

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

Question no. 1 is compulsory

Attempt any four question from the remaining six questions

Question 1.

XYZ Company, engaged in the manufacturing of several types of electronic goods is having its branches all over the World. The company wishes to centralize and consolidate the information flowing from its branches in a uniform manner across various levels of the Organization.

The factories are already working on legacy systems using an intranet and collating information. But each factory and branch is using different software and varied platforms, which do not communicate with each other. This not only results in huge inflow of data which could not be consolidated for analysis but also the duplication of data. Even one percent change in any data entry or analysis translates into millions of Rupees and can sometimes wipe out the profits of the organization. So the company needs a system that would help them to be responsive and act fast.

Read the above carefully and answer the following with justifications:

- (a) What are the problems that the company is facing now? (5 Marks)
- (b) Should the company go for ERP solution? If yes, will the company be able to share a common platform with its dealers to access servers and database to update the information of issues of mutual interest? (5 Marks)
- (c) For the selection of ERP package, state the issues to be considered. (5 Marks)
- (d) Suggest how to go about the implementation of ERP package. (5 Marks)

Answer

- (a) XYZ company, having its branches all over the world, is engaged in manufacturing of several types of electronic goods. It is confronted with the problem of centralizing and consolidating the information flowing in from its various branches in uniform manner across various levels of the organization.

No doubt, the factories are working on legacy systems using an intranet and collating information. As each factory is using different type of software on varied platforms, therefore, they are not able to communicate with each other. Because of this reason, there is a huge inflow of data which could not be consolidated for analysis. Lack of communication among factories has not only resulted into duplication of the data entry which is not only costly, slight change in data entry and analysis may translate into millions of rupees that can sometimes wipe out the profits of the organization. Hence, there is an urgent need of a system that would help the branches to be responsive and to act fast.

- (b) Yes, the company should go for ERP solutions. ERP implementation brings different business functions, personalities, procedures, ideologies and philosophies on one platform, with an aim to pool knowledge base to effectively integrate and bring worthwhile and beneficial changes throughout the organization. Some of the major features of ERP

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

are that it provides the support to multi platform, multi facility, multi mode, manufacturing, multi currency, multi lingual facilities. It supports strategic and business planning activities, operational planning and execution activities, creation of material and resources. All these functions are effectively integrated for flow and updation of information immediately upon entry of any information, thereby providing a company-wide Integrated Information System.

In case, the company decides to include a module for dealers which provides limited/restricted access to company databases and server, dealers will be able to update the information of issues of mutual interest.

- (c) While selecting the ERP package, the performance of following issues should be taken into account:
 - (i) Better inventory management and control.
 - (ii) Improved financial reporting and control.
 - (iii) Automation of certain tasks that were performed manually to increase productivity.
 - (iv) Improved production planning.
 - (v) Better information on stocks at various locations.
 - (vi) Using an integrated system as opposed to disparate systems at different locations, thereby eliminating errors of duplicate entries.
 - (vii) More accurate costing of products.
 - (viii) Better credit control.
 - (ix) Improved cash flow planning.
 - (x) Automatic quality control and tracking.
 - (xi) Better after sales services.
 - (xii) Better information and reporting to top management.
- (d) In the stated scenario, several steps involved in the implementation of a typical ERP package are enumerated below:
 - (i) Identifying the needs for implementing an ERP package.
 - (ii) Evaluating the 'As Is' situation of the business i.e., to understand the strength and weakness prevailing under the existing circumstances.
 - (iii) Deciding the 'Would be' situation for the business i.e., the changes expected after the implementation of ERP.
 - (iv) Reengineering the Business Process to achieve the desired results in the existing processes.
 - (v) Evaluating the various available ERP packages to assess suitability.
 - (vi) Finalizing of the most suitable ERP package for implementation.
 - (vii) Installing the required hardware and networks for the selected ERP package.

FINAL EXAMINATION : JUNE, 2009

(viii) Finalizing the Implementation consultants who will assist in implementation.

(ix) Implementing the ERP package.

Question 2.

(a) The top management of company has decided to develop a computer information system for its operations. Is it essential to conduct the feasibility study of system before implementing it? If answer is yes, state the reasons. Also discuss three different angles through which the feasibility study of the system is to be conducted.

(10 Marks)

(b) "While reviewing a client's control system, an information system auditor will identify three components of internal control." State and briefly explain these three components.

(5 Marks)

(c) While testing a software, how will you involve the people working in the system areas?

(5 Marks)

Answer

(a) Yes, it is essential to carry out the feasibility study of the project before its implementation. After possible solution options are identified, project feasibility-the likelihood that these systems will be useful for the organization-is determined. A feasibility study is carried out by the system analysts for this purpose. Feasibility study refers to a process of evaluating alternative systems through cost/benefit analysis so that the most feasible and desirable system can be selected for development. It is carried out by the system analysts.

The feasibility study of the system is undertaken from three angles i.e. technical, economic and operational. The proposed system is evaluated from a technical view point first and if technically feasible, its impact on the organization and staff is assessed. If a compatible technical and social system can be devised, it is then tested for economic feasibility.

