algorithms (employed in CBSD) have been validated. *Component qualification* is a two-staged process, namely- *discovery* and *evaluation*. In the *discovery* stage, the characteristic features of the component such as its interface, reusability, dependability on the product, functionality and so on, are identified. This is not a well-defined process and is often thwarted by complexities in identifying the intricate information about the component prior to its integration with the new system. To standardise the component qualification study, *evaluation*, which is a more refined approach, is adopted. Internationally accepted standards (prescribed by the ISO) for product evaluation guide the evaluation process. *Evaluation* process, involves paper-based studies of the various components. It takes into consideration, the opinion of the users of the component before developing a prototype.

□ *Component adaptation:* Component adaptation refers to acclimatising the component to the new system. Every component is designed and developed to meet different needs. Hence, it is very important to ensure these components get along well with the new system. The three different approaches employed in *component adaptation* are *white box*, *grey box* and *black box*. These approaches differ from each other in the extent to which they make the internal code of a component accessible. E.g. a white box approach allows accessing and rewriting the internal code of the component so as to make it compatible with the new system. A black box approach makes the internal code inaccessible, limiting the use of the code only to execution. Since white box approach allows modification of codes, it leads to increase in developing and maintaining costs.

□ *Component assembling:* Individual components are integrated using a definite and distinct architecture. Various examples of infrastructure employed for assembling are database (that controls all the operational data centrally), message bus (that has separate data stores to notify changes in the components) and so on.

□ *System evolution:* System evolution involves repairing the errors in the component, updating them, and transforming them into reusable units. Further, any additional functionality that may be required is incorporated in a new component and added in the system.

Answer: [c] user requirement analysis

Reference No:M7122

Question: Which of the following processes is the same for both RAD and SDLC?

- [a] Concept definition
- [b] User requirement definition
- [c] Rapid prototyping
- [d] Iterative approach

Module 7 – How RAD surpasses traditional approach of Software development:

Introduction

The changing needs of a business, calls for a faster approach of software development. With the expansion of the market, the information requirements also change rapidly, thereby inducing the

need for faster changes and updates in the information systems. The traditional approach i.e. the SDLC (System Development Life Cycle), also known as the waterfall approach, falls short of coping with the rapid changes in system requirements. Such limitations in SDLC has paved way for Rapid Application Development (RAD). RAD reduces development costs and time.

A Comparative assessment of SDLC and RAD

□ *Developmental phases of the two approaches:*

SDLC (System Development Life Cycle)	RAD (Rapid Application Development)
Concept definition (feasibility analysis)	Concept definition (feasibility analysis)
User requirement definition	Implementation of a skeletal system
System design	User evaluation and concept refinement
Implementation	Implementation of refined requirements
Integration and testing	User evaluation and concept definition
Acceptance installation	
Maintenance	

□ *Underlying concept of the two approaches:* SDLC starts off with user requirement specification prior to any other step, i.e. in SDLC the requirement specification is done much before the commencement of the project. This leaves less or no scope for changes in requirement analysis, during the course of system development. While on the other hand, RAD initially, develops a prototype / model of the system to be designed and it provides adequate room for improvising the requirement specification (which can be evidently seen in the second, fourth and fifth steps of RAD)

Further, in SDLC, the system design phase (which establishes the features and functions in detail using process diagrams and pseudocode) is rigid, while in RAD prior to system design, re-evaluation of end user's requirement is carried out thereby ensuring that the project does not deviate from the primary objective.

□ *Merits and demerits of RAD and SDLC:* Due to the shortcomings in the SDLC approach, RAD was sought for as a replacement. Unlike the SDLC, RAD offers a faster approach to software development with better quality.

