PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

Question No. 1 is compulsory.

*Attempt any **five** questions from the remaining **six** questions.*

Question 1

ABC Udyog, a leading automobile company is having several manufacturing units, located in different parts of the world and manufacturing several types of automobiles. The units are working on legacy systems using an internet and collating information, but using different software and varied platforms (Operating Systems) which do not allow communication with each other. This results in huge inflow of duplicate data.

The company wishes to centralize and consolidate the information flowing from its manufacturing units in a uniform manner across various levels of the organizations, so that the necessary data required for preparing MIS reports, budget, and profit/loss accounts etc. could be available timely.

The company decided to engage XYZ consultancy Services for the development of new system. Being a Senior Project Leader of the Consultancy Services, you are entrusted with the responsibilities of handling this project.

Read the above carefully and answer the following with justifications:

(a) What areas are required to be studied in order to know about the present system? Write the problems that the ABC Udyog is presently facing. (5 Marks)

(b) Will you suggest ERP solution to overcome the problems? If yes, explain why. (5 Marks)

(c) What kind of training you will recommend to enrich the human resources for effective utilization of the proposed new system and standards? (5 Marks)

(d) What are various backup techniques? Which backup technique, you will recommend and why ? (5 Marks)

Answer

(a) The following are the major areas, which should be studied in depth in order to understand the present system:

(i) Review historical aspects: A brief history of the organization is a logical starting point for an analysis of the present system. The historical facts shall identify the major turning points and milestones that have influenced its growth. A review of annual reports and organization charts can identify the growth of management levels as well as the development of various functional areas and departments.

(ii) Analyze inputs: A detailed analysis of the present inputs is important since they are basic to the manipulation of data. Source documents are used to capture the originating data for any type of system.

(iii) Review data files maintained: The analyst should investigate the data files maintained by each department, noting their number and size, where they are located, who uses them and the number of times per given time interval these are used.

(iv) Review methods, procedures and data communications: A system analyst also needs to review and understand the present data communications used by the organization. S/he must review the types of data communication equipments, including data interface, data links, modems, dial-up and leased lines and multiplexers.

(v) Analyze outputs: The outputs or reports should be scrutinized carefully by the system analysts in order to determine 'how well they will meet the organization's needs'.

(vi) Review internal controls: A detailed investigation of the present information system is not complete until internal controls are reviewed. Locating the control points helps the analyst to visualize the essential parts and framework of a system.

(vii) Model the existing physical system and logical system: As the logic of inputs, methods, procedures, data files, data communications, reports, internal controls and other important items are reviewed and analyzed in a top down manner; the process must be properly documented.

(viii) Undertake overall analysis of present system: The final phase of the detailed investigation includes the analysis of the present work volume; the current personnel requirements; the present benefits and costs and each of these must be investigated thoroughly.

Presently, ABC Udyog is facing the following major problems:

- The company having its branches all over the world, is engaged in manufacturing of several types of automobiles. The units are working on legacy systems using an internet and collating information. Each unit is using different type of software on varied platforms (operating systems), 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 units has resulted *into duplication of the data entry,* which is very costly. In addition, *timely availability of necessary and relevant data* required for the preparation of MIS Reports, budget, profit/loss account etc. is another important concern in the present system.
- It is confronted with the problem of *centralizing and consolidating the information flowing in from its various units* in uniform manner across various levels of the organization. Hence, there is an urgent need of a system that would entrust the company to address these important issues.

(b) Yes, we recommend that ABC Udyog should implement ERP Solution to overcome the above mentioned problems. ERP implementation will bring different business functions, personalities, procedures, ideologies and philosophies on one platform. In addition, ERP effectively integrates different modules and brings worthwhile and beneficial changes throughout the organization.

Following are the major reasons to implement ERP solutions:

- It provides multi-platform, multi-facility, multi-mode manufacturing, multi-currency, multi-lingual facilities.
- It supports strategic and business planning activities, operational planning and execution activities etc. All these functions are effectively integrated for flow and update of information immediately upon entry of any information.
- It facilitates company-wide Integrated Information System covering all functional areas like manufacturing, selling and distribution, payables, receivables, inventory, accounts, human resources, purchases etc.
- It provides complete integration of systems not only across the departments but also across the companies under the same management.
- It is the solution for better project management.
- It allows automatic introduction of the latest technologies like Electronic Fund Transfer (EFT), Internet, Intranet, Video conferencing, E-Commerce etc.
- It eliminates most business problems like material shortages, productivity enhancements, customer service, cash management, inventory problems, quality problems, prompt delivery etc.
- It provides intelligent business tools like decision support system, Executive information system, Data mining and easy working systems to enable better decisions.