Technical feasibility: It is concerned with hardware and software. Essentially, the analyst ascertains whether the proposed system is feasible with existing or expected computer hardware and software technology. The technical issues usually raised during the feasibility stage of investigation include the following:

(i) Does the necessary technology exist to do what is suggested (and can it be acquired)?

(ii) Does the proposed equipment have the technical capacity to hold the data required to use the new system?

(iii) Will the proposed system provide an adequate response to inquires, regardless of the number or location of users?

(iv) Can the system be expanded if developed?

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- (v) Are there technical guarantees of accuracy, reliability, ease of access, the data security?

Some of the technical issues to be considered are given in the Table-1 below.

Design Considerations	Design Alternatives
Communications channel configuration	Point to point, multidrop, or line sharing
Communications channels	Telephone lines, coaxial cable, fiber optics, microwave, or satellite
Communications network	Centralized, decentralized, distributed, or local area
Computer programs	Independent vendor or in-house
Data storage medium	Tape, floppy disk, hard disk, or hard copy
Data storage structure	Files or database
File organization and access	Direct access or sequential files
Input medium	Keying, OCR, MICR, POS, EDI, or voice recognition
Operations	In-house or outsourcing
Output frequency	Instantaneous, hourly, daily, weekly, or monthly
Output medium	CRT, hard copy, voice, or turnaround document
Output scheduling	Predetermined times or on demand
Printed output	Preprinted forms or system-generated forms
Processor	Micro, mini, or mainframe
Transaction processing	Batch or online
Update frequency	Instantaneous, hourly, daily, weekly, or monthly

Table-1: Technical Issues

Due to tremendous advancements in computer field these days, the technology is available for most business data processing systems but sometimes not within the constraints of the firm's resources or its implementation schedule. Therefore, trade offs are often necessary. A technically feasible system may not be economically feasible or may be so sophisticated that the firm's personnel cannot effectively operate it.

Economic feasibility: It includes an evaluation of all the incremental costs and benefits expected if the proposed system is implemented. This is the most difficult aspect of the study. The financial and economic questions raised by analysts during the preliminary investigation are for the purpose of estimating the following:

- (i) The cost of conducting a full system's investigation.
- (ii) The cost of hardware and software for the class of applications being considered.
- (iii) The benefits in the form of reduced costs or fewer costly errors.

FINAL EXAMINATION : JUNE, 2009

- (iv) The cost if nothing changes (i.e. the proposed system is not developed).

The procedure employed is the traditional cost-benefit study.

Operational feasibility: It is concerned with ascertaining the views of workers, employees, customers and suppliers about the use of computer facility. The support or lack of support that the firm's employees are likely to give to the system is a critical aspect of feasibility. A system can be highly feasible in all respects except s the operational and fails miserably because of human problems. Some of the questions which may help in conducting the operational feasibility of a project are stated below:

- (i) Is there sufficient support for the system from management? From users? If the current system is well liked and used to the extent that persons will not be able to see reasons for a change, there may be resistance.
 - (ii) Are current business methods acceptable to user? If they are not, users may welcome a change that will bring about a more operational and useful system.
 - (iii) Have the users been involved in planning and development of the project? Early involvement reduces the chances of resistance to the system and changes in general and increases the likelihood successful projects.
 - (iv) Will the proposed system cause harm? Will it produce poorer results in any respect or area? Will loss of control results in any areas? Will accessibility of information be lost? Will individual performance be poorer after implementation than before? Will performance be affected in an undesirable way? Will the system slow performance in any areas?
- (b) The basic purpose of information system controls in an organization is to ensure that the business objectives are achieved and undesired risk events are prevented or detected and corrected. This is achieved by designing an effective information control framework, which comprises of policies, procedures, practices, and organization structure to give reasonable assurances that the business objectives will be achieved.

While reviewing a client's control systems, the auditor will be able to identify three components of internal controls. Each component is aimed at achieving different objectives as stated below:

- (i) **Accounting Controls:** These controls are extended to safeguard the client's assets and ensure reliability of financial records.
 - (ii) **Operational Controls:** These deal with the day to day operations, functions and activities to ensure that the operational activities are contributing to business objectives.
 - (iii) **Administrative Control:** These are concerned with ensuring efficiency and compliance with management policies, including the operational controls.
- (c) Following are the main testing techniques which involve the people working in the system areas:
- (i) **White Box Testing:** White box testing is a test case design method that uses the control structure of the procedural design to derive test cases. Test cases can be derived to