- SDLC is a slower process when implemented. On the contrary RAD is fast in developing a system, since it uses iterative prototyping (i.e. uses tools like Object oriented System design - OOSD, Joint application development-JAD, and Computer Aided Software Development-CASE). These tools allow reusability of code, and faster software modelling.
- SDLC is too extensive and leads to high costs of developing and maintenance, therefore is incompetent in developing medium scale systems with low budget. On the contrary, RAD cuts development and maintenance costs.
- SDLC assumes that the user requirement can be ascertained at the very beginning of the project and it remains unchanged during the course of project, which is not the case. User requirements keep changing and often need to be modified. RAD involves the user in various workshops and end-user meetings in order to re-evaluate the requirements, thus is flexible to changes.

- However, RAD requires dedicated team effort as a major part of a RAD process rests on informal evaluation and there is no rigid set of rules defining each phase. Thus, RAD would not be feasible for a large system. On the contrary, SDLC is reliable in developing extensive systems as the processes followed in SDLC are comprehensive and exhaustive, larger systems can be developed with greater accuracy.

Answer: [a] Concept definition

Explanation: Both RAD and SDLC start off with feasibility. RAD proceeds by implementing an informal model (a skeletal model) while, an SDLC progresses in refining user requirements and then goes for implementation.

Reference No:M7123

Question: Which of the following is "TRUE" with respect to audit of software licensing?

- [a] Management need not have a license to run the software
- [b] All the employees of the company should be entitled to use the software
- [c] Procedure should exist for identifying which software is obsolete
- [d] There should be no restriction on using the software

Module 7 – Audit of Software Licensing

Software refers to various kinds of programs that are required to operate the computer and related devices. The management must ensure that the software used by the company are either licensed or are free software. In this article we focus on audit of licensed software. (Refer our article on software policy)

We shall categorise the audit of software licensing into three phases - pre-audit, audit and post audit.

Pre-audit

Inventory of the software: The auditor should obtain a list of all authorised software that is used in the organisation from the management. It should include the details regarding the

- Software, its version number and the platform on which it can run
- Number of persons entitled to use the software at a time or number of copies purchased
- Date of purchase
- Any updates done and the date on which they were done or modifications
- Proof of licence - The evidence should be substantial enough for the management to be something which the management can prove that they have a right their right to use of using the software
- Details of the systems on which the software is used
- Restriction on using the software, if any

- Maintenance agreement

Policies and procedures: Policies and procedures related to the software acquisition should be obtained to gather information on the management's guidelines on using personal software or other software that can be downloaded from the Internet and the like. He should also obtain the results of management's test on compliance with the policies and procedures, circumstances where there was non-compliance, the actions taken and the like.

Audit

Risks and their measurement: With respect to risk and their measurement the auditor should review whether

- Software purchase, its distribution , and control include an element of risk. If yes, whether a risk assessment has been made
- Risk factors that are identified by the management are appropriate
- Results of cost/benefit analysis

Compliance: The auditor must ensure that policies and procedures defined by the management are adhered to. He should ensure that

- Techniques are implemented for monitoring the compliance with the policies and procedures
- Actions taken in case of non-compliance where appropriate
- Actions taken where documented and distributed to the required users
- Where required, the non-compliance was escalated to senior management
- Instances, where the management has not implemented any techniques to ensure compliance, the auditor should conduct the compliance test

Security: The authorised software should be adequately secured by implementing both physical and logical security. The security should also extend to copyrights, license and the like. The auditor should determine the adequacy of the security methods that are implemented.

Obsolete software: The software that is no longer required or is not in use can be disposed off. Depending on the agreement with the licensor the organisation can sell, transfer or dispose of the software. The sale or transfer should include transfer of all media on which software is stored, license, and manuals. It should also be ensured that software is deleted from the computer systems and back ups. The following should be ensured with respect to obsolete software

- Process of identifying which software is obsolete
- Person responsible for identifying it
- Method of disposal
- Review of records of disposal

For the conduct of audit the auditor can use the commercial software that are available.

Post-audit: The auditor should ensure that his findings and recommendations are considered by the management and implemented where appropriate.

Answer: [c] Procedure should exist for identifying which software is obsolete

Reference No:M7124

Question: Which of the following is not security issue related to the offshore development?

