

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

Information Systems Concepts

1. (a) What do you understand by MIS? Discuss the important characteristics of an effective MIS.
(b) What are the major constraints that come in the way of operating an MIS? Explain in brief.
2. 'There is a practical set of principles to guide the design of measures and indicators to be included in an EIS'. Explain those principles in brief.

Software Development Life Cycle Methodology

3. What is agile methodology? Discuss its basic principles in brief.
4. (a) What are the issues that are typically addressed in the feasibility study of a project under SDLC?
(b) 'While eliciting information to delineate the scope, what are the aspects that are needed to be kept in mind during preliminary investigation of a project under SDLC'?
5. (a) Discuss the important characteristics of a good coded program.
(b) Distinguish between phased implementation and pilot implementation.

Control Objectives

6. (a) What do you mean by Corrective Controls? Also explain their main characteristics.
(b) What is antivirus software? Also explain its types in brief.
7. What is cryptosystem? Briefly discuss Data Encryption Standard.
8. (a) What do you mean by asynchronous attacks? Also explain its various forms of attacks.
(b) What are the points, which are required to be kept in mind by an IS Auditor while working with logical access control mechanisms?

Testing – General and Automated Controls

9. (a) Which types of information may be collected by the auditors by using SCARF?
(b) Describe the advantages of Continuous Auditing techniques in brief.

Risk Assessment Methodologies and Applications

10. (a) State and explain four commonly used techniques to assess and evaluate risks.
(b) Discuss the threats due to cyber crimes.

Business Continuity Planning and Disaster Recovery Planning

11. (a) Discuss the methodology of developing a Business Continuity Plan.
- (b) Explain audit tools and techniques used for disaster recovery plan.

An Overview of Enterprise Resource Planning (ERP)

12. (a) Write down the general guidelines, which are to be followed before starting the implementation of an ERP package.
- (b) What are the steps involved in the implementation of an ERP package?

Information Systems Auditing Standards, Guidelines, Best Practices

13. Discuss 'Physical and Environmental Security with Controls and Objectives' with respect to information Security Policy?
14. What do you understand by Software Process Maturity? Discuss five levels of Software Process Maturity of Capability Maturity Model (CMM).

Drafting of IS Security Policy, Audit Policy, IS Audit Reporting- A Practical Perspective

15. (a) What should be the major components of a good security policy? Explain in brief.
- (b) What purpose an information system audit policy will serve? Explain in brief.

Information Technology (Amendment) Act 2008

16. (a) Discuss the Duties of Certifying Authorities under Section 30 of the Information Technology (Amendment) Act 2008 to facilitate e-Governance.
- (b) Describe the 'Acceptance of a Digital Signature Certificate' with respect to the Section 41 of Information Technology (Amendment) Act, 2008.
17. Discuss the composition of a Cyber Appellate Tribunal under Section 49 of Information Technology (Amendment) Act, 2008.

Questions based on Short Notes

18. Write short notes on the following:
 - (a) Operational Feasibility
 - (b) Knowledge Acquisition Subsystem of an expert system
 - (c) Probability or Likelihood Assessment under Risk Management
19. Write short notes on the following:
 - (a) Full backup and Incremental Backup
 - (b) Worms
 - (c) Weaknesses of Waterfall Model

20. Write short notes on the following:

- (a) HIPAA
- (b) Cold Site and Hot Site
- (c) Retention of Electronic Records in the light of Section 7 of Information Technology (Amendment) Act, 2008

Questions based on Case Studies

21. ABC Ltd. is a leading company in the manufacturing of various types of toys. After detailed deliberations among various stakeholders, top management of the company felt to automate its various business processes. They decided to undergo systems' development in a phased manner. Generally, system development refers to the process of examining a business situation with the intent of improving it through better procedures and methods. In addition, system development can generally be thought of having two major components: System Analysis and System Design. Here, System Analysis is the process of gathering and interpreting facts, diagnosing problems, and using the information to recommend improvements to the system. On the other hand, System Design is the process of planning a new business system or one to replace or complement an existing system. But, before planning, one must thoroughly understand the old system and determine how computers can be used to make its operations more effective.

Read the above carefully and answer the following:

- (a) What is system development? Also explain system analysis and system design.
 - (b) It is observed that sometimes, organizations fail to achieve their systems development objectives. What may be the possible reasons for the same in your opinion? Give any five.
 - (c) How accountants can be involved in the development work? Give your opinion.
22. PQR Ltd. is a leading organization focused on the manufacturing of electrical appliances. Founded in the year 1960, the company has its head office, 5 regional offices and 120 sales offices located in various major cities of India. The company did not have any formal IT department responsible for all the IT related activities. Recently, the company realized the need for the same and appointed M/s ABC consultants to build an IT governance structure and bringing IT transformation within the organization to strengthen its operational efficiency. Accordingly, ABC Consultants conducted an initial feasibility study and submitted a detailed report, which recommended the company to go for a complete business transformation and listed all the business areas requiring transformation such as Finance, Inventory Management, new web portal, HR, Sales and Distribution etc. As a next step, as per the recommendation of the consultant, an expression of interest was released by the company inviting various organizations to

showcase their capabilities and suggest a good business solution as per the requirement of the company.

Read the above carefully and answer the following:

- (a) What is the major lacking on the part of PQR Ltd. and how the company is trying to address the same? Also discuss how the consultant is moving forward to address the need of the company?
 - (b) Feasibility study of a system is accomplished under various dimensions such as technical, financial, economical, operational, legal etc. Out of these, explain technical feasibility in brief.
 - (c) 'Determination of the project scope is an important activity for any business processes. What are the two primary methods with the help of which the scope of a project can be analyzed?
23. XYZ Consultants is a leading consultancy firm dealing with the consultation of various domains of information systems and its audit. Recently, the company has taken a project of ABC Ltd. relating to risk assessment. Risk assessment seeks to identify 'which business processes and related resources are critical to the business', 'what threats or exposures exists that can cause an unplanned interruption of business processes', and 'what costs accrue due to an interruption'. There are various analytical procedures that are used to determine various risks, threats, and exposures faced by an organization. These are known by various names, such as Business Impact Analysis (BIA), Risk Impact Analysis (RIA) etc. Risk assessment consists of two basic components namely data collection and its analysis. The data collected in risk assessment should include a comprehensive list of business processes and their resource dependencies. The purpose of risk analysis involves threat identification and risk mitigation.

Read the above carefully and answer the following:

- (a) What is the interpretation of the term 'risk assessment'? What are two basic components of risk assessment?
 - (b) 'There exist various common threats to the computerized environment'. Explain any five out of them.
 - (c) Discuss any three common risk mitigation techniques in brief.
24. ABC Industries Ltd., a company engaged in a business of manufacturing and supplying of automobile components to various automobile companies in India, had been developing and adopting office automation systems, at random and in isolated pockets of its departments. The company has recently obtained three major supply contracts from International Automobile companies and the top management has felt that the time is appropriate for them to convert its existing information system into a new one and to integrate all its office activities. One of the main objectives of taking this exercise is to

maintain continuity of business plans even while continuing the progress towards e-governance.