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- guarantee that all independent paths within a module have been exercised at least once,
 - exercise all logical decisions on their true and false sides,
 - execute all loops at their boundaries and within their operational bounds, and
 - exercise internal data structures to ensure their validity
- (ii) Unit Testing: In computer programming, a unit test is a method of testing the correctness of a particular module of source code. The idea is to write test cases for every non-trivial function or method in the module so that each test case is separate from the others if possible. This type of testing is mostly done by the developers.
- (iii) Requirements Testing: These test conditions are generalized ones, which become test cases as the SDLC progresses until system is fully operational. The main usage of this testing technique is
- to ensure that system performs correctly
 - to ensure that correctness can be sustained for a considerable period of time.
 - system can be tested for correctness through all phases of SDLC but in case of reliability the programs should be in place to make system operational.
- (iv) Regression Testing: Under this testing technique, test cases, which were used previously for the already tested segment are, re-run to ensure that the results of the segment tested currently and the results of same segment being tested earlier, are same. Test automation is needed to carry out the test transactions (test condition execution) else the process is very time consuming and tedious. In this case of testing, cost/benefit should be carefully evaluated else the efforts spent on testing would be more and payback would be minimum. The major objectives are as follows:
- System documents remain current.
 - System test data and test conditions remain current.
 - Previously tested system functions properly without getting effected though changes are made in some other segment of application system.
- (v) Manual Support Testing: It involves testing of all the functions performed by the people while preparing the data and using these data from automated system. The major objectives of this testing technique are to
- verify that manual support documents and procedures are correct,
 - determine that manual support responsibility is correct,
 - determine that manual support people are adequately trained,
 - determine that manual support and automated segment are properly interfaced.

FINAL EXAMINATION : JUNE, 2009

- (vi) Internal System Testing: This technique is used to ensure interconnection between application functions correctly. The major objectives of the testing are to ensure that
- proper parameters and data are correctly passed between the applications,
 - documentation for involved system is correct and accurate,
 - proper timing and coordination of functions exists between the application systems.

Question 3.

- (a) A company is engaged in the stores taking data activities. Whenever, input data error occurs, the entire stock data is to be reprocessed at a cost of Rs. 50,000. The management has decided to introduce a data validation step that would reduce errors from 12% to 0.5% at a cost of Rs. 2,000 per stock taking period. The time taken for validation causes an additional cost of Rs. 200. (i) Evaluate the percentage of cost-benefit effectiveness of the decision taken by the management and (ii) suggest preventive control measures to avoid errors for improvement. (10 Marks)
- (b) What are the issues that should be considered by a system auditor at post implementation review stage before preparing the audit report? (5 Marks)
- (c) "Always, there exist some threats due to Cyber Crimes." Explain these threats. (5 Marks)

Answer

- (a) (i) The percentage of cost benefit effectiveness based on the information is calculated in the following table:

S. No.	Particulars	Without validation Procedure	With Validation Procedure
1.	Cost of reprocessing the stock data	Rs. 50,000	Rs. 50,000
2.	Risk of data errors	12%	0.5%
3.	Expected processing cost	Rs. 6,000	Rs. 250
4.	Cost of validation procedure	Nil	Rs. 2,000
5.	Cost of delay due to validation	Nil	Rs. 200
6.	Total cost involved	Rs. 56,000	Rs. 52,450
7.	Net expected benefit		Rs. 3,550
	in %		6.3%

Hence there is 6.3% cost benefit effectiveness of the decision taken by the management.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

(ii) Preventive Control Measures

Preventive controls are those inputs, which are designed to prevent an error, omission or malicious act occurring. An example of a preventive control is the use of passwords to gain access to a financial system. The broad characteristics of preventive controls are:

- (i) A clear-cut understanding about the vulnerabilities of the asset.
- (ii) Understanding probable threats.
- (iii) Provision of necessary controls for probable threats from materializing.

Any control can be implemented in both manual and computerized environment for the same purpose. Only the implementation methodology may differ from one environment to the other.

Some of the major preventive controls to avoid errors are as follows:

- Employ qualified personnel
- Segregation of duty
- Access controls
- Vaccination against disease
- Maintain proper documentation
- Prescribing appropriate books for a course
- Training and retraining of personnel
- Authorization of transactions
- Validation, edit checks in the application programmes
- Firewalls
- Anti-virus software
- Passwords

The above list in no way is exhaustive, but is a mix of manual and computerized preventive controls. The following table enumerates the kind of manual controls and computerized controls applied to a similar scenario.

Scenario	Manual Control	Computerized Control
Restrict unauthorized entry into the premises	Build a gate and post a security guard.	Use access control software, smart card, biometrics, etc.
Restricted unauthorized entry into the software applications	Keep the computer in a secured location and allow only authorized person to use the applications.	Use access control, viz. User ID, password, smart card, etc.