(c) The human resources involved in the proposed new system and standards can be enriched by the following activities/trainings:

- Training Personnel: A system can succeed or fail depending on the way it is operated and used. Therefore, the quality of training received by the personnel involved with the system in various capacities helps in the successful implementation of the proposed system and standards. Thus, training is a major component of systems implementation. When a new system is acquired, which often involves new hardware and software, both users and computer experts need training organized by the vendor through hands-on learning techniques.
- Training Systems Operators: The effective implementation of new systems and standards also depend on the computer-centre personnel, who are responsible for keeping the equipment running as well as for providing the necessary support services. Their training must ensure that they are able to handle all possible operations, both routine and extra-ordinary. As part of their training, operators should be given a trouble shooting list that identifies possible problems and remedies for them. Training also involves familiarization with run procedures, which involve working through the sequence of activities needed to use a new system on an on-going basis.

- User's training: User's training deals with the operation of the system itself. The users need to have the skill for using the functionality relevant to their roles. They should understand the basic concepts of ERP and also how to perform the day-to-day activities in the ERP system.
- Managers' Training: Others, who require training, include managers, who should have at least an appreciation of 'what the system does'. Ideally, the project manager should have a good understanding of all the aspects of the system so that s/he can be effective in dealing with any issues raised. It is also required to have managers directly involved in evaluating the effectiveness of training activities because training deficiencies can translate into reduced user productivity level.
- System Administrators' Training: The system administrators need to be able to setup the system and then maintain it. They will require knowledge about how to handle system security and deal with technical problems. They will need to develop a level of understanding of the functionality so that, at some stage after implementation when the project team is disbanded, they are able to manage the system smoothly.
- Training other Personnel: A selected number of people will require more specific technical training so that they can design databases, write scripts, manage users, generate reports and run query in the database for specific requirements.

(d) Various back-up techniques are described as follows:

(i) Full Backup: A full backup captures all the 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.

(ii) 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. You will have to start with recovering the last full backup, and then recovering from every incremental backup taken since.

(iii) Differential Backup: A differential backup stores files that have changed since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up. Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

Restoring from a differential backup is a two-step operation: Restoring from the last full backup; and then restoring the appropriate differential backup. The downside to

using differential backup is that each differential backup will probably include files that were already included in earlier differential backups.

(iv) Mirror back-up: A mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they can not be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

In the present system, we recommend incremental backup because ABC Udyog has manufacturing units working on the legacy systems. Secondly, incremental backup 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, which is the current need of the automobile company.

Question 2

(a) Define the term "Information". Discuss various important attributes that are required for useful and effective information. (8 Marks)

(b) At the end of analysis phase, the System Analyst prepares a document called "Systems Requirement Specifications (SRS)". Write the contents of SRS. (4 Marks)

(c) What is the significance of Post Implementation Review? How it is performed? (4 Marks)

Answer

(a) Information: Information is the data that have been put into a meaningful and useful context. It has been defined by Davis and Olson as-"Information is data that has been processed into a form that is meaningful to the recipient and is of real or perceived value in current or progressive decision". For example, data regarding sales by various salesmen can be merged to provide information regarding total sales through sales personnel. This information is of vital importance to a marketing manager who is trying to plan for future sales.

Attributes of Information: The important attributes of useful and effective information are as follows:

- Availability: This is a very important property of information. If information is not available at the time of need, it is useless. Data is organized in the form of facts and figures in databases and files from where various information is derived for useful purpose.
- Purpose: Information must have purposes at the time, it is transmitted to a person or machine, otherwise it is simple data. Information communicated to people has a variety of purposes because of the variety of activities performed by them in business organizations. The basic purpose of information is to inform, evaluate, persuade, and organize.
- Mode and format: The modes of communicating information to humans are sensory (through sight, hear, taste, touch and smell) but in business they are either

visual, verbal or in written form. Format of information should be so designed that it assists in decision making, solving problems, initiating planning, controlling and searching.