Read the above carefully and answer the following:

- (a) When the existing information system is to be converted into a new system, what are the activities involved in the conversion process?
 - (b) What are the types of operations into which the different office activities can be broadly grouped under office automation systems?
 - (c) What is meant by Business Continuity Planning? Explain the areas covered by Business Continuity.
 - (d) What is the procedure to apply for a license to issue electronic signature certificates, under Section 22, Information Technology (Amendment) Act, 2008?
25. ABC Technologies is a leading company in the BPO sector. Its most of the business processes are automated. The company is relying on Information Technology for information and transaction processing. The growth of E-commerce supported by the growth of the Internet has completely revolutionized and reengineered business processes. The company's new business models and new methods presume that the information required by the business managers is available all the time; it is accurate, it is reliable and no unauthorized disclosure of the same is made. Further, it is also presumed that the virtual business organization is up and running all the time on 24×7 basis. However, generally, the technology-enabled and technology-dependent organizations are more vulnerable to security threats than ever before.

Read the above carefully and answer the following:

- (a) Discuss the security objective of the organization.
- (b) 'There are certain basic ground rules that must be addressed sequentially, prior to know the details of 'how to protect the information systems'. Explain those rules in brief.
- (c) What are the major information security policies relevant for the organization in your opinion?

SUGGESTED ANSWERS / HINTS

1. (a) Many experts have defined Management Information System (MIS) in different ways. However, one of the well accepted definitions of MIS has been given by Davis and Olson as "An integrated user-machine system designed for providing information to support operational control, management control and decision making functions in an organization". MIS assist managers in decision making and problem solving in contrast to TPS, which is operations oriented. They use results produced

by the TPS, but they may also use other information. In any organization, decisions must be made on many issues that recur regularly and require a certain amount of information. Because the decision making process is well understood, the manager can identify the information that will be needed for the purpose. In turn, the information systems can be developed so that reports are prepared regularly to support these recurring decisions.

Some of the important characteristics of an effective MIS are given as follows:

- ◆ **Management Oriented:** It means that effort for the development of the information system should start from an appraisal of management needs and overall business objectives. Such a system is not necessarily for top management only; it may also meet the information requirements of middle level or operating levels of management as well.
- ◆ **Management Directed:** Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts. For system's effectiveness, it is necessary for management to devote their sufficient time not only at the stage of designing the system but for its review as well to ensure that the implemented system meets the specifications of the designed system.
- ◆ **Integrated:** Development of information should be an integrated one which means that all the functional and operational information sub-system should be tied together into one entity. An integrated Information system has the capability of generating more meaningful information to management by taking a comprehensive view or a complete look at inter locking sub-systems that operate within a company.
- ◆ **Common Data Flows:** It means the use of common input, processing and output procedures and media whenever required. Data is captured by system analysts only once and as close to its original source as possible. They, then, try to utilize a minimum of data processing procedures and sub-systems to process the data and strive to minimize the number of output documents and reports produced by the system. This eliminates duplication in data collections, simplifies operations and produces an efficient information system.
- ◆ **Heavy Planning Element:** An MIS usually takes 3 to 5 years and sometimes even longer period to get established firmly within a company. Therefore, a MIS designer must be present in MIS development who should keep in view future objectives and requirements of firm's information in mind.
- ◆ **Sub System Concept:** Even though the information system is viewed as a single entity, it must be broken down into digestible sub-systems which can be implemented one at a time by developing a phasing plan. The breaking down of MIS into meaningful sub-systems sets the stage for this phasing plan.

- ◆ **Common Database:** Database is the mortar that holds the functional systems together. It is defined as a "super-file" which consolidates and integrates data records formerly stored in many separate data files. The organization of a database allows it to be accessed by several information sub-systems and thus, eliminates the necessity of duplication in data storage, updating, deletion and protection.
- ◆ **Computerized:** Though MIS can be implemented without using a computer, the use of computers increases the effectiveness of the system. In fact, its use equips the system to handle a wide variety of applications by providing their information requirements quickly. Other necessary attributes of the computer to MIS are accuracy and consistency in processing data and reduction in clerical staff. These attributes make computer a prime requirement in management information system.

(b) Major constraints, which come in the way of operating an MIS are given as follows:

- ◆ Non-availability of experts, who can diagnose the objectives of the organization and provide a desired direction for installing an operating system. This problem may be overcome by grooming internal staff, which should be preceded by proper selection and training.
- ◆ Experts usually face the problem of selecting the sub-system of MIS to be installed and operated upon. The criteria, which should guide the experts depend upon the need and importance of a function for which MIS can be installed first.
- ◆ Due to varied objectives of business concerns, the approach adapted by experts for designing and implementing MIS is a non-standardized one.
- ◆ Non-availability of cooperation from staff is a crucial problem, which should be handled tactfully. This task should be carried out by organizing lectures, showing films and also explaining to them the utility of the system. Besides this, some persons should also be involved in the development and implementation of the system.

2. A practical set of principles to guide the design of measures and indicators to be included in an EIS is given as follows:

- ◆ EIS measures must be easy to understand and collect. Wherever possible, data should be collected naturally as part of the process of work. An EIS should not add substantially to the workload of managers or staff.
- ◆ EIS measures must be based on a balanced view of the organization's objective. Data in the system should reflect the objectives of the organization in the areas of productivity, resource management, quality and customer service.
- ◆ Performance indicators in an EIS must reflect everyone's contribution in a fair and

consistent manner. Indicators should be as independent as possible from variables outside the control of managers.

- ◆ EIS measures must encourage management and staff to share ownership of the organization's objectives. Performance indicators must promote both team-work and friendly competition. Measures will be meaningful for all staff; people must feel that they, as individuals, can contribute to improving the performance of the organization.
- ◆ EIS information must be available to everyone in the organization. The objective is to provide everyone with useful information about the organization's performance. Information that must remain confidential should not be part of the EIS or the management system of the organization.
- ◆ EIS measures must evolve to meet the changing needs of the organization.

3. **Agile Methodology:** This is a group of software development methodologies based on the *iterative and incremental* development, where requirements and solutions evolve through collaboration between self organizing, cross-functional teams. It promotes adaptive planning, evolutionary development and delivery; time boxed iterative approach and encourages rapid and flexible response to change. It is a conceptual framework that promotes foreseen interactions throughout the development life cycle.