- [a] Loss of adequate control
- [b] Difference of opinions between the client and the offshore developer
- [c] Increase in the complexity of the network
- [d] Increase in the revenue of the vendor

Module 7 - Offshore development and the related security issues

There has been a tremendous growth in the Indian software market. The main reason behind this is Offshore Development projects undertaken by the Indian software companies or Offshore development centres (ODC) as they are called by the outsourcers of the software. Many developed countries outsource their development activity to Asian countries owing to low development costs, availability of trained personnel and the like.

ODC may develop software for various companies or may cater to the needs of single company. The analyst of the client states the system specifications and requirements. The programs and codes are generated by the ODC. ODC can be connected to the client either through the Internet, a leased line or virtual private network. This leaves scope for vulnerabilities to creep in. Vulnerabilities could range from viruses, intrusions or unauthorised access into sensitive information of the client and the like.

Security risks related to Offshore Development

Every company is required to assess their threats and take counter measures to overcome them. The threats could be from outside the company like denial of service, networking intrusions or could be inside the company like fraud, sabotage by disgruntled employees and the like. However it may not be possible to take measures to prevent all the risks. The company should assess the estimated loss of each risk and decide on the level of risk it can tolerate. The investment in security should be proportionate to the risks.

Some of the main risks associated with the offshore development are

- **Inadequate control:** When a company out sources the development of software it has very less control about the conditions in which the software is developed. Also the company needs a regular communication with the ODC. This creates hardships for the security personnel, as he will find it difficult to authenticate the users from ODC.
- **Complexity of the network:** Complexity of the network and its continuous expansion has made its management more difficult. The access of the ODC adds more to this difficulty specially when the ODC serves many clients and is not dedicated to a single client.

- Difference of opinions: It is not necessary that the approach of the ODC and the client regarding the measures to be taken against known vulnerabilities should be the same. These could create differences and create vulnerabilities for both the ODC and his client.
- Intellectual property: When the company goes in for offshore development it has to give information about its trade secrets, data related to customers and other financial information. A company would suffer severe damages if the intellectual property were misused, as the dispute would be subject to international laws.
- Other legal issues: Data related to the customers is subject to privacy policy of the company and privacy law of the country. It is difficult for a company to ensure that the privacy policy and law are abided to by the offshore developer.

Answer: [d] Increase in the revenue of the vendor

Reference No:M7125

Question: Which of the following statements is not true about Kiviati charts?

- [a] Kiviati chart is a performance index
- [b] Kiviati chart gives a comprehensive diagrammatic representation of system utilisation
- [c] The center or the hub of a kiviati chart represents an idle processor
- [d] Accuracy in interpretation of Kiviati chart depends on user's experience and knowledge

Module 7 - Performance evaluation using Kiviati Diagrams

Introduction

In order to monitor and evaluate the performance of a system, the numeric values (or quantitative measures) should be converted to their equivalent qualitative values, i.e. for ensuring infallible performance evaluation the qualitative throughput of a system has to be accurately assessed. Performance measures can be represented by employing various charts like Gant chart, Kiviati chart, benchmark test etc.

Performance index is maintained to represent the equivalent numerical values for qualitative measures of a system. A *performance index* is a descriptor used for representing the performance level of a system (taking into consideration some of the aspects of the system). These indices are carefully defined so as to measure each and every aspect of performance of a system. E.g. 'Productivity' can be taken as a performance index class having production rate, data processing rate, maximum throughput etc as its indices. Or for example, for turnaround time, reaction time and the like can be indices of a performance index class named '*responsiveness*'.

The Kiviati graph

A Kiviati chart is a display adapted from many other related graphs that are used in performance evaluation. It gives a geometric representation for every individual performance index's (like say productivity, responsiveness etc) utilisation.

A Kiviati chart incorporates all the data required to evaluate the qualitative performance of a system, in a single chart. Thus, a Kiviati chart gives the evaluator a summary of the complete system utilisation.