- Decay: Value of information usually decays with time and usage and so it should be refreshed from time to time. From example, we access the running score sheet of a cricket match through Internet sites and this score sheet is continually refreshed at a fixed interval or based on status of the state.
- Rate: The rate of transmission/reception of information may be represented by the time required to understand a particular situation. Quantitatively, the rate for humans may be measure by the number of numeric characters transmitted per minute, such as sales reports from a district office. For machines the rate may be based on the number of bits of information per character (sign) per unit of time.
- Frequency: The frequency with which information is transmitted or received affects its value. Financial reports prepared weekly may show so little changes that they have small value, whereas monthly reports may indicate changes big enough to show problems or trends.
- Completeness: The information should be as complete as possible. The classical ROI or Net Present Value (NPV) models just provide a point estimate and do not give any indication of the range within which these estimates may vary. Hartz's model for investment decisions provides information on mean, standard deviation and the shape of the distribution of ROI and NPV. With this complete information, the manager is in a much better position to decide whether or not to undertake the venture.
- Reliability: It is just not authenticity or correctness of information; rather technically it is a measure of failure or success of using information for decision making. If information leads to correct decision on many occasions, we say the information is reliable.
- Validity: It measures the closeness of the information to the purpose which it purports to serve. For example, some productivity measure may not measure, for the given situation, what they are supposed to do e.g., the real rise or fall in productivity. The measure suiting the organization may have to be carefully selected or evolved.
- Quality: Quality refers to the correctness of information. Information is likely to be spoiled by personal bias. For example, an over-optimistic salesman may give rather too high estimates of the sales. This problem, however, can be circumvented by maintaining records of salesman's estimates and actual sales and deflating or inflating the estimates in the light of this.
- Transparency: If information does not reveal directly 'what we want to know for decision-making', it is not transparent. For example, total amount of advance does not give true picture of utilization of fund for decision about future course of action; rather deposit-advance ratio is perhaps more transparent information in this matter.

- Value of information: It is defined as difference between the value of the change in decision behavior caused by the information and the cost of the information. In other words, given a set of possible decisions, a decision-maker may select one on basis of the information at hand. If new information causes a different decision to be made, the value of the new information is the difference in value between the outcome of the old decision and that of the new decision, less the cost of obtaining the information.
- Adequacy: To be useful, an information must be adequate so that the desired actions can be initiated. Required information should flow on different directions within the organization and to and from its environment. Further, the type of information that flows within the organization or across, it should have adequate and relevant contents.

(b) At the end of the analysis phase, the System Analyst prepares a document called "Systems Requirement Specifications (SRS)". A SRS contains the following:

- Introduction: Goals and Objectives of the software context of the computer-based system;
- Information Description: Problem description; Information content, flow and structure; Hardware, software, human interfaces for external system elements and internal software functions.
- Functional Description: Diagrammatic representation of functions; Processing narrative for each function; Interplay among functions; Design constraints.
- Behavioral Description : Response to external events and internal controls
- Validation Criteria: Classes of tests to be performed to validate functions, performance and constraints.
- Appendix: Data flow / Object Diagrams; Tabular Data; Detailed description of algorithms charts, graphs and other such material.
- SRS Review : It contains the following :
  - The development team makes a presentation and then hands over the SRS document to be reviewed by the user or customer.
  - The review reflects the development team's understanding of the existing processes. Only after ensuring that the document represents existing processes accurately, should the user sign the document. This is a technical requirement of the contract between users and development team / organization.

(c) A Post Implementation Review answers the question "Did we achieve what we set out to do in business terms?" It examines the efficacy of all elements of the working business solution to see if further improvements can be made to optimize the benefits delivered.

After a development project is completed, a post implementation review should be performed to determine if the anticipated benefits were achieved. Reviews help to control project development activities. The full scope of a post implementation review ("PIR") will depend largely on the scale and complexity of the project.

The post implementation review is performed jointly by the project development team and the appropriate end users. Alternatively, an independent group not associated with the development process, either internal or external, should carry out the audit, to meet the following objectives:

- *Business objectives e.g.* delivered within budget and deadline; producing predicted savings and benefits, etc.;
- *User expectations e.g.* user friendly, carries the workload, produces the required outputs, good response time, reliable, good ergonomics, etc.;
- *Technical requirements e.g.* capable of expansion, easy to operate and maintain, interfaces with other systems, low running cost, etc.

The PIR is undertaken after any changes and tuning that are necessary to achieve a stable system have been completed, and any significant problems have had a chance to surface. Sufficient time should also be allowed for the system's users to become familiar with it. These criteria should be met between six and twelve months after implementation. If the PIR is delayed beyond twelve months there will be an increasing risk that changing requirements - leading to further releases of the system - will obscure the outcome from the original development; also, that the need for a PIR will be overtaken by other priorities.

Question 3

(a) How will you define a risk assessment? Briefly explain various review areas to be focused upon. *(8 Marks)*

(b) Following are involved in the System Development Life Cycle(SDLC). Discuss their roles:

(i) Project Manager

(ii) System Analyst

(iii) Database Administrator (DBA)

(iv) IS Auditor *(4 Marks)*

(c) Draw the flowchart to find the sum of first 50 even numbers, starting from 2. *(4 Marks)*

Answer

(a) Risk assessment is the analysis of threats to resources (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status in the minimum time in case of a disaster. Risk assessment is a useful technique to assess the risks involved

in the event of unavailability of information, to priorities applications, identify exposures and develop recovery scenarios.