Table-2: Manual & Computerized Controls

FINAL EXAMINATION : JUNE, 2009

- (b) An auditor will consider following issues at PIR (Post Implementation Review) stage before preparing the audit report:
- (i) Interview business users in each functional area covered by the system, and assess their satisfaction with, and overall use of, the system.
 - (ii) Interview security, operations and maintenance staff and, within the context of their particular responsibilities, assess their reactions to the system.
 - (iii) Based on the User Requirements Specification, determine whether the system's requirements have been met. Identify the reasons(s) why any requirements are not to be provided, are yet to be delivered, or which do not work properly.
 - (iv) Confirm that the previous system has been de-commissioned or establish the reasons(s) why it remains in use.
 - (v) Review system problem reports and change proposals to establish the number and nature (routine, significant, major) of problems, and changes being made to remedy them. The volume of system change activity can provide an indicator of the quality of systems development.
 - (vi) Confirm that adequate internal controls have been built into the system, that these are adequately documented, and that they are being operated correctly. Review the number and nature of internal control rejections to determine whether there are any underlying system design weaknesses.
 - (vii) Confirm that an adequate Service Level Agreement has been drawn up and implemented. Identify and report on any area where service delivery either falls below the level specified, or is inadequate in terms of what was specified.
 - (viii) Confirm that the system is being backed up in accordance with user requirements, and that it has been successfully restored from backup media.
 - (ix) Review the Business Case and determine whether:
 - anticipate benefits have / are been achieved;
 - any unplanned benefits have been identified;
 - costs are in line with those estimated;
 - benefits and costs are falling with the anticipated time-frame.
 - (x) Review trends in transaction throughput and growth in storage use to identify that the anticipated growth of the system is in line with the forecast.
- (c) Any computerized environment is dependent on people. Though they play a critical role in success of an enterprise computing, it is a fact that threats always exist due to cyber crimes committed by people. The special skill sets of IT operational team, programmers; data administrator, etc. are key links in ensuring that the IT infrastructure delivers output as per user requirements. At the same time, social engineering risks target key persons to get sensitive information to exploit the information resources of the enterprise. Threats also arise on account of dependence on external agencies. IT computing

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

services are significantly dependant on various vendors and service providers for equipment supply and support, consumables, systems and program maintenance, air-conditioning, hot-site providers, utilities, etc. Following are some of the serious threats due to cyber crimes:

- **Embezzlement:** It is unlawful misappropriation of money or other things of value, by the person to whom it was entrusted (typically an employee), for his/her own use or purpose.
- **Fraud:** It occurs on account of internal misrepresentation of information or identity to deceive others, the unlawful use of credit/debit card or ATM, or the use of electronic means to transmit deceptive information, to obtain money or other things of value. Fraud may be committed by someone inside or outside the company.
- **Theft of proprietary information:** It is illegal to obtain of designs, plans, blueprints, codes, computer programs, formulas, recipes, trade secrets, graphics, copyrighted material, data, forms, files, lists, and personal or financial information, usually by electronic copying.
- **Denial of service:** There can be disruption or degradation of service that is dependent on external infrastructure. Problems may erupt through internet connection or e-mail service that result in an interruption of the normal flow of information. Denial of service is usually caused by events such as ping attacks, port scanning probes, and excessive amounts of incoming data.
- **Vandalism or sabotage:** It is the deliberate or malicious, damage, defacement, destruction or other alteration of electronic files, data, web pages, and programs.
- **Computer virus:** Viruses are hidden fragments of computer codes which propagates by inserting themself into or modifying other programs.
- **Other:** Threat includes several other cases such as intrusion, breaches and compromises of the respondent's computer networks (such as hacking or sniffing) regardless of whether damage or loss were sustained as a result.

Question 4.

- (a) As a system auditor, what control measures will you check to minimize threats, risks and exposures in a computerized system? (10 Marks)
- (b) State and explain four commonly used techniques to assess and evaluate risks. (5 Marks)
- (c) What are the audit tools and techniques used by a system auditor to ensure that disaster recovery plan is in order? Briefly explain them. (5 Marks)

Answer

- (a) To minimize threats to the confidentiality, integrity, and availability, of data and computer systems and for successful business continuity, the system auditor should evaluate

FINAL EXAMINATION : JUNE, 2009

potential threats to computer systems. Discussed hereunder are various control measures that will be checked by him to minimize threats, risks and exposures in a computerized system:

- (i) Lack of integrity : Control measures to ensure integrity include implementation of security policies, procedures and standards, use of encryption techniques and digital signatures, inclusion of data validation, editing, and reconciliation techniques for inputs, processes and outputs, updated antivirus software, division of job and layered control to prevent impersonation, use of disk repair utility, implementation of user identification, authentication and access control techniques, backup of system and data, security awareness programs and training of employees, installation of audit trails, audit of adequacy of data integrity.
- (ii) Lack of confidentiality: Control measures to ensure confidentiality include use of encryption techniques and digital signatures, implementation of a system of accountability by logging and journaling system activity, development of a security policy procedure and standard, employee awareness and training, requiring employees to sign a non-disclosure undertaking, implementation of physical and logical access controls, use of passwords and other authentication techniques, establishment of a documentation and distribution schedule, secure storage of important media and data files, installation of audit trails, and audit of confidentiality of data.
- (iii) Lack of system availability: Control measures to ensure availability include implementation of software configuration controls, a fault tolerant hardware and software for continuous usage and an asset management software to control inventory of hardware and software, insurance coverage, system backup procedure to be implemented, implementation of physical and logical access controls, use of passwords and other authentication techniques, incident logging and report procedure, backup power supply, updated antivirus software, security awareness programmes and training of employees, installation of audit trails, audit of adequacy of availability safeguards.
- (iv) Unauthorized users attempt to gain access to the system and system resources: Control measures to stop unauthorized users to gain access to system and system resources include identification and authentication mechanism such as passwords, biometric recognition devices, tokens, logical and physical access controls, smart cards, disallowing the sharing of passwords, use of encryption and checksum, display of warning messages and regular audit programs.

