

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

Question No. 1 is compulsory.