The areas to be focused upon for review are given below:

(a) Prioritization: All applications are inventoried and critical ones identified. Each of the critical applications is reviewed to assess its impact on the organization, in case a disaster occurs. Subsequently, appropriate recovery plans are developed.

(b) Identifying critical applications: Amongst the applications currently being processed the critical applications are identified. Further analysis is done to determine specific jobs in the applications which may be more critical. Even though the critical value would be determined based on its present value, future changes should not be ignored.

(c) Assessing their impact on the organization: Business continuity planning should not concentrate only on business disruption but should also take into account other organizational functions which may be affected. The areas to be considered include:

- Legal liabilities;
- Interruptions of customer services;
- Possible losses; and
- Likelihood of fraud and recovery procedures.

(d) Determining recovery time-frame: Critical recovery time period is the period of time in which business processing must be resumed before the organization incurs severe losses. This critical time depends upon the nature of operations. It is essential to involve the end users in the identification of critical functions and critical recovery time period.

(e) Assess Insurance coverage: The information system insurance policy should be a multiperil policy, designed to provide various types of coverage. Depending on the individual organization and the extent of coverage required, suitable modifications may be made to the comprehensive list, which include various items namely, hardware facilities, software reconstruction, extra expenses, business interruption, valuable paper and records, Errors and omissions, fidelity coverage, and media transportation.

(f) Identification of exposures and implications: It is not possible to accurately predict as to when and how a disaster would occur. So, it is necessary to estimate the probability and frequency of disaster.

(g) Development of recovery plan: The plan should be designed to provide for recovery from total destruction of a site.

(b) (i) Project Manager : A project manager is normally responsible for more than one project and liaisons with the client or the affected functions. S/he is responsible for

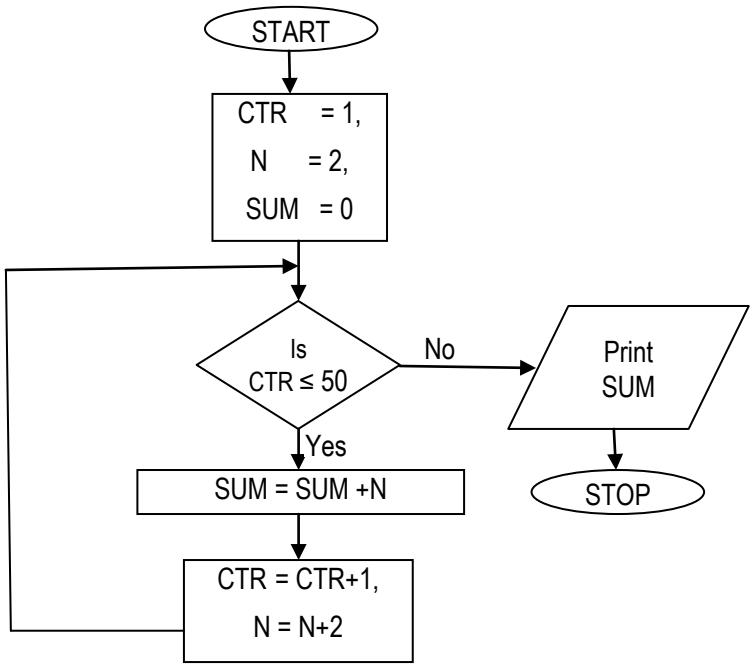
delivery of the project within the time and budget and periodically reviewing the progress of the project with the project leader and his/her team.

(ii) Systems Analyst: The systems/business analysts' main responsibility is to conduct interviews with users and understand their requirements. S/he is a link between the users and the programmers to convert the users requirements in the system requirements and plays a pivotal role in the Requirements analysis and Design phase.

(iii) Database Administrator (DBA) : The data in a database environment has to be maintained by a specialist in database administration so as to support the application program. The DBA handles multiple projects; ensures the integrity and security of information stored in the database and also helps the application development team in database performance issues. Inclusion of new data elements has to be done only with the approval of the database administrator.

(iv) IS Auditor : As a member of the team, IS Auditor ensures that the application development also focuses on the control perspective. He should be involved at the Design Phase and the final Testing Phase to ensure the existence and the operations of the Controls in the new software.