Following are the basic principles of this methodology:

- ◆ Customer satisfaction by rapid delivery of useful software;
 - ◆ Welcoming changing requirements, even late in development;
 - ◆ Working software is delivered frequently (weeks rather than months);
 - ◆ Working software is the principal measure of progress;
 - ◆ Sustainable development; able to maintain a constant pace;
 - ◆ Close, daily co-operation between business people and developers;
 - ◆ Face-to-face conversation is the best form of communication (co-location);
 - ◆ Projects are built around motivated individuals, who should be trusted;
 - ◆ Continuous attention to technical excellence and good design;
 - ◆ Simplicity;
 - ◆ Self-organizing teams; and
 - ◆ Regular adaptation to changing circumstances.
4. (a) The following issues are typically addressed in the Feasibility Study of a project under SDLC:
- ◆ Determining whether the solution is as per the business strategy;

- ◆ Determining whether the existing system can rectify the situation without a major modification,
 - ◆ Defining the time frame for which the solution is required;
 - ◆ Determining the approximate cost to develop the system; and
 - ◆ Determining whether the vendor product offers a solution to the problem.
- (b) While eliciting information to delineate the scope, few aspects, which are needed to be kept in mind during preliminary investigation of a project under SDLC, are given as follows:
- ◆ Different users will represent the problem and required solution in different ways. The system developer should elicit the need from the initiator of the project alternately called champion or executive sponsor of the project, addressing his concerns should be the basis of the scope.
 - ◆ While the initiator of the project may be a member of the senior management, the actual users may be from the operating levels in an organization. An understanding of their profile helps in designing appropriate user interface features.
 - ◆ While presenting the proposed solution for a problem, the development organization has to clearly quantify the economic benefits to the user organization. The information required has to be gathered at this stage. For example - when a system is proposed for Road tax collection, data on the extent of collection and defaults is required to quantify benefits that will result to the Transport Department.
 - ◆ It is also necessary to understand the impact of the solution on the organization- its structure, roles and responsibilities. Solutions, which have a wide impact are likely to meet with greater resistance. ERP implementation in organizations is a classic example of change management requirement. Organizations that have not been able to handle this have had a very poor ERP implementation record, with disastrous consequences.
 - ◆ While economic benefit is a critical consideration when deciding on a solution, there are several other factors that have to be given weight-age too. These factors have to be considered from the perspective of the user management and resolved. For example- in a security system, how foolproof it is, may be a critical a factor like the economic benefits that entail.
5. (a) A good coded program should have the following characteristics:
- ◆ **Reliability:** It refers to the consistency, which a program provides over a period of time. However poor setting of parameters and hard coding some data, subsequently could result in the failure of a program after some time.
 - ◆ **Robustness:** It refers to the process of taking into account all possible inputs and outputs of a program in case of least likely situations.

- ◆ **Accuracy:** It refers not only to what program is supposed to do, but should also take care of what it should not do. The second part becomes more challenging for quality control personnel and auditors.
 - ◆ **Efficiency:** It refers to the performance, which should not be unduly affected with the increase in input values.
 - ◆ **Usability:** It refers to a user-friendly interface and easy-to-understand document required for any program.
 - ◆ **Readability:** It refers to the ease of maintenance of program even in the absence of the program developer.
- (b) **Phased implementation:** With this strategy, implementation can be staged with conversion to the new system taking place by degrees. For example - some new files may be converted and used by employees whilst other files continue to be used on the old system i.e. the new is brought in stages (phases). If each phase is successful then the next phase is started, eventually leading to the final phase when the new system fully replaces the old one as shown in the following Fig.:

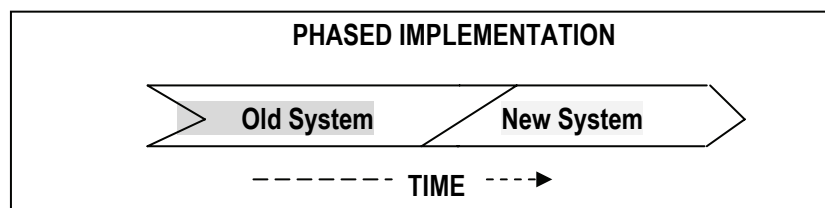


Fig. : Phased Implementation

Pilot implementation: With this strategy, the new system replaces the old one in one operation but only on a small scale. Any errors can be rectified or further beneficial changes can be introduced and replicated throughout the whole system in good time with the least disruption. For example - it might be tried out in one branch of the company or in one location.

If successful then the pilot is extended until it eventually replaces the old system completely. The following Fig. depicts Pilot Implementation.

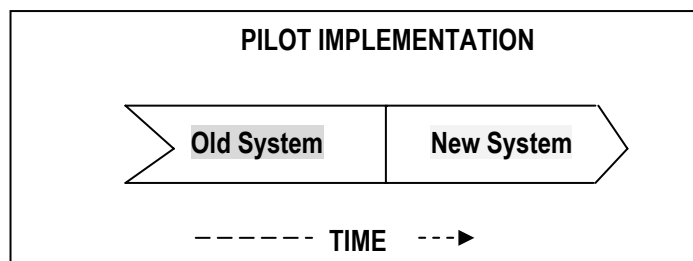


Fig. : Pilot Implementation

6. (a) **Corrective Controls:** Corrective controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. A business continuity plan is considered to be a significant corrective control. Some of the examples of Corrective Controls are:
- ◆ Contingency planning,
 - ◆ Backup procedure,
 - ◆ Rerun procedures,
 - ◆ Treatment procedures for a disease,
 - ◆ Changing input value to an application system, and
 - ◆ Investigating budget variance and report violations.
- The main characteristics of the corrective controls are:
- ◆ To minimize the impact of the threat,
 - ◆ To identify the cause of the problem,
 - ◆ To mitigate the problems discovered by detective controls,
 - ◆ To get feedback from preventive and detective controls,
 - ◆ To correct error arising from a problem, and
 - ◆ To modify the processing systems to minimize future occurrences of the problem.
- (b) **Anti-virus Software:** It is a program that is used to detect viruses, and prevent their further propagation and harm. There are three major types of anti-virus software, which are given as follows:
- ◆ **Scanners:** Scanners look for a sequence of bits called virus signatures that are characteristic of virus codes. They check memory, disk boot sectors, executables and systems files to find matching bit patterns. As new viruses emerge frequently, it is necessary to frequently update the scanners with the data on virus code patterns for the scanners to be reasonably effective.
 - ◆ **Active Monitor and Heuristic Scanner:** This looks for critical interrupt calls and critical operating systems functions such as OS calls and BIOS calls, which resemble virus action.
 - ◆ **Integrity Checkers:** These can detect any unauthorized changes to files on the system. These can detect any unauthorized changes to the files on the system. The software performs a “take stock” of all files resident on the system and computes a binary check data called the Cyclic Redundancy Check (CRC). When a program is called for execution, the software computes the CRC again and checks with the parameter stored on the disk.

7. **Cryptosystem:** A cryptosystem refers to a suite of algorithms needed to implement a particular form of encryption and decryption. Typically, it consists of following three algorithms:

- ◆ *Key Generation Algorithm,*
- ◆ *Encryption Algorithm and*
- ◆ *Decryption Algorithm.*

The pair of algorithms of Encryption and Decryption is referred as Cipher or Cipher.

Data Encryption Standard (DES): It is a cipher. It is a mathematical algorithm for encrypting and decrypting binary coded information. Encrypting of data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. Encryption and Decryption operations are done by using a binary number called a key. A key consists of 64(bits) binary digits. Among these 64 bits, 56 bits are used for encryption/decryption and remaining 8 bits are used for error detection. Authorized users of the encrypted data must have the unique key that was used to encipher the data in order to decrypt it. Selection of a different key causes the cipher that is produced for any given set of inputs to be different. The cryptographic security of the data depends on the security provided for the key used to encipher and decipher the data. A standard algorithm based on a secure key thus provides a basis for exchanging encrypted computer data by issuing the key used to encipher it to those authorized to have the data.