Data transmitted over a public or shared network may be intercepted by an unauthorized user, security breaches may occur due to improper use or bypass of available security features, strong identification and authentication mechanisms such as biometric, tokens, layered system access controls, documentation procedures, quality assurance controls and auditing.

- (v) Hostile software e.g. virus, worm, Trojan horses, etc.: Establishment of policies regarding sharing and external software usage, updated anti-virus software with

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

detection, identification and removal tools, use of diskless PCs and workstations, installation of intrusion detection tools and network filter tools such as firewalls, use of checksums, cryptographic checksums and error detection tools for sensitive data, installation of change detection tools, protection with permissions required for the 'write' function.

- (vi) Disgruntled employees: Control measures to include installation of physical and logical access controls, logging and notification of unsuccessful logins, use of disconnect feature on multiple unsuccessful logins, protection of modem and network devices, installation of one time use only passwords, security awareness programs and training of employees, application of motivation theories, job enrichment and job rotation.
 - (vii) Hackers and computer crimes: Control measures to include installation of firewall and intrusion detection systems, change of passwords frequently, installation of one time use passwords, discontinuance of use of installed and vendor installed passwords, use of encryption techniques while storage and transmission of data, use of digital signatures, security of modem lines with dial back modems, use of message authentication code mechanisms, installation of programs that control change procedures, and prevent unauthorized changes to programs, installation of logging feature and audit trails for sensitive information.
 - (viii) Terrorism and industrial espionage: Control measures to include usage of traffic padding and flooding techniques to confuse intruders, use of encryption during program and data storage, use of network configuration controls, implementation of security labels on sensitive files, usage of real-time user identification to detect masquerading, installation of intrusion detection programs.
- (b) Four most commonly used techniques to access and evaluate risks are:
- Judgment and intuition
 - The Delphi Approach
 - Scoring
 - Quantitative Techniques

A brief discussion on each of them is given as follows:

- (i) Judgment and intuition: In many situations, the auditors have to use their judgment and intuition for risk assessment. This mainly depends on the personal and professional experience of the auditors and their understanding of the system and its environment. Together with it, systematic education and ongoing professional updating is also required.
- (ii) The Delphi Approach: This techniques is used for obtaining a consensus opinion. A panel of experts is engaged and each expert is asked to give his opinion in a written and independent method. They enlist the estimate of the cost benefits and the reasons why a particular system is to be chosen, the risks and exposures of the system. These estimates are then compiled together. The estimates falling within a

FINAL EXAMINATION : JUNE, 2009

pre-decided acceptable range are taken. The process may be repeated four times for revising estimates falling beyond the range. Then a curve is drawn taking all the estimates as points on the graphs. The median is drawn and this is the consensus opinion.

- (iii) **The Scoring Approach:** In this approach, the risks in the system and their respective exposures are listed. Weights are then assigned to the risks and to the exposures depending on the severity, impact of occurrence and costs involved. The product of the risk weight with the exposure weight of every characteristic gives the weighted score. The sum of these weighted score gives the risk and exposure score of the system. System risks and exposures are then ranked according to the scores.
 - (iv) **Quantitative Techniques:** Quantitative techniques involve the calculating of an annual loss exposure value based on the probability of the event and the exposure in terms of estimated costs. This helps the organization to select cost effective solutions. It is the assessment of potential damage in the event of occurrence of unfavorable events, keeping in mind how often such an event may occur.
- (c) Audit tools and techniques used by a system auditor to ensure that the disaster recovery plan is in order, are briefly discussed below:

The best audit tool and technique is a periodic simulation of a disaster. Other audit techniques would include observations, interviews, checklists, inquiries, meetings, questionnaires and documentation reviews. These are categorized as follows:

- (i) **Automated tools:** They make it possible to review large computer systems for a variety of flaws in a short time period. They can be used to find threats and vulnerabilities such as weak access controls, weak passwords, and lack of integrity of the system software.
- (ii) **Internal Control auditing:** This includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance for laws and regulations.
- (iii) **Disaster and Security Checklists:** These checklists are used to audit the system. The checklists should be based upon disaster recovery policies and practices, which form the baseline. Checklists can also be used to verify changes to the system from contingency point of view.
- (iv) **Penetration Testing:** It is used to locate vulnerabilities to the system.

Question 5.

- (a) When an organization is audited for the effective implementation of ISO 27001-(BS 7799: part II)-Information Security Management System, what are to be verified under.

(10 Marks)

- (i) Establishing Management Framework
- (ii) Implementation
- (iii) Documentation.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- (b) The Information Security Policy of an organization has been defined and documented as given below:

“Our organization is committed to ensure Information Security through established goals and principles. Responsibilities for implementing every aspect of specific applicable proprietary and general principles, standards and compliance requirements have been defined. This is reviewed at least once a year for continued suitability with regard to cost and technological changes.”

Identify the salient components that have not been covered in the above policy. (5 Marks)

- (c) Briefly explain Asset Classification and Control under Information Security Management Systems. (5 Marks)

Answer

- (a) ISO 27001 –(BS7799: Part II) – Specification for Information Security Management Systems

It deals with the Information Security Management Standard (ISMS). In general, organizations shall establish and maintain documented ISMS addressing assets to be protected, organization approach to risk management, control objectives and control, and degree of assurance required.