(c)



Question 4

(a) Explain the various general components of Disaster Recovery Plan.' *(6 Marks)*

(b) What is Data Privacy? Explain the major techniques that are used to address Privacy Protection for IT Systems. (6 Marks)

(c) In what ways, an audit trails is used to support security objectives? Describe each one of them. (4 Marks)

Answer

(a) The general components of a disaster recovery plan are given as follows:

- The conditions for activating the plans, which describe the process to be followed before each plan, are activated.
- Emergency procedures, which describe the actions to be taken following an incident which jeopardizes business operations and/or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities e.g. police, fire, services and local government.
- Fallback procedures, which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time-scale.
- Resumption procedures, which describe the actions to be taken to return to normal business operations.
- A maintenance schedule, which specifies how and when the plan will be tested, and the process for maintaining the plan.
- Awareness and education activities, which are designed to create an understanding of the business continuity, process and ensure that the business continues to be effective.
- The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
- Contingency plan document distribution list.
- Detailed description of the purpose and scope of the plan.
- Contingency plan testing and recovery procedure.
- List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
- Checklist for inventory taking and updating the contingency plan on a regular basis.
- List of phone numbers of employees in the event of an emergency.
- Emergency phone list for fire, police, hardware, software, suppliers, customers, back-up location, etc.
- Medical procedure to be followed in case of injury.
- Back-up location contractual agreement, correspondences.
- Insurance papers and claim forms.

- Primary computer centre hardware, software, peripheral equipment and software configuration.
- Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
- Alternate manual procedures to be followed such as preparation of invoices.
- Names of employees trained for emergency situation, first aid and life saving techniques.
- Details of airlines, hotels and transport arrangements.

The answer stated above described general components of a Disaster Recovery Plan(DRP). However, these components can be categorized under the four heads namely, Emergency Plan, Recovery Plan, Backup Plan and Test Plan. The solution to the question can also be presented as follows:

The general components of the disaster recovery plan which is described as the contingency measures that organizations have adopted at key computing sites to recover from, or to prevent any monumentally bad event or disaster are as follows:

- Emergency Plan: This part of the Disaster Recovery Plan (DRP) outlines the actions to be undertaken immediately after a disaster occurs. It identifies the personnel to be notified immediately, for example, fire service, police, management, insurance company etc. It provides guidelines on shutting down the equipment, termination of power supply, removal of storage files and disks, if any. It sets out evacuation procedures like sounding the alarm bell, activating fire extinguishers, evacuation of personnel. It also provides return procedures as soon as the primary facility is ready for operation like backing up data files at offsite, deleting data from disk drives at third party's site, relocation of proper versions of backup files, etc.
- Recovery Plan: This part of the DRP sets out how the full capabilities will be restored. A recovery committee is constituted. Preparing specifications of recovery like setting out priorities for recovery of application systems, hardware replacement etc. will be the responsibility of the Recovery Committee. The following steps may be carried out under this plan:
  - (i) An inventory of the hardware, application systems, system software, documentation etc. must be taken.
  - (ii) Criticality of application systems to the organization and the importance of their loss must be evaluated. An indication must be given of the efforts and cost involved in restoring the various application systems.
  - (iii) An application systems hierarchy must be spelt out.
  - (iv) Selection of a disaster recovery site must be made. A reciprocal agreement with another organization having compatible hardware and software could be made.

(v) A formal back agreement with another company must be made. This should cover the periodical exchange of information between the two sites regarding changes to hardware/software, the time and duration of systems availability, modalities of testing the plan etc.

- Backup Plan: Organizations no matter how physically secure, their systems are always vulnerable to the disaster. Therefore, an effective safeguard is to have a backup of anything that could be destroyed, be it hardware or software. As regards hardware, stand by must be kept with regard to the needs of particular computer environments. So far as the software is concerned, it is necessary to make copies of important programs, data files, operating systems and test programs etc. The backup copies must be kept in a place, which is not susceptible to the same hazards as the originals.
- Test Plan: To provide assurance that the disaster recovery plan is complete, it should be tested, several times. A disaster recovery test plan contains information for simulating various levels of disasters and recording an organization's ability to cover. Any needed recovery actions that are not specified in the plan should be added.

(b) Data Privacy: This refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data. Privacy problems exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. The most common sources of data that are affected by data privacy issues are:

- Health information,
- Criminal justice,
- Financial information,
- Genetic information, and
- Location information.

Privacy protection for IT systems: Increasingly, as heterogeneous information systems with different privacy rules are interconnected, technical control and logging mechanisms (policy appliances) will be required to reconcile, enforce and monitor privacy policy rules (and laws) as information is shared across systems and to ensure accountability for information use. There are several technologies to address privacy protection in enterprise IT systems. These falls into two categories: communication and enforcement.