The encryption and decryption processes are depicted in the following diagram:

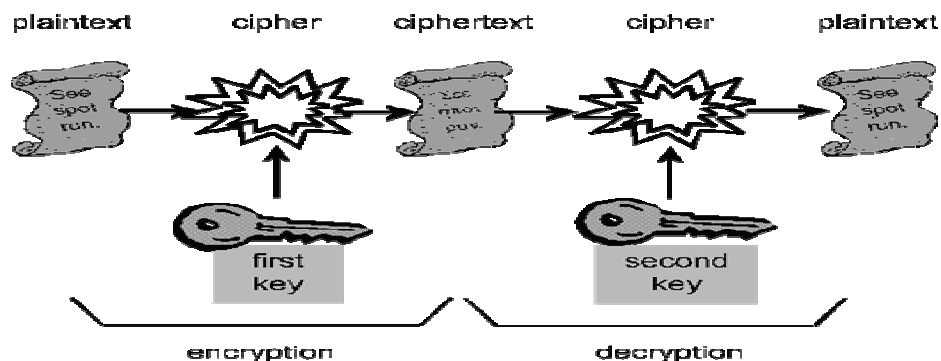


Fig.: DES

Some documentation/experts distinguishes DES from its algorithms. It refers algorithms as DEA (*Data Encryption Algorithm*).

8. (a) **Asynchronous Attacks :** They occur in many environments where data can be moved asynchronously across telecommunication lines. Numerous transmissions must wait for the clearance of the line before data being transmitted. Data that are waiting to be transmitted are liable to unauthorized access called asynchronous attack. These attacks are hard to detect because they are usually very small pin like insertions. There are many forms of asynchronous attacks; some of them are

given as follows:

- (i) *Data Leakage*: Data is critical resource for an organization to function effectively. Data leakage involves leaking information out of the computer by means of dumping files to paper or stealing computer reports and tape.
- (ii) *Wire-tapping*: This involves spying on information being transmitted over telecommunication network.

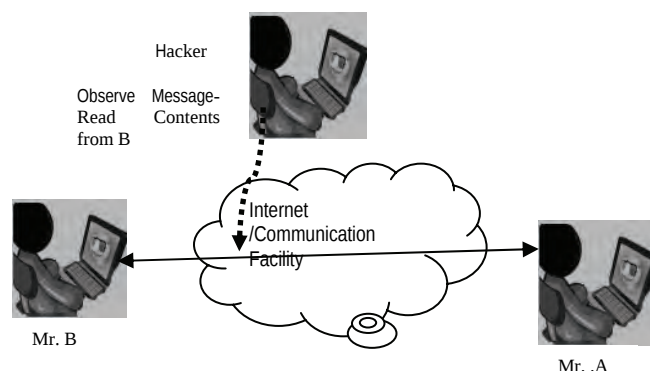


Fig. : Wire Tapping

- (iii) *Piggybacking*: This is the act of following an authorized person through a secured door or electronically attaching to an authorized telecommunication link that intercepts and alters transmissions. This involves intercepting communication between the operating system and the user and modifying them or substituting new messages. A special terminal is tapped into the communication for this purpose.

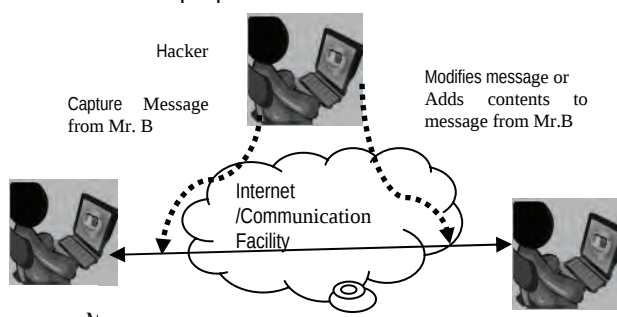


Fig. : Piggybacking

- (iv) *Shut Down of the Computer/Denial of Service(DoS)*: This is initiated through terminals or microcomputers that are directly or indirectly connected to the computer. Individuals, who know the high-level systems log on-ID initiate shutting down process. This security measure will function effectively only if there are appropriate access controls on the logging on through a

telecommunication network. When overloading happens some systems have been proved to be vulnerable to shutting themselves. Hackers use this technique to shut down computer systems over the Internet.

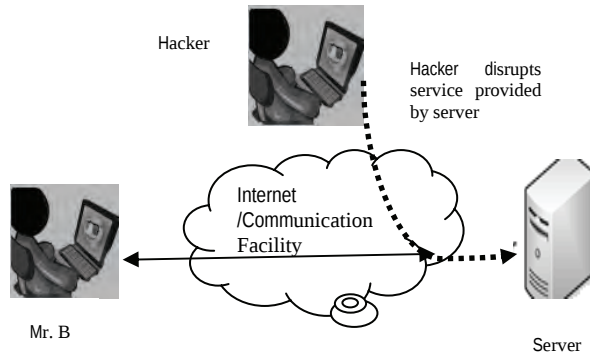


Fig.: Denial of Service(DoS)

(b) An IS auditor should keep the following points in mind while working with logical access control mechanisms:

- ◆ Reviewing the relevant documents pertaining to logical facilities and risk assessment and evaluation techniques and understanding the security risks facing the information processing system.
- ◆ The potential access paths into the system must be evaluated by the auditor and documented to assess their sufficiency.
- ◆ Deficiencies or redundancies must be identified and evaluated.
- ◆ By supplying appropriate audit techniques, s/he must be in a position to verify test controls over access paths to determine its effective functioning.
- ◆ S/he has to evaluate the access control mechanism, analyze the test results and other auditing evidences and verify whether the control objectives have been achieved.
- ◆ The auditor should compare security policies and practices of other organizations with the policies of their organization and assess its adequacy.

9. (a) Auditors might use SCARF to collect the following types of information:

- ◆ **Application system errors** - SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.
- ◆ **Policy and procedural variances** - Organizations have to adhere to the policies, procedures and standards of the organization and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.

- ◆ **System exception** - SCARF can be used to monitor different types of application system exceptions. For example, salespersons might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.
- ◆ **Statistical sample** -Some embedded audit routines might be statistical sampling routines, SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.
- ◆ **Snapshots and extended records** - Snapshots and extended records can be written into the SCARF file and printed when required.
- ◆ **Profiling data** - Auditors can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.
- ◆ **Performance measurement** - Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.

(b) Some of the main advantages of continuous audit techniques are as under:

- ◆ **Timely, comprehensive and detailed auditing:** Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analysed rather than examining the inputs and the outputs only.
- ◆ **Surprise test capability:** As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.
- ◆ **Information to system staff on meeting of objectives:** Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
- ◆ **Training for new users:** Using the ITFs, new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

10. (a) Four most commonly used techniques to access and evaluate risks are:

- ◆ Judgment and intuition,
- ◆ The Delphi Approach,
- ◆ Scoring, and
- ◆ 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 upon 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 technique is used for obtaining consensus opinion. A panel of experts is engaged and each expert is asked to give his/her 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 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.
- (b) 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(DoS):** 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 propagate by inserting themselves into or modifying other programs.
- ◆ **Others:** 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.