How to draw a Kiviati chart

- A system comprises of a number of processors, each functioning in its own way with varying performance levels. Hence, for a comprehensive performance evaluation, an in-depth measure of qualitative utilisation of each processor has to be done. Thus, prior to drawing a Kiviati chart, each processor is represented by a spoke of wheel. Any arbitrary point on the spoke determines the recent most average fractional utilisation of each processor. The centre of the wheel is taken as 'zero' (i.e. the processor is in idle state) and outer rim of the wheel is taken as 'one' (i.e. the processor is completely busy).
- A polygon is drawn taking the points of all the processors as vertices. Since it is assumed that the center is zero and rim of the wheel is one, it can be very easily deduced that concentration of the polygon near the center indicates 'Low utilisation' and a 'High utilisation' is indicated if the polygon is towards the rim of the wheel. Thus, a good system (a balanced one) has a star like picture in a Kiviati chart.
- A strongly skewed or asymmetric polygon will show a poor load balance. Moreover, slightest change in the load balance is quite evident in the Kiviati diagram.
- 'Current utilisation' (i.e. if the processor is at the given particular instant of time) is indicated using dark shading in the graph.

A sample Kiviati chart

The following diagram illustrates how a Kiviati chart looks like. The rim of the wheel indicates that the processor is in busy state and the centre indicates that the processor is idle. Difference of opinions: It is not necessary that the approach of the ODC and the client regarding the measures to be taken against known vulnerabilities should be the same. These could create differences and create vulnerabilities for both the ODC and his client.

Merits of using a Kiviati representation

- Since, a Kiviati diagram puts down the utilisation of every processor in a system, it becomes easier for the observer to comprehend the performance of the system.
- Any problem that might be present with the working of any processor can be identified at one glance.
- Moreover, since the choice of the quantitative measures (of each processor) is arbitrary, an unbiased judgement can be formed on the performance of the system as a whole.

Limitations of Kiviati charts

- All the axes of the Kiviati diagram are taken to be of equal length, which may not be the case in practical implementation (since the measure of quality cannot be standardised).
- Extreme values i.e. the values at the rim of the wheel are always considered to be better, but a higher value of quality measure does not prove desirable always.
- Moreover, Kiviati representation is an art (since it does not have any standard or generalised interpretation) that improves with practice and continuing observation. Hence, a successful conception of a Kiviati graph totally lies in the knowledge and discretion of the user.

Answer: [a] Kiviart chart is a performance index

Reference No:M7126

Question: Which of the following must be considered before entering into software maintenance agreement?

- [a] Provisions in the agreement
- [b] Date of purchase
- [c] List price of the software
- [d] None of the above

Module 7 – IT budget

At times companies are forced to cut down their IT budgets and control their Information system purchases. This necessitates software maintenance agreement, an essential step in minimising the IT budget.

Software licensing, maintenance and technical support are the three general things that are considered in determining the price of the software at the time of purchase. Software maintenance agreement enables an IT organisation to incorporate all the modifications to the software according to the recent changes.

The cost of maintenance ranges from 10% to 90% of the cost of software depending on the type of application and vendors. Hence it is essential to negotiate well before entering into software maintenance agreements.

The following are some guidelines for software maintenance agreements that help IT organisations to minimise the cost:

5. **Provisions in the agreement:** The maintenance provisions must be clearly known before entering into an agreement. For example, an agreement may contain a provision for modifications or upgradation for Microsoft windows but may not provide the advancements like new versions of Microsoft windows.
6. **Date of commencement:** Negotiate and determine the installation date for the software in the agreement instead of installing immediately after the purchase.
7. **Price negotiation:** The price of the maintenance agreement must be determined on the basis of proper negotiation between the parties. Organisations should take care that it is not based on the list price. Further the contract must be thoroughly reviewed to evaluate its compliance with the vendor's invoice.
8. **Flexibility:** Restrictions in the agreement minimise the flexibility to change. Especially in case of mergers, vendors do not permit companies to merge their licenses and terms. Ensure that the agreement does not contain any provisions that restrict the expanding options.

Finally the benefits derived out of the maintenance agreement must be recorded by counting the number of bugs addressed by the vendor.