(i) Policy Communication

- P3P – This is the Platform for Privacy Preferences. P3P is a standard for communicating privacy practices and comparing them to the preferences of individuals.

(ii) Policy Enforcement

- XACML - The extensible Access Control Markup Language (XACML) together with its Privacy Profile is a standard for expressing privacy policies in a machine readable language which a software system can use to enforce the policy in enterprise IT systems.
- EPAL - The Enterprise Privacy Authorization Language (EPAL) is very similar to XACML, but is not yet a standard.
- WS-Privacy - "Web Service Privacy" will be a specification for communicating privacy policy in web services. For example, it may specify how privacy policy information can be embedded in the SOAP envelope of a web service message.

(c) Audit trails can be used to support security objectives in three ways:

- Detecting unauthorized access to the system,
- Facilitating the reconstruction of events, and
- Promoting personal accountability.

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

(i) Detecting Unauthorized Access: Detecting unauthorized access can occur in real time or after the fact. The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls. A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by a virus or worm. After-the-fact detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.

(ii) Reconstructing Events: Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors. Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future.

(iii) Personal Accountability: Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behavior. Individual accountability will normally increase because their actions will be recorded in an audit log.

Question 5

(a) As a system auditor, what control measures will you check to minimize threats, risks and exposures to a computerized system? *(8 Marks)*

(b) Describe the advantage and disadvantage of Continuous Auditing Techniques in brief. *(4 Marks)*

(c) What are commonly used techniques to assess and evaluate risks? Explain each one of them. (4 Marks)

Answer

(a) Various control measures that will be checked by the system auditor to minimize threats, risks and exposures in a computerized system are discussed below:

(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, and audit of adequacy of data integrity etc.

(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, procedures and standards, 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 programs 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 polices regarding sharing and external software usage, updated anti-virus software with detection, identification and removal tools, use of diskless PCs and workstations, installation of intrusion detection and prevention 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) Continuous Auditing Technique: Continuous auditing enables auditors to shift their focus from the traditional 'transaction' audit to the 'system and operations' audit.

Advantages: Some of the 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 analyzed 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 testing 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.

Disadvantages: The following are some of the disadvantages and limitations of the continuous audit system:

- Auditors should be able to obtain resources required from the organization to support development, implementation, operation, and maintenance of continuous audit techniques.
- Continuous audit techniques are more likely to be used if auditors are involved in the development work associated with a new application system.
- Auditors need the knowledge and experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.
- Continuous auditing techniques are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.
- Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.

(c) Following are the most commonly used techniques to access and evaluate risks:

- Judgment and intuition,
- The Delphi Approach,
- Scoring,
- Quantitative Techniques, and
- Qualitative 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 technique 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 complied 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.

(v) Qualitative Techniques: These are by far the most widely used approach to risk analysis. Probability data is not required and only estimated potential loss is used. Most qualitative risk analysis methodologies make use of a number of interrelated elements, namely, threats, vulnerabilities, and controls.

Question 6

(a) What is take significance of a Business Impact Analysis? Enumerate the tasks to be undertaken in this analysis. In what ways the information can be obtained for this analysis? (8 Marks)

(b) Give the hierarchy of Information Security Policies and discuss each one of them. (4 Marks)

(c) Describe the composition and powers of Cyber Regulatory Appellate Tribunal. (4 Marks)

Answer

(a) Business Impact Analysis: Business Impact Analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. It enables the business continuity team to identify critical systems, processes and functions, assess the economic impact of incidents and disasters that result in a denial of access to the system, services and facilities, and assess the "pain threshold," that is, the length of time business units can survive without access to the system, services and facilities.

The business impact analysis is intended to help and understand the degree of potential loss (and various other unwanted effects), which could occur. This will cover not just direct financial loss, but other issues, such as reputation damage, regulatory effects, etc.

A number of tasks are to be undertaken in this phase as enumerated under:

(i) Identify organizational risks - This includes single point of failure and infrastructure risks. The objective is to identify risks and opportunities and to minimize potential threats that may lead to a disaster.

(ii) Identify critical business processes.

(iii) Identify and quantify threats/ risks to critical business processes both in terms of outage and financial impact.

(iv) Identify dependencies and interdependencies of critical business processes and the order in which they must be restored.

(v) Determine the maximum allowable downtime for each business process.