11. (a) The methodology for developing a business continuity plan can be sub-divided into eight different phases. The extent of applicability of each of the phases has to be tailored to the respective organisation. The methodology emphasises on the following:

- (i) Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
- (ii) Obtaining commitment from appropriate management to support and participate in the effort;
- (iii) Defining recovery requirements from the perspective of business functions;
- (iv) Documenting the impact of an extended loss to operations and key business functions;
- (v) Focusing appropriately on disaster prevention and impact minimisation, as well as orderly recovery;
- (vi) Selecting business continuity teams that ensure the proper balance required for plan development;
- (vii) Developing a business continuity plan that is understandable, easy to use and maintain; and
- (viii) Defining how business continuity considerations must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.

(b) **Audit Tools and Techniques for a Disaster Recovery Plan:** 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 tools and methods may be categorized as under:

- (i) **Automated Tools:** Automated tools 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, lack of integrity of the system software etc.
- (ii) **Internal Control Auditing:** This includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance of laws and regulations.
- (iii) **Disaster and security checklists:** A checklist can be used against which the systems can be audited. The checklist 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:** Penetration testing can be used to locate vulnerabilities.

12. (a) Following are the general guidelines, which are to be followed before starting the implementation of an ERP package:
- ◆ Understanding the corporate needs and culture of the organization and then adopt the implementation technique to match these factors;
 - ◆ Doing a business process redesigning exercise prior to starting the implementation;
 - ◆ Establishing a good communication network across the organization;
 - ◆ Providing a strong and effective leadership so that people down the line are well motivated;
 - ◆ Finding an efficient and capable project manager;
 - ◆ Creating a balanced team of implementation consultants, who can work together as a team;
 - ◆ Selecting a good implementation methodology with minimum customization;
 - ◆ Training end-users; and
 - ◆ Adapting the new system and making the required changes in the working environment to make effective use of the system in future.
- (b) The steps involved in the implementation of an ERP package are given as follows:
- (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) Re-engineering 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;
- (viii) Finalizing the implementation consultants, who will assist in implementation; and
- (ix) Implementing the ERP package.

- 13. Physical and Environmental Security:** This is the beginning point of any security plan. It is designed to prevent unauthorized access, damage and interference to business premises and information. This involves physical security perimeter, physical entry control, creating secure offices, rooms, facilities, providing physical access controls, providing protection devices to minimize risks ranging from fire to electromagnetic radiation, providing adequate protection to power supplies and data cables. Cost effective design and constant monitoring are two key aspects to maintain adequate physical security control.

Maintenance of the physical operating environment in a computer server room is as important as ensuring that paper records are not subject to damage by mould, fire or fading. Supporting equipments such as air conditioning plant etc. should be properly maintained. Physical controls may be difficult to manage as they rely to some extent on building structure, but good physical security can be very effective.

The detailed controls and objectives for this type of security are:

- ◆ *Secure areas:* To prevent unauthorized access, damage and interference to business premises and information,
- ◆ *Equipment Security:* To prevent loss, damage or compromise of assets and interruption to business activities, and
- ◆ *General Controls:* To prevent compromise or theft of information and information processing facilities.

- 14.** A software process is a set of activities, methods, practices, and transformations that are used to develop and maintain software and the associated products such as project plans, design documents, code, test cases, and user manuals.

Software process maturity is the extent to which a specific process is explicitly defined, managed, measured, controlled, and effective. Maturity implies a potential for growth in capability and indicates both the richness of an organization's software process and the consistency with which it is applied in projects throughout the organization. As a software

organization gains in software process maturity, its institutionalization in software process building takes place.

Five Levels of Software Process Maturity

Continuous process improvement is based on many small, evolutionary steps rather than revolutionary innovations. The CMM provides a framework for organizing these evolutionary steps into five maturity levels that lay successive foundations for continuous process improvement. These five maturity levels are discussed below and shown in the figure:

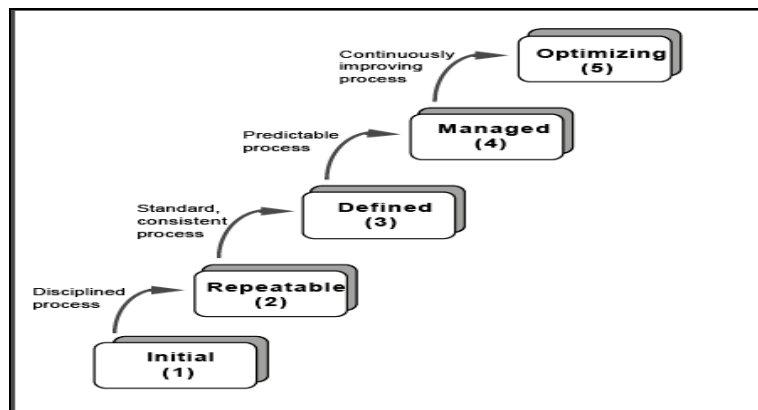


Fig.: Various Levels of CMM

- (i) *Level 1 - The Initial Level:* At the Initial Level, the organization typically does not provide a stable environment for developing and maintaining software. At this Level, capability is a characteristic of the individuals, not of the organization. During a crisis of software success depends entirely on having an exceptional manager and a seasoned and effective software team. But if someone leaves the project, it is difficult to handle the crises and a challenging task.
- (ii) *Level 2 - The Repeatable Level:* At this Level, policies for managing a software project and procedures to implement those policies are established. Planning and managing new projects is based on experience with similar projects. An effective process can be characterized as one which is practiced, documented, enforced, trained, measured, and able to improve. This Level makes the organizations to install basic software management controls. Software project standards are defined. The project's process is under the effective control of a project management system, following realistic plans based on the performance of previous projects.
- (iii) *Level 3 - The Defined Level:* At this Level, documentation for development and maintenance is prepared. This standard process is referred to throughout the CMM as the organization's standard software process, to help the software managers and technical staff performs more effectively. A group of experts standardize the process. An organization-wide training program is implemented to ensure that the staff and managers have the knowledge and skills required to fulfill their assigned

roles. This process capability is based on a common, organization-wide understanding of the activities, roles, and responsibilities in a defined software process.

- (iv) *Level 4 - The Managed Level:* At the Managed Level, the organization sets quantitative quality goals for both software products and processes. Productivity and quality are measured for important software process activities across all projects as part of an organizational measurement program. An organization-wide software process database is used to collect and analyze the data available from the projects' defined software processes.

This level of capability allows an organization to product trend in process and product quality within qualitative limits. Because of the stability and measured data when some exceptional circumstance occurs, the special cause of variation can be identified and addressed. The software products are of predictably high quality.

- (v) *Level 5 - The Optimizing Level:* The entire organization is focused on continuous process improvement. The organization has the means to identify weaknesses and strengthen the process proactively, with the goal of preventing the occurrence of defects. Data on the effectiveness of the software process is used to perform cost benefit analyses of new technologies and proposed changes to the organization's software process. In short, the cost of development is cut, best engineering practices are developed and used. Continuous improvement is done. Technology and process improvements are planned and managed as ordinary business activities.