Organisations even have other options to minimise the expenditure rather than squeezing IT budget. Restructuring the expenditure for instance. An IT department may have to spend huge amount of resources on certain aspects, which are unavoidable. Thus, secure private networks,

encryption, virtual private networks and security are the main concerns in this context. Ignoring these or cutting the investment in security aspects may expose the business to risk. On the other hand it is essential to cut costs to release financial resources. Undertaking a cross-departmental strategy that leverage the IT investment in saving the cost of other departments will benefit the organisation as a whole. For example, a collaborative workgroup software tool implemented in the organisation will increase the cost of IT department. At the same time it reduces the travelling expenses of other departments and improves the long run productivity of the company.

Answer: [a] Provisions in the agreement

Reference No:M7127

Question: Which of the following accounting issues may cause problems while implementing accounting software?

- [a] Adequate controls to ensure the integrity of accounting data
- [b] Altering the accounting procedures whenever software is altered
- [c] Ignoring policies and procedures by employees
- [d] None of the above

Module 7 – Accounting Software

Accounting software package must improve the accounting performance of an organisation. Thus it becomes essential to analyse the accounting needs and integrate them with the software performance. Several factors need to be considered before undertaking new software. The following are some of the accounting issues that may present problems while dealing with the software.

I. Lack of controls: Without existence of proper controls any amount of investment in new software will go waste. Hence proper checks and balances must be established to ensure the integrity of accounting data.

The following are some of the controls that an organisation can incorporate while using the software

- Group the source documents into manageable size and verify the totals of these groups after posting.
- In batch processing, review all the items like dates, period and amounts before posting.
- Recheck the calculations and processed data by an alternative method if possible.
- Check the numbers at regular intervals by reconciling related things like cashbook and bank statement.

Frequent reconciliation and testing of transactions ensures the accounting data integrity.

II. Lack of appropriate procedures: Organisations usually face problems when they use the same old controls in the new accounting package. The accounting procedures must be duly altered whenever there is an alteration in the accounting software.

III. Ignoring accounting procedures: Quite often employees ignore policies and procedures designed to prevent accounting errors. Supervisors must ensure that employees follow these procedures. Proper training and encouragement must be given to employees in the usage of such procedures. They must be made readily accessible to the users.

Organisations may also consider the following issues related to software:

5. ***Optimum utilisation of the software:*** The existing software must be utilised to its fullest. It is not feasible to install new software for a single additional feature, which can actually be added by upgrading the old software or understanding the existing software.

Further an active software support agreement with the vendors and adequate training to employees ensures appropriate use of software.

6. ***Thorough understanding of software working:*** A thorough understanding of working of the software will avert problems. Monitor the defaults regularly and modify the software according to the requirements.
7. ***Discontent with the system's speed:*** Software speed is another issue. However, this can be resolved through utilities available in the packages. These utilities control the size of the files and enhance the speed of the software. Hardware aspects like operating systems and network configuration will also affect the system speed. Therefore, upgrading the hardware and monitoring the network configuration will resolve the hardware related speed problems.
8. ***Discontent with reporting capabilities:*** Many accounting packages contain built-in standard reporting formats. But organisations may find it difficult to capture the required data. Even if the data is captured, they may not be able to get it in the required format. Organisations, in such a case, need not go for new software. Redesigning the existing system can help organisations in generating useful reports.

Finally, provide continuous training on software and incorporate any upgrades to the software. Possible ways for optimum software utilisation must be identified.

Answer: [c] Ignoring policies and procedures by employees

Reference No:M7129

Question: Which of the following is not a risk factor associated with a DSS?

- [a] Simplification of models
- [b] Misuse
- [c] Confusion between theory and reality
- [d] Improper field testing

Module 7 - Decision Support Systems (DSS)-Risks

Introduction

The class of systems that aid the decision making process are termed as Decision Support Systems (DSS). Decision support systems have given ample opportunities for organisations and their decision makers to arrive at intelligent and rational decisions. DSS fits into the top level and higher middle level of an organisation as they cater to structured & unstructured information. Success of DSS depends on its proper usage and implementation. This because, DSS is being incorporated in many of the systems inherent in an organisation like file drawer systems, data analysis, accounting systems,

representational systems, optimisation systems and suggestion models. An extensive utilisation exposes it to a number of risks.