- (i) Establishing Management Framework: This would include the following activities:
- Define information security policy;
 - Define scope of ISMS including functional, asset, technical, and locational boundaries;
 - Make appropriate risk assessment ;
 - Identify areas of risk to be managed and degree of assurance required;
 - Select appropriate controls;
 - Prepare Statement of Applicability.
- (ii) Implementation: Effectiveness of procedures to implement controls to be verified while reviewing security policy and technical compliance.
- (iii) Documentation: The documentation shall consist of evidence of action undertaken under establishment of the following:
- Management control
 - Management framework summary, security policy, control objective, and implemented control given in prepare Statement of Applicability
 - Procedure adopted to implement control under Implementation clause
 - ISMS management procedure
 - Document Control: The issues focused under this clause would be

FINAL EXAMINATION : JUNE, 2009

- o Ready availability
 - o Periodic review
 - o Maintain version control;
 - o Withdrawal when obsolete
 - o Preservation for legal purpose
 - Records: The issues involved in record maintenance are as follows:
 - o Maintain to evidence compliance to Part 2 of BS7799.;
 - o Procedure for identifying, maintaining, retaining, and disposing of such evidence;
 - o Records to be legible, identifiable and traceable to activity involved.
 - o Storage to augment retrieval, and protection against damage.
- (b) A Policy is a plan or course of action, designed to influence and determine decisions, actions and other matters. The security policy is a set of laws, rules, and practices that regulates how assets including sensitive information are managed, protected, and distributed within the user organization.

An information Security policy addresses many issues such as disclosure, integrity and availability concerns, who may access what information and in what manner, basis on which access decision is made, maximized sharing versus least privilege, separation of duties, who controls and who owns the information, and authority issues.

Issues to address: This policy does not need to be extremely extensive, but clearly state senior management's commitment to information security, be under change and version control and be signed by the appropriate senior manager. The policy should at least address the following issues:

- a definition of information security,
- reasons why information security is important to the organization, and its goals and principles,
- a brief explanation of the security policies, principles, standards and compliance requirements,
- definition of all relevant information security responsibilities, and
- reference to supporting documentation.

The auditor should ensure that the policy is readily accessible to all employees and that all employees are aware of its existence and understand its contents. The policy may be a stand-alone statement or part of more extensive documentation (e.g. a security policy manual) that defines how the information security policy is implemented in the organization. In general, most if not all employees covered by the ISMS scope will have some responsibilities for information security, and auditors should review any

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

declarations to the contrary with care. The auditor should also ensure that the policy has an owner who is responsible for its maintenance and that it is updated responding to any changes affecting the basis of the original risk assessment.

In the stated scenario of the question, the ISMS Policy of the given organization does not address the following issues:

- (i) Definition of information security,
 - (ii) Reasons why information security is important to the organization,
 - (iii) A brief explanation of the security policies, principles, standards and compliance, and
 - (iv) Reference to supporting documents.
- (c) Asset Classification and Control

One of the most laborious but essential task is to manage inventory of all the IT assets, which could be information assets, software assets, physical assets or other similar services. These information assets need to be classified to indicate the degree of protection. The classification should result into appropriate information labeling to indicate whether it is sensitive or critical and what procedure, is appropriate to copy, store, transmit or destruction of the information asset.

An Information Asset Register (IAR) should be created detailing each of the following information asset within the organization:

- Databases
- Personnel records
- Scale models
- Prototypes
- Test samples
- Contracts
- Software licenses
- Publicity material

The Information Asset Register (IAR) should also describe who is responsible for each information asset and whether there is any special requirement for confidentiality, integrity or availability. For administrative convenience, separate register may be maintained under the subject head of IAR e.g. 'Media Register' will detail the stock of software and its licenses. One major advantage of following this practice is that, it provides a good back-up for example, in case the carton/label containing password is accidentally misplaced, media register will provide the necessary information. Similarly, 'Contracts Register' will contain the contracts signed and thus other details. The impact that is an addendum to mere maintenance of a register is control and thus protection of

FINAL EXAMINATION : JUNE, 2009

valuable assets of the corporation. The value of each asset can then be determined to ensure that appropriate security is in place.

The detailed control and objectives thereof are as follows:

- Accountability for assets: to maintain appropriate protection of organizational assets,
- Information Classification: to ensure that information assets receive an appropriate level of protection.

Question 6.

- (a) What purpose the information system audit policy will serve? Briefly describe the scope of information system audit. (10 Marks)
- (b) State the duties of the subscriber of a digital signature as specified in Section 40 to 42 of Chapter VIII of Information Technology Act, 2000. (5 Marks)
- (c) What are the conditions subject to which electronic record may be authenticated by means of affixing digital signature? (5 Marks)

Answer

- (a) Purpose of the Audit Policy

Purpose of the audit policy is to provide the guidelines to the audit team to conduct an audit of IT based infrastructure system. The Audit is done to protect entire system from the most common security threats which includes the following:

- Access to confidential data
- Unauthorized access of the department computers
- Password disclosure compromise
- Virus infections
- Denial of service attacks
- Open ports, which may be accessed by outsiders
- Unrestricted modems, unnecessarily open ports

Audits may be conducted to ensure integrity, confidentiality and availability of information and resources. The IS Audit Policy should lay out the objective and the scope of the Policy.