15. (a) A good security policy should clearly state the following :

- ◆ Purpose and scope of the document and the intended audience,
- ◆ The Security infrastructure,
- ◆ Security policy document maintenance and compliance requirements,
- ◆ Incident response mechanism and incident reporting,
- ◆ Security organization Structure,
- ◆ Inventory and classification of assets,
- ◆ Description of technologies and computing structure,
- ◆ Physical and environmental security,
- ◆ Identity management and access control,
- ◆ IT operations management,
- ◆ IT communications,
- ◆ System development and maintenance controls,

- ◆ Business Continuity Planning (BCP),
- ◆ Legal compliances,
- ◆ Monitoring and auditing requirements, and
- ◆ Underlying technical policy.

However, above mentioned components are the major contents of a typical security policy. The policy is very organization specific and a study of the organizations functions, their criticality and the nature of the information would determine the content of the security policy.

(b) 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, and
- ◆ 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,
- ◆ Maintenances of Data Integrity,
- ◆ Maintenance of System Effectiveness,
- ◆ Ensuring System Efficiency, and
- ◆ Compliance with Information System related policies, guidelines, circulars, and any other instructions requiring compliance in whatever name called.

16. (a) [Section 30] Duties of Certifying Authorities :

This section provides that every Certifying Authority shall follow certain procedures in respect of Digital Signatures as given below: Every Certifying Authority shall-

- (a) make use of hardware, software, and procedures that are secure from intrusion and misuse:

- (b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;
- (c) adhere to security procedures to ensure that the secrecy and privacy of the Electronic Signature are assured (**Amended vide ITAA 2008**)
- (ca) be the repository of all Electronic Signature Certificates issued under this Act (Inserted vide ITAA 2008)
- (cb) publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and (Inserted vide ITAA 2008)
- (d) observe such other standards as may be specified by regulations.

(b) [Section 41] Acceptance of Digital Signature Certificate :

- (1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate -
 - (a) to one or more persons;
 - (b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.
- (2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that –
 - (a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;
 - (b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;
 - (c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

17. [Section 49] Composition of Cyber Appellate Tribunal (Substituted vide ITAA 2008):

- (1) The Cyber Appellate Tribunal shall consist of a Chairperson and such number of other Members, as the Central Government may, by notification in the Official Gazette, appoint (Inserted vide ITAA-2008).

Provided that the person appointed as the Presiding Officer of the Cyber Appellate Tribunal under the provisions of this Act immediately before the commencement of the Information Technology (Amendment) Act 2008 shall be deemed to have been appointed as the Chairperson of the said Cyber Appellate Tribunal under the provisions of this Act as amended by the Information Technology (Amendment) Act, 2008 (Inserted Vide ITAA 2008).

- (2) The selection of Chairperson and Members of the Cyber Appellate Tribunal shall be made by the Central Government in consultation with the Chief Justice of India. (Inserted vide ITAA-2008).
- (3) Subject to the provisions of this Act-
- (a) the jurisdiction, powers and authority of the Cyber Appellate Tribunal may be exercised by the Benches thereof
 - (b) a Bench may be constituted by the Chairperson of the Cyber Appellate Tribunal with one or two members of such Tribunal as the Chairperson may deem fit.
Provided that every Bench shall be presided over by the Chairperson or the Judicial Member appointed under sub-section (3) of section 50 (ITAA 2008)
 - (c) the Benches of the Cyber Appellate Tribunal shall sit at New Delhi and at such other places as the Central Government may, in consultation with the Chairperson of the Cyber Appellate Tribunal, by notification in the Official Gazette, specify.
 - (d) the Central Government shall, by notification in the Official Gazette, specify the areas in relation to which each Bench of the Cyber Appellate Tribunal may exercise its jurisdiction.
(Inserted vide ITAA-2008).
- (4) Notwithstanding anything contained in sub-section (3), the Chairperson of the Cyber Appellate Tribunal may transfer a Member of such Tribunal from one Bench to another Bench (Inserted vide ITAA-2008)
- (5) If at any stage of the hearing of any case or matter, it appears to the Chairperson or a Member of the Cyber Appellate Tribunal that the case or matter is of such a nature that it ought to be heard by a Bench consisting of more Members, the case or matter may be transferred by the Chairperson to such Bench as the Chairperson may deem fit. (Inserted vide ITAA-2008)
- 18. (a) Operational Feasibility :** It is concerned with ascertaining the views of workers, employees, customers and suppliers about the use of computer facility. A system can be highly feasible in all respects except the operational and fails miserably because of human problems. Some of the questions, which help in testing the operational feasibility of a project are stated below:
- ◆ Is there sufficient support for the system from management and from users?
 - ◆ Are current business methods acceptable to users?
 - ◆ Have the users been involved in planning and development of the project?
 - ◆ Will the proposed system cause harm? Will it produce poorer results in any respect or area? Will loss of control result in any areas? Will accessibility of information be lost?

- ◆ Will individual performance be poorer after implementation than before?

This analysis may involve a subjective assessment of the political and managerial environment in which the system will be implemented. In general, the greater the requirements for change in the user environment in which the system will be installed, the greater the risk of implementation failure.

- (b) **Knowledge Acquisition Subsystem (KAS) of an Expert System:** The Knowledge Acquisition Subsystem is the software component of an Expert System that enables the Knowledge Engineer (KE) a specialized systems analyst responsible for designing and maintaining the expert System to build and refine an expert systems knowledge base. The KE works with the knowledge acquisition subsystem to model decision logic, derive industries and update the knowledge base.

Knowledge base development and maintenance can be done using special, reasonably user-friendly software. This software provides a convenient and efficient means of capturing and storing the contents of the knowledge base. Users are often presented with easy-to-operate menus and templates for entering rules, facts and relationship among facts. Once these are entered, the software correctly stores the information in the knowledge base. Such software notes are much easier and less expensive to develop, update and refine the KB.

- (c) **Probability or Likelihood Assessment:** Likelihood is the estimation of the frequency or the chance of a threat happening. A likelihood assessment considers the presence, tenacity and strength of threats, as well as, the effectiveness of safeguards. In general, historical information about many threats is weak, particularly with regard to human threats; hence the judgment and experience in this area is of relevance. Some threats affect data especially threats to physical assets such as fires, floods etc. Care needs to be taken in using any statistical threat data; the source of data otherwise the analysis may be inaccurate or incomplete. In general, the greater the likelihood of a threat occurring, the greater is the risk.

To some extent, the nature and value of information assets affect the likelihood of occurrence of a threat. If the asset is of high value, e.g. proprietary software packages, it is a prime target for piracy attempts. Thus, the identification and valuation of assets also assists with the identification of threats and their likelihood of occurrence. Periodically, the likelihood of occurrence of a threat needs to be reassessed due to changes occurring in the structure, direction, and environment of an organization.

- 19. (a) **Full Backup :** A full backup captures all files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data.

Incremental Backup : An incremental backup captures files that were created or changed since the last backup, regardless of backup type. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space.

Normally, incremental backup are very difficult to restore. One have to start with recovering the last full backup, and then recovering from every incremental backup taken since.

- (b) **Worms:** A worm does not require a host program like a Trojan to relocate itself. Thus, a Worm program copies itself to another machine on the network. Since, worms are stand-alone programs, and they can be detected easily in comparison to Trojans and computer viruses.