Factors responsible for poor adoption of DSS

Some of the reasons for improper functioning of the DSS in organisations could be attributed to the following:

- Improper definition of the target group and clients
- Unclear collection of inputs from the end users or target group before devising a DSS
- Mismatch of DSS with the decision making style of the organisation/its managers
- Managers are not given a proper reason for adapting a DSS and thus results in resistance to change
- Lack of proper field testing
- Lack of technical support in the form of training or orientation

Apart from these, a number of other constraints like poor marketing, knowledge transfer or dissemination, lack of training in hardware and software, short shelf life of DSS software, poor user interface and operational constraints come in the way of a successful DSS.

Risks

A DSS should be analysed for a number of risks, more so in the implementation model stage. Some of the typical risks include misuse, simplification leading to misleading outputs and confusion between model and reality.

Misuse: The decision makers could probably fall under the weight of the system by itself. That is, they could make the system responsible for any of their actions or decisions. So, it gives an alibi for the decision makers to exploit the system for their personal agenda as they could easily address the failure of any decisions to the system.

Simplification of models: A simplified model of DSS could result in giving a wrong picture of the intended outputs or results. This aspect is more important in the making of the model itself as the purpose for devising a support system must hold good for everyone in the organisation. A model aimed at economic benefits may not necessarily keep the client or end users benefit in mind.

Confusion between model and reality: The users may not be aware of the assumptions and limitations of the model underlying the making of a particular decision making system. They end up having big expectations about the software and hardware capabilities of the system. This arises due to the huge gap that exists between theory and practice.

Answer: [d] Improper field testing

Reference No:M7130

Question: Which of the following is an advantage of an automated software-testing tool?

- [a] Minimises cost and increases effectiveness
- [b] Replaces the manual testing process
- [c] Modifies the manual testing process
- [d] Develops a standalone testing environment

Module 7 - Automated software testing process

An automated software testing process is an essential requirement for software testing in today's market. It minimises the cost and increases the effectiveness of the testing process. Several automated tools are available for mainframe and GUI based applications. But companies find it difficult to implement these tools. Many are faced with problems like increased working time and difficulty in understanding. The two part series of the article provides an overview on the successful implementation of an automated testing tool.

Automated testing

Automated testing refers to mechanising the manual testing process. The essential criterion to implement the automated tools is the existence of prescribed manual testing process in the organisation. An effective manual process should have: -

- 3. Detailed test cases
- 4. A standalone testing environment

The basic purpose of automating the testing process is to minimise the work in case of repeatable tests. Repeatable tests are run to determine the unintended consequences while altering an application. Therefore, a database showing the detailed test cases must exist.

Costs and benefits

Automated testing is performed in addition to the normal manual testing. Basically, automated testing involves high cost and time if an ineffective method is used. For example, if record/playback (a feature included in many tools) method is used for testing, it takes more time than the manual testing. Therefore, a little thinking before applying the tool to the process makes it effective.

- 6. Select the tool, which is consistent with the organisational testing requirements.
- 7. The tests that are subject to repeated operation must be automated and not the one-time tests.
- 8. Avoid costly and ineffective methods like record/playback testing.
- 9. Automating the complex test process may prove to be a costly affair because of the problems involved. Hence, simple and straightforward processes are best suited for automation.
- 10. Finally, data-driven automated testing method must be selected. Data-driven methodology helps in building generic test scripts. Functional decomposition method and key word driven method are the two types of data-driven methods.

The purchasing blunder

The reason for the failure of most automated tools is blunders made at the time of purchase. For example, consider record/playback method. If this tool is selected for testing, a user may face the following problems:

- Immeasurable and unacceptable level of costs.
- The entire test has to be re-recorded in case an error is made while entering data.
- The tests also have to be re-recorded if there is any change in the application
- Unreliable scripts used
- Scripts have to be changed in case of any change in the application

In such cases an automated testing methodology is an appropriate method to ensure proper and effective testing. The following article deals with such methodologies.