An IS audit is conducted to:

- Safeguarding of Information System Assets/Resources
- Maintenance of Data Integrity
- Maintenance of System Effectiveness
- Ensuring System Efficiency

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- Compliance with Information System related policies, guidelines, circulars, and any other instructions requiring compliance in whatever name called.

Scope of IS Audit

The scope of information system auditing should encompass the examination and evaluation of the adequacy and effectiveness of the system of internal control and the quality of performance by the information system. Information System Audit will examine and evaluate the planning, organizing, and directing processes to determine whether reasonable assurance exists that objectives and goals will be achieved. Such evaluation, in the aggregate, provides information to appraise the overall system of internal control.

The scope of the audit will also include the internal control system (s) for the use and protection of information and the information system, as under:

- Data
- Application systems
- Technology
- Facilities
- People

The information System auditor will consider whether the information obtained from the above reviews indicates coverage of the appropriate areas. The information system auditor will examine, among other, the following:

- Information system mission statement and agreed goals and objectives for information system activities.
- Assessment of the risks associated with the use of the information systems and approach to managing those risks.
- Information system strategy plans to implement the strategy and monitoring of progress against those plans.
- Information system budget and monitoring of variances.
- High level policies for information system use and the protection and monitoring of compliance with these policies.
- Major contract approval and monitoring of performance of the supplier.
- Monitoring of performance against service level agreements
- Acquisition of major systems and decisions on implementation.
- Impact of external influences on information system such as internet, merger of suppliers or liquidation etc.
- Control of self-assessment reports, internal and external audit reports, quality assurance reports or other reports on Information System.

FINAL EXAMINATION : JUNE, 2009

- Business Continuity Planning, Testing thereof and Test results.
- Compliance with legal and regulatory requirements
- Appointment, performance monitoring and succession planning for senior information system staff including internal information system audit management and business process owners.

(b) The duties of the subscriber of a Digital Signature as specified in Section 40 to 42 of Chapter VII of IT Act- 2000 are as follows:

On acceptance of the Digital Signature Certificate the subscriber shall generate a key pair using a secure system.

A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate-

- (i) to one or more persons;
- (ii) in a repository, or otherwise demonstrates his approval of the Digital Signature
- (iii) certificate in any manner.

By accepting a Digital Signature Certificate, the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that –

- (i) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;
- (ii) all representations made by the subscriber to the Certificate Authority and all material relevant to the information contained in the Digital Signature Certificate are true;
- (iii) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

The subscriber shall exercise all reasonable care to retain control of his private key corresponding to the public key. If such private key has been compromised (i.e., endangered or exposed), the subscriber must immediately communicate the fact to the Certifying Authority.

Otherwise, the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

(c) Chapter-II of IT Act, 2000 gives legal recognition to electronic records and digital signatures. It contains only section 3.

This Section deals with the conditions subject to which an electronic record may be authenticated by means of affixing digital signature which is created in two definite steps. First the electronic record is converted into a message digest by using a mathematical function known as “Hash function” which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tampering with the contents of the electronic record will

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

immediately invalidate the digital signature. Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by any body who has the public key corresponding to such private key. This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message.

For the purposes of this sub-section, “hash function” means an algorithm mapping or translation of one sequence of bits into another, generally smaller set known as “hash result” such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible-

- to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
- that two electronic records can produce the same hash result using the algorithm.

Question 7.

Write short notes on the following:

(4x5=20 Marks)

- (a) System Manual
- (b) Control Objectives for Information related Technology (COBIT)
- (c) Firewalls
- (d) White Box Testing.

Answer

- (a) System Manual: The basic output of the system design is a description of the task to be performed, complete with layouts and flowcharts. This is called the job specifications manual or system manual. It contains:
 - (i) General description of the existing system.
 - (ii) Flow of the existing system.
 - (iii) Outputs of the existing system - the documents produced by existing system are listed and briefly described, including distribution of copies.
 - (iv) General description of the new system - its purposes and functions and major differences from the existing system are stated together with a brief justification for the change.
 - (v) Flow of the new system - this shows the flow of the system from and to the computer operation and the flow within the computer department.
 - (vi) Output Layouts.