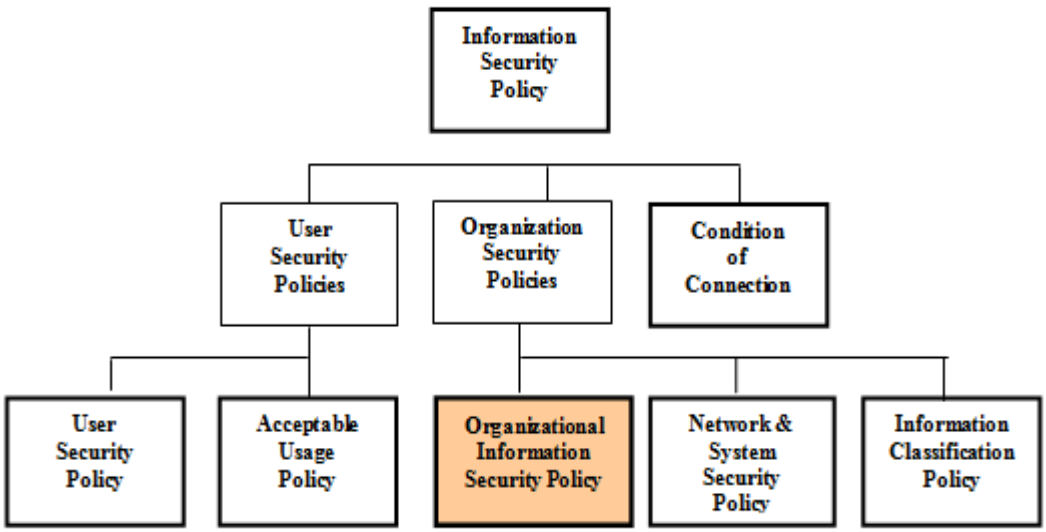
(vi) Identify the type and the quantity of resources required for recovery e.g. tables, chairs, faxes, photocopies, safes, desktops, printers, etc.

(vii) Determine the impact to the organization in the event of a disaster, e.g. financial reputation, etc.

There are a number of ways to obtain this information:

- Questionnaires,
- Workshops,
- Interviews, and
- Examination of documents.

(b) The hierarchy of various Information Security Policies is shown in the following figure:



Each of the Information Security Policy given in the above figure is briefly discussed below:

- Information Security Policy – This policy provides a definition of Information Security, its overall objective and the importance that 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 sets out the Group policy for the security of its information assets and the Information Technology (IT) systems processing this information. Though it is positioned at the bottom of the hierarchy, 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.

(c) Cyber Regulatory Appellate Tribunal: As per Information Technology (Amendment) Act, 2008, the cyber regulation appellate tribunal shall consist of one person only called the Presiding Officer of the Tribunal who shall be appointed by the Central Government. The person must be qualified to be a Judge of a High Court or is or has been a member of Indian Legal Services in the post in Grade I of that service for at least three years. The Presiding Officer shall hold the office for a term of five years or upto a maximum age limit of 65 years, whichever is earlier.

Some of the powers specified are given as follows:

(i) Summoning and enforcing the attendance of any person and examining him on oath;

(ii) Requiring the discovery and production of documents or other electronic records;

(iii) Receiving evidence on affidavits;

(iv) Issuing commissions for examination of witnesses or documents;

(v) Reviewing the decisions;

(vi) Dismissing an application for default or deciding its ex party;

(vii) Any other matter which may be prescribed.

Question 7

Write Short Notes on any FOUR of the following:

(a) Objectives of an Operating System (4 Marks)

(b) Information System Maintenance (4 Marks)

(c) Client/ Server Technology (4 Marks)

(d) Locks on Doors with respect to Physical Access Control (4 Marks)

(e) HIPAA (4 Marks)

Answer

(a) Objectives of an Operating System : An operating system (OS) is a program that controls the execution of an application program and acts as an interface between the user of a computer and computer hardware. The purpose of an OS is to provide an environment in which a user can execute programs in a convenient and efficient manner. An operating system is an important part of almost every computer system. It is considered to be the backbone of a computer, managing both software and hardware resources. Operating systems are responsible for everything from the control and allocation of memory to recognizing input from external devices and transmitting output to computer displays. They also manage files on computer hard drives and control peripherals, like printers and scanners.

Major objectives/functions of an operating system are given as follows:

- *Scheduling of Jobs:* Operating Systems can determine the sequence in which jobs are executed, using priorities established.
- *Managing Hardware and Software Resources:* They can first cause the user's application program to be executed by loading it into primary storage and then cause the various hardware units to perform as specified by the application.
- *Maintaining System Security:* They may require users to enter a password - a group of characters that identifies users as being authorized to have access to the system.
- *Enabling Multiple User Resource Sharing:* They can handle the scheduling and execution of the application programs for many users at the same time, a feature called multiprogramming.
- *Handling Interrupts:* An interrupt is a technique used by the operating system to temporarily suspend the processing of one program in order to allow another program to be executed. Interrupts are issued when a program requests an operation that does not require the CPU, such as input or output, or when the program exceeds some predetermined time limit.
- *Maintaining Usage Records:* They can keep track of the amount of time used by each user for each system unit - the CPU, secondary storage, and input and output

devices. Such information is usually maintained for the purpose of charging users' departments for their use of the organization's computing resources.