Worms can help to sabotage systems yet they can also be used to perform some useful tasks. For example, worms can be used in the installation of a network. A worm can be inserted in a network and we can check for its presence at each node. A node, which does not indicate the presence of the worm for quite some time, can be assumed as not connected to the network.

Examples of worms are Existential Worm, Alarm clock Worm etc. The Alarm Clock worm places wake-up calls on a list of users. It passes through the network to an outgoing terminal while the sole purpose of existential worm is to remain alive.

Existential worm does not cause damage to the system, but only copies itself to several places in a computer network.

- (c) **Weaknesses of Waterfall Model:** Major weaknesses of the Waterfall Model are given as follows:

- ◆ Inflexible, slow, costly, and cumbersome due to significant structure and tight controls.
- ◆ Project progresses forward, with only slight movement backward.
- ◆ Little room for use of iteration, which can reduce manageability if used.
- ◆ Depends upon early identification and specification of requirements, yet users may not be able to clearly define what they need early in the project.
- ◆ Requirement inconsistencies, missing system components and unexpected development needs are often discovered during design and coding.
- ◆ Problems are often not discovered until system testing.
- ◆ System performance cannot be tested until the system is almost fully coded, and under capacity may be difficult to correct.
- ◆ Difficult to respond to changes. Changes that occur later in the life cycle are more costly and are thus discouraged.

- ◆ Produces excessive documentation and keeping it updated as the project progresses is time-consuming.
- ◆ Written specifications are often difficult for users to read and thoroughly appreciate.
- ◆ Promotes the gap between users and developers with clear vision of responsibility.

20. (a) **HIPAA** : Health Insurance Portability and Accountability Act (HIPAA) was enacted by the U.S. Congress in 1996. Major points are given as follows:

- ◆ Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.
- ◆ Title II of HIPAA, the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The AS provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the US health care system. What is of interest here is the Security Rule issued under the Act.

(b) **Cold site**: If an organisation can tolerate some downtime, cold-site backup might be appropriate. A cold site has all the facilities needed to install a mainframe system—raised floors, air conditioning, power, communication lines, and so on. An organisation can establish its own cold-site facility or enter into an agreement with another organisation to provide a cold-site facility.

Hot site: If fast recovery is critical, an organisation might need hot site backup. All hardware and operations facilities will be available at the hot site. In some cases, software, data and supplies might also be stored there. A hot site is expensive to maintain. They are usually shared with other organisations that have hot-site needs.

(c) **[Section 7] Retention of Electronic Records:**

- (1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, -
 - (a) the information contained therein remains accessible so as to be usable for a subsequent reference;
 - (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

- (c) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

However, this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

- (2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records. Publication of rules, regulation, etc. in Electronic Gazette.

21. (a) **System development:** It refers to the process of examining a business situation with the intent of improving it through better procedures and methods.

Generally, system development can generally be thought of having two major components:

- ◆ System Analysis, and
- ◆ System Design.

System Analysis is the process of gathering and interpreting facts, diagnosing problems, and using the information to recommend improvements to the system.

System Design is the process of planning a new business system or one to replace or complement an existing system.

- (b) Five reasons, which may be responsible for the organizations failing to achieve their systems development objectives are given as follows:

- ◆ *Lack of senior management support and involvement in information systems development.* Developers and users of information systems watch senior management to determine which systems development projects are important and act accordingly by shifting their efforts away from any project which is not receiving management attention. In addition, management can see that adequate resources, as well as budgetary control over use of those resources, are dedicated to the project.
- ◆ *Shifting user needs.* User requirements for information technology are constantly changing. As these changes accelerate, there will be more requests for systems development and more development projects. When these changes occur during a development process, the development team faces the challenge of developing systems whose very purposes might change since the development process began.
- ◆ *Development of strategic systems.* Because strategic decision making is unstructured, the requirements, specifications, and objectives for such development projects are difficult to define.

- ◆ *Overworked or under-trained development staff.* In many cases, systems developers often lack sufficient educational background. Furthermore, many companies do little to help their development personnel stay technically sound. Currently in these organizations, a training plan and training budget do not exist.
- ◆ *Resistance to change.* People have a natural tendency to resist change, and information systems development projects signal changes - often radical - in the workplace. When personnel perceive that the project will result in personnel cutbacks, threatened personnel will dig in their heels, and the development project is doomed to failure.

- (c) **Accountants' involvement in the Development work:** Accountants are uniquely qualified to participate in systems development because they may be among the few people in an organization, who have an in-depth as well as combined knowledge of IT, business, accounting, and internal control, as well as behavior and communications, to ensure that new systems meet the needs of the user and possess adequate internal controls.

They have specialized skills - such as accounting and auditing - that can be applied to the development project. For example, an accountant might perform the analysis of a proposed system's costs and benefits.

22. (a) The major lacking on PQR Ltd. is not having any formal IT department responsible for all the IT related activities in the organization.

For addressing this issue, the company is taking the following steps:

- ◆ As a first step, the company realized the need for an IT department in the organization.
- ◆ Moving a step further, the company appointed M/s ABC consultants to build an IT governance structure.
- ◆ The company also asked the consultant to bring IT transformation within the organization to strengthen its operational efficiency.

The consultant is moving forward to address the need of the company in the following ways:

- ◆ First of all, the consultant conducted an initial feasibility study.
- ◆ In addition, they submitted a detailed report, which recommended the company to go for a complete business transformation
- ◆ They also listed all the business areas requiring transformation such as Finance, Inventory Management, new web portal, HR, Sales and Distribution etc.
- ◆ As a next step, as per the recommendation of the consultant, an expression of interest was also released by the company inviting various organizations to showcase their capabilities and suggest a good business solution as per the requirement of the company.

(b) **Technical Feasibility:** It is concerned with the issues pertaining to hardware and software. Essentially, an 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:

- ◆ Does the necessary technology exist to do what is suggested (and can it be acquired)?
- ◆ Does the proposed equipment have the technical capacity to hold the data required to use the new system?
- ◆ Can the proposed application be implemented with existing technology?
- ◆ Will the proposed system provide adequate responses to inquiries, regardless of the number or location of users?
- ◆ Can the system be expanded if developed?
- ◆ Are there technical guarantees of accuracy, reliability, ease of access, and data security?

(c) Two primary methods with the help of which the scope of the project can be analyzed are given as follows:

- ◆ **Reviewing Internal Documents:** The analysts conducting the investigation first try to learn about the organization involved in, or affected by, the project. For example, to review an inventory system proposal, the analyst will try to know how the inventory department operates and who are the managers and supervisors. Analysts can usually learn these details by examining organization charts and studying written operating procedures.
- ◆ **Conducting Interviews:** Written documents tell the analyst how the systems should operate, but they may not include enough details to allow a decision to be made about the merits of a systems proposal, nor do they present users' views about current operations. To learn these details, analysts use interviews. Interviews allow analysts to know more about the nature of the project request and the reasons for submitting it. Usually, preliminary investigation interviews involve only management and supervisory personnel.

23. (a) Risk assessment seeks to identify the following key points:

- ◆ which business processes and related resources are critical to the business;
- ◆ what threats or exposures exist that can cause an unplanned interruption of business processes; and
- ◆ what costs accrue due to an interruption.