Answer: [a] Minimises cost and increases effectiveness

Reference No:M7131

Question: Which of the following is an advantage of functional decomposition method of automated software testing process?

- [a] Requires less technical knowledge
- [b] Use of multiple data files for particular test case
- [c] Scripts can be aligned with higher level test script
- [d] Scripts done in spreadsheet format can be used a number of times

Module 7 – Automated software testing process – II

The first part of the article on automated software testing process dealt with the introduction and cost/benefits analysis of an automated testing method. Present article will focus on two types of data-driven automated software testing methods and the requirements for its successful implementation.

I. Functional Decomposition method:

This method is superior to record/playback method. Under this method, the test cases are minimised to their basic tasks. Such tasks are performed independently with the help of user defined, business function and utility scripts. The process includes four steps:

5. Navigation
6. Specific function
7. Data verification
8. Return navigation

Merits

- Minimises duplication of effort in developing scripts by using modular design
- Scripts can be aligned with higher-level test script easily
- Expected results, utilised for verification, are stored in simple test records

Demerits

- Requires high-level technical knowledge
- Data has to be re-entered continuously in various files
- Due care must be taken for data file format
- Usage of multiple data files for particular test case

II. Keyword driven method

It is also referred to as Test plan method. It is totally data driven method and superior to functional decomposition method. Key words are used to perform specific functions by processing input parameters. Template for a test case is developed through spreadsheet program. Copying this template can perform additional test cases.

Merits

- Scripts do not have to be written again once done in spreadsheet format
- Scope for reusing the generic utility tests
- Translation of any existing format into spreadsheet is not difficult

Demerits

- Requires knowledge of scripting language for customised function development
- In case of more number of functions, more keywords have to be learnt by testers. It consumes time.

Change management

While adopting an automated testing tool, an enterprise may face resistance to change from tester. This is because tester involvement is less in tool selection. Therefore, management should have a definite approach to manage these changes. For instance the following are some of

the fears of testers and the solutions to tackle those:

- 1. Complete replacement:** Testers fear that if an automated tool is implemented manual requirement will be reduced. However it is a helpful tool for testers. It saves their time and effort.
- 2. Training:** Training on the new tool involves much time. But in reality it is not so. For example, test-plan method requires only minimal learning on spreadsheet usage.
- 3. Difficulty in usage:** Testers in fact do not use it. A test tool specialist appointed specifically for the purpose uses it.

Staff selection

A senior level programmer is an appropriate person for the position of test tool specialist. However, it is not specifically required. The following are his functions:

- Establishing automated scripts
- Establishing procedures and standards
- Framing procedures for managing change
- Establishing required infrastructure
- Managing and executing the test scripts
- Test running and furnishing results to testers

Answer: [c] Scripts can be aligned with higher-level test script

Reference No:M7132

Question: Which of the following is not expected of an RFP (Request for Proposal)?

- [a] Specifications
- [b] Time saving
- [c] Sending to prospective vendors
- [d] Sending outside for budget planning

Module 7 – Request for proposal

What is a RFP?

A Request For Proposal (RFP) is a formal procedure followed by companies to notify vendors or service providers that they intend to purchase goods and/or services and invite proposals. Large organisations invest huge amounts of money to purchase good and services from vendors.

Purpose

RFP's are developed and implemented in order to:

- Ensure that vendors deliver the product or service as per the customers' requirements.

- Institute and standardise the vendor's proposal for the purpose of easy understanding, analysis, interpretation and comparison.
- Notify the vendors that the purchase is bid competitively.

Instructions

A typical RFP contains instructions to the vendor on the following aspects:

Specifications: RFPs must furnish detailed information on the specifications of the product or service the buyer is seeking.

Proposal Content: This contains specific instructions on how the response (a proposal) should be crafted or prepared.