(b) Information System Maintenance : Maintaining the system is an important aspect of SDLC. As key personnel change positions in the organization, new changes will be implemented, which will require system updates. Most information systems require at least some modification after development. The need for modification arises from a failure to anticipate all requirements during system design and/or from changing organizational requirements.

Maintenance can be categorized in the following ways:

- *Scheduled maintenance*: Scheduled maintenance is anticipated and can be planned for. For example, the implementation of a new inventory coding scheme can be planned in advance.
- *Rescue maintenance*: Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate solution. A system that is properly developed and tested should have few occasions of rescue maintenance.
- *Corrective maintenance*: Corrective maintenance deals with fixing bugs in the code or defects found. A defect can result from design errors, logic errors; coding errors, data processing and system performance errors. The need for corrective maintenance is usually initiated by bug reports drawn up by the end users. Examples of corrective maintenance include correcting a failure to test for all possible conditions or a failure to process the last record in a file.
- *Adaptive maintenance*: Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system. The term environment in this context refers to the totality of all conditions and influences which act from outside upon the system, for example, business rule, government policies, work patterns, software and hardware operating platforms. The need for adaptive maintenance can only be recognized by monitoring the environment.
- *Perfective maintenance*: Perfective maintenance mainly deals with accommodating to new or changed user requirements and concerns functional enhancements to the system and activities to increase the system's performance or to enhance its user interface.
- *Preventive maintenance*: Preventive maintenance concerns activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system. The long-term effect of corrective, adaptive and perfective changes increases the system's complexity. As a large program is continuously changed, its complexity, which reflects deteriorating structure, increases unless work is done to maintain or reduce it. This work is known as preventive change.

(c) Client/Server Technology : Client/Server (C/S) technology refers to computing technologies in which the hardware and software components (i.e., clients and servers) are distributed across a network. The client/server software architecture is a versatile, message-based and modular infrastructure that is intended to improve usability, flexibility, interoperability, and scalability as compared to centralized, mainframe, time sharing computing. This technology includes both the traditional database-oriented C/S technology, as well as more recent general distributed computing technologies. The use of LANs has made the client/server model even more attractive to organizations.

Client/server is described as a `cost-reduction' technology. Some of the Implementation examples of client / server technology are: Online banking application, internal call centre application, Applications for end-users that are stored in the server etc. Major characteristics that reflect the key features of a client / server system are given as follows:

- Client/server architecture consists of a client process and a server process that can be distinguished from each other.
- The client portion and the server portions can operate on separate computer platforms.
- Either the client platform or the server platform can be upgraded without having to upgrade the other platform.
- The server is able to service multiple clients concurrently; in some client/server systems, clients can access multiple servers.
- The client/server system includes some sort of networking capability.
- A significant portion of the application logic resides at the client end.
- Action is usually initiated at the client end, not the server end.
- A user-friendly graphical user interface (GUI) generally resides at the client end.
- A structured query language (SQL) capability is characteristic of the majority of client/ server systems.
- The database server should provide data protection and security.

(d) Locks on Doors with respect to physical access control: Different types of locks on doors for physical security are discussed below:

- Cipher Locks (combination Door Locks): The Cipher Lock consists of a pushbutton panel that is mounted near the door outside of a secured area. There are ten numbered buttons on the panel. To enter, a person presses a four digit number sequence, and the door will unlock for a predetermined period of time, usually ten to thirty seconds.

Cipher Locks are used in low security situations or when a large number of entrances and exists must be usable all the time. More sophisticated and expensive cipher locks can be computer coded with a person's handprint. A matching handprint unlocks the door.

- Bolting Door Locks: A special metal key is used to gain entry when the lock is a bolting door lock. To avoid illegal entry the keys should not be duplicated.
- Electronic Door Locks: A magnetic or embedded chip based plastics card key or token may be entered into a sensor reader to gain access in these systems. The sensor device upon reading the special code that is internally stored within the card activates the door locking mechanism.
- Biometric Door Locks: These locks are extremely secure where an individual's unique body features, such as voice, retina, fingerprint or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected, such as in the military.

(e) 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.