Risk assessment consists of two basic components, which are given as follows:

- ◆ data collection, and

- ◆ its analysis.

The data collected in risk assessment should include a comprehensive list of business processes and their resource dependencies. The purpose of risk analysis involves threat identification and risk mitigation.

(b) Five common threats to the computerized environment are given as follows:

- ◆ **Power failure:** Power failure can cause disruption of entire computing equipments since computing equipments depends on power supply.
- ◆ **Communication failure :** Failure of communication lines result in inability to transfer data which primarily travel over communication lines. Where the organization depends on public communication lines e.g. for e-banking, communication failure present a significant threat that will have a direct impact on operations.
- ◆ **Disgruntled Employees:** A disgruntled employee presents a threat since, with access to sensitive information of the organization, s/he may cause intentional harm to the information processing facilities or sabotage operations.
- ◆ **Errors:** Errors, which may result from technical reasons, negligence or otherwise can cause significant integrity issues. A wrong parameter setting at the firewall to “allow” attachments instead of “deny” may result in the entire organization network being compromised with virus attacks.
- ◆ **Malicious Code :** Malicious code such as viruses and worms which freely access the unprotected networks may affect organizational and business networks that use these unprotected networks.

(c) Three common risk mitigation techniques are given as follows:

- ◆ **Insurance:** An organization may buy insurance to mitigate such risk. Under the scheme of the insurance, the loss is transferred from the insured entity to the insurance company in exchange of a premium. However while selecting such an insurance policy one has to look into the exclusion clause to assess the effective coverage of the policy.
- ◆ **Outsourcing:** The organization may transfer some of the functions to an outside agency and transfer some of the associated risks to the agency. One must make careful assessment of whether such outsourcing is transferring the risk or is merely transferring the management process. For example, outsourcing of telecommunication line viz. subscribing to a leased line does not transfer the risk. The organization remains liable for failure to provide service because of a failed telecommunication line. Consider the same example where the organization has outsourced supply and maintenance of a dedicated leased line communication channel with an agreement that states the minimum service level performance and a compensation clause in the

event failure to provide the minimum service level results in to a loss. In this case, the organization has successfully mitigated the risk.

- ◆ **Service Level Agreements:** Some of risks can be mitigated by designing the service level agreement. This may be entered into with the external suppliers as well as with the customers and users. The service agreement with the customers and users may clearly exclude or limit responsibility of the organization for any loss suffered by the customer and user consequent to the technological failure.

24. (a) Conversion from existing information system to a new system involves the following activities:

- ◆ Defining the procedures for correcting and converting the data into the new application, determining 'what data can be converted through software and what data manually';
- ◆ Performing data cleansing before data conversion;
- ◆ Identifying the methods to assess the accuracy of conversion like record counts and control totals;
- ◆ Designing exception reports showing the data which could not be converted through software; and
- ◆ Establishing responsibility for verifying and signing off and accepting overall conversion by the system owner.

(b) The types of operations into which different office activities under Office Automation Systems can be broadly grouped, are discussed as under:

- ◆ **Document capture:** Documents originating from outside sources like incoming mails, notes, handouts, charts, graphs etc. need to be preserved.
- ◆ **Document Creation:** This consists of preparation of documents, dictation, editing of texts etc. and takes up major part of the secretary's time.
- ◆ **Receipts and Distribution:** This basically includes distribution of correspondence to designated recipients.
- ◆ **Filling, Search, Retrieval and Follow-up:** This is related to filling, indexing, searching of documents, which takes up significant time.
- ◆ **Calculations:** These include the usual calculator functions like routine arithmetic, operations for bill passing, interest calculations, working out the percentages and the like.
- ◆ **Recording Utilization of Resources:** This includes, where necessary, record keeping in respect of specific resources utilized by office personnel.

All the activities mentioned have been made very simple and effective by the use of computers. The application of computers to handle the office activities is also termed as office automation.

- (c) Business Continuity Planning (BCP) is the creation and validation of a practical logistical plan for how an organization will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a Business Continuity Plan. Planning is an activity to be performed before the disaster occurs otherwise it would be too late to plan an effective response. The resulting outage from such a disaster can have serious effects on the viability of a firm's operations, profitability, quality of service, and convenience.

Business Continuity covers the following areas:

- (i) **Business resumption planning** – The Operation's piece of business continuity planning;
 - (ii) **Disaster recovery planning** – The technological aspect of BCP, the advance planning and preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of a disaster.
 - (iii) **Crisis Management** – The overall co-ordination of an organization's response to a crisis in an effective timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation or ability to operate.
- (d) Procedure to apply for a license to issue electronic signature under Section 22, IT (Amendment) Act, 2008 is given follows:
- 1. Every application for issue of a license shall be in such form as may be prescribed by the Central Government.
 - 2. Every application for issue of a license shall be accompanied by
 - (i) a certification practice statement;
 - (ii) a statement including the procedure with respect to identification of the applicant;
 - (iii) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government; and
 - (iv) such other documents, as may be prescribed by the Central Government.

25. (a) **Security Objective** : The objective of information system security is "the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of confidentiality, integrity, and availability".

For any organization, the security objective comprises three universally accepted attributes:

- ◆ **Confidentiality**: Prevention of the unauthorized disclosure of information.

- ◆ *Integrity*: Prevention of the unauthorized modification of information.
- ◆ *Availability*: Prevention of the unauthorized withholding of information.

The relative priority and significance of confidentiality, integrity and availability vary according to the data within the information system and the business context in which it is used.

(b) Prior to know the details of 'how to protect the information systems', we need to define a few basic ground rules that must be addressed sequentially. These rules are:

- ◆ Rule #1: We need to know that 'what the information systems are' and 'where these are located'.
- ◆ Rule #2: We need know the value of the information held and how difficult it would be to recreate if it were damaged or lost.
- ◆ Rule #3: We need to know that 'who is authorized to access the information' and 'what they are permitted to do with the information'.
- ◆ Rule #4: We need to know that 'how quickly information needs to be made available should and it become unavailable for whatever reason (loss, unauthorized modification, etc.)'

(c) Major Information Security Policies relevant for the organization are given as follows:

- ◆ **Information Security Policy**: This policy provides a definition of Information Security, its overall objective and the importance applies to all users.
- ◆ **User Security Policy**: This policy sets out the responsibilities and requirements for all IT system users. It provides security terms of reference for Users, Line Managers and System Owners.
- ◆ **Acceptable Usage Policy**: This sets out the policy for acceptable use of email and Internet services.
- ◆ **Organizational Information Security Policy**: This policy (the one you are reading) sets out the Group policy for the security of its information assets and the Information Technology (IT) systems processing this information. (Although it is positioned at the bottom of the above hierarchy diagram, it is the main IT security policy document.)
- ◆ **Network & System Security Policy**: This policy sets out detailed policy for system and network security and applies to IT department users
- ◆ **Information Classification Policy**: This policy sets out the policy for the classification of information
- ◆ **Conditions of Connection**: This policy sets out the Group policy for connecting to their network. It applies to all organizations connecting to the Group, and relates to the conditions that apply to different suppliers' systems.