Timing: Some questions like "when does the business expect the proposals?" are to be addressed here. More precisely, it is known as the RFP close date. This allows the company issuing the RFP to plan and schedule their decision-making process.

Benefits

Product Purchase Satisfaction: The buyer is able to set criteria to evaluate proposals by using an RFP. It makes it clear to vendors that proposals not living up to the requirements mentioned in the RFP will not be entertained. If not for RFP's, buyers would end up buying things whatever comes their way. This would result in customer dissatisfaction due to improper communication about the product.

Product Price Satisfaction: With the help of an RFP all the vendors know that many others are bidding for the purchase. This shall give the vendor an incentive for a best price on the first proposal.

Vendor Product Comparison: Once the RFP has expired and the buyer has proposals, comparisons are possible because the vendor has responded to a common set of requirements.

Time Savings: Though the time taken to devise an RFP is more, the time spent preparing an RFP is relatively more when compared to the time devoted on explaining the requirements to every vendor and making the best price quote. Buyers are in no way bound to waste time with vendors who are not in a position to deliver the product or services they require.

Distribution of the RFP

The RFP's are to be sent eight to ten weeks before the requested submission date. This is because, writing a detailed proposal takes time, and there should be enough time provided for potential vendors to think about and respond to the RFP's.

- The RFPs are to be distributed to the vendors who have been identified as being able to produce the materials that the buyer wants
- RFP's are not to be sent to organisations with which the buyer has no intention to work
- An in-house project should not be sent to an outside party for project planning
- RFP's should not be sent outside for planning the budget

Answer: [d] Sending outside for budget planning

Reference No:M7133

Question: The internal logic of the program is tested by which one of the following test: -

- [a] Black box
- [b] white box
- [c] Unit test
- [d] Integration test

Module 7 – Comparison between Black box testing and White box testing

Testing

Testing is one of the most important elements of software quality assurance. Testing is executing the software application intended to check for as many errors as possible, before the software is delivered to the customer.

There are basically two types of testing: -

3. White box testing
4. Black box testing

White box testing is performed at early stage of the testing process while black box testing is performed at the later stage. This is due to the reason that black box testing deliberately neglects the control structures and the focus is shifted towards information domain.

White box testing

Also called glass box testing, it is conducted on code component of the software by analysing the internal working of a software product. Different tests are performed to ensure that all the internal processes and functions are carried out according to specifications. White box testing can be done only by close examination of procedural details. Hence specific programming knowledge is required to determine the output.

White box testing helps in ascertaining that:

- All the independent paths in a program are executed at least once.
- All logical decisions are taken as intended.
- All the loops in a program are started and terminated as desired.
- Internal data structure has been checked for their validity.
- Internal interfaces are verified for reliability.

Pros and cons of white box testing

Pros

- Developers can verify the functionality of their components at the time of software development cycle.

- Quality assurance time is reduced as the assembled product has fewer bugs.

Cons

- It is very expensive
- Not suitable for large applications
- It is time consuming process

Black box testing

It is also called behavioral testing. It is done by understanding the specific function (s) that the software product is designed to perform. A series of tests are conducted to know that all the functions are being carried out accordingly, inputs are being properly accepted and desired outputs are delivered. Simultaneously, black box tests find errors in each function. Black box testing is no alternative to white box testing but it is an integral approach which covers different set of errors than that of white box testing. Black box testing is done to: -

- Identify incorrect and unnoticed functions
- Identify all external interface errors
- Check errors in data structure
- Identify problems in database access
- Check behavioral and performance errors
- Validate the capability of system hardware and software to recover the loss due to external or environmental threats.

Pros and cons of black box testing

Pros

- Black box testing is done from end user perspective
- Tester need not to know about internal working of the program
- One can even test the environment in which the program is executed
- The resources and effort used for testing can be used multiple times.

Cons

- ❑ Requirements should be clear and unambiguous otherwise difficulty in test cases is possible
- ❑ All properties of a software product cannot be tested
- ❑ The reason behind the failure of any functionality cannot be identified.

Answer: [b] White box

End

[illegible]