FINAL EXAMINATION : JUNE, 2009

- (vii) Output distribution - the distribution of the new output document is indicated and the number of copies, routing and purpose in each department shown. The output distribution is summarized to show what each department will receive as a part of the proposed system.
 - (viii) Input layouts - the inputs to the new system are described and complete layouts of the input documents and input disks or tapes provided.
 - (ix) Input responsibility - the source of each input document is indicated as also the user department responsible for each item on the input documents.
 - (x) Macro-logic- the overall logic of the internal flow will be briefly described by the systems analyst, wherever useful.
 - (xi) Files to be maintained - the specifications will contain a listing of the tape, disk or other permanent record files to be maintained, and the items of information to be included in each file. There must be complete layouts for intermediate or work file; these may be prepared later by the programmer.
 - (xii) List of programs - a list of the programs to be written shall be a part of the systems specifications.
 - (xiii) Timing estimates - a summary of approximate computer timing is provided by the system analyst.
 - (xiv) Controls - this shall include type of controls, and the method in which it will be operated.
 - (xv) Audit trail - a separate section of the systems specifications shows the audit trail for all financial information. It indicates the methods with which errors and defalcation will be prevented or eliminated.
 - (xvi) Glossary of terms used.
- (b) Control Objectives for Information Related Technology (COBIT): The Information Systems Audit and Control Foundation (ISACF) developed the Control Objectives for Information and Related Technology (COBIT). COBIT is a trademark of generally applicable information systems security and control practices for IT controls. The framework allows:
- (i) management to benchmark the security and control, practices of IT environments;
 - (ii) users of IT services to be assured that adequate security and control exist, and
 - (iii) auditors to substantiate their opinions on internal control and to advice on IT security and control matters.

The framework addresses the issue of control from three vantage points, or dimensions:

- (1) Business Objectives. To satisfy business objectives, information must conform to certain criteria the COBIT refers to as business requirements for information. The criteria are divided into seven distinct yet overlapping categories that map into the COSO objectives: effectiveness (relevant, pertinent, and timely), efficiency,

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

confidentiality, integrity, availability, compliance with legal requirements and reliability.

- (2) IT resources, while include people, application systems, technology, facilities, and data.
- (3) IT processes, which are broken into four domains: planning and organization, acquisition and implementation, delivery and support, and monitoring.

COBIT, which consolidates standards from 36 different sources into a single framework, is having a big impact on the information systems profession. It is helping managers to learn how to balance risk and control investment in an information system environment. It provides users with greater assurance that the security and IT controls provided by internal and third parties are adequate. It guides auditors as they substantiate their opinions and as they provide advice to management on internal controls.

- (c) Firewall: A firewall is a collection of components (computers, routers, and software) that mediate access between different security domains. All traffic between the security domains must pass through the firewall, regardless of the direction of the flow. Since the firewall serves as an access control point for traffic between security domains, they are ideally situated to inspect and block traffic and coordinate activities with network intrusion detection system (IDSs).

There are four primary firewall types from which to choose: packet filtering, stateful inspection, proxy servers, and application-level firewalls. Any product may have characteristics of one or more firewall types. The selection of firewall type is dependent on many characteristics of the security zone, such as the amount of traffic, the sensitivity of the systems and data, and applications. Additionally, consideration should be given to the ease of firewall administration, degree of firewall monitoring support through automated logging and log analysis, and the capability to provide alerts for abnormal activity.

Typically, firewalls block or allow traffic based on rules configured by the administrator. Rule sets can be static or dynamic. A static rule set is an unchanging statement to be applied to packet header, such as blocking all incoming traffic with certain source addresses. A dynamic rule set often is the result of coordinating a firewall and an IDS. For example, an IDS that alerts on malicious activity may send a message to the firewall to block the incoming IP address. The firewall, after ensuring that the IP is not on a "white list", creates a rule to block the IP. After a specified period of time the rule expires and traffic is once again allowed from that IP.

Firewalls are subject to failure. When firewalls fail, they typically should fail closed, blocking all traffic, rather than failing open and allowing all traffic to pass. Firewalls provide some additional services such as network address translation, dynamic host configuration protocols and virtual private network gateways.

- (d) White Box Testing

White box testing is a test case design method that uses the control structure of the procedural design to derive test cases. Test cases can be derived that

FINAL EXAMINATION : JUNE, 2009

- guarantee that all independent paths within a module have been exercised at least once,
- exercise all logical decisions on their true and false sides,
- execute all loops at their boundaries and within their operational bounds, and
- exercise internal data structures to ensure their validity.

The Nature of Software Defects

Logic errors and incorrect assumptions are inversely proportional to the probability that a program path will be executed. General processing tends to be well understood while special case processing tends to be prone to errors.

We often believe that a logical path is not likely to be executed when it may be executed on a regular basis. Our unconscious assumptions about control flow and data lead to design errors that can only be detected by path testing. Typographical errors are random.

Basis Path Testing

This method enables the designer to derive a logical complexity measure of a procedural design and use it as a guide for defining a basis set of execution paths. Test cases that exercise the basis set are guaranteed to execute every statement in the program at least once during testing.

Flow Graphs

Flow graphs can be used to represent control flow in a program and can help in the derivation of the basis set. Each flow graph node represents one or more procedural statements. The edges between nodes represent flow of control. An edge must terminate at a node, even if the node does not represent any useful 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.

Loop Testing

This white box technique focuses exclusively on the validity of loop constructs. Four different classes of loops can be defined:

- Simple loops
- Nested loops
- Concatenated loops
- Unstructured loops

Other white box testing techniques include:

1. Condition testing which exercises the logical conditions in a program.
2. Data flow testing which selects test paths according to the locations of definitions and uses of variables in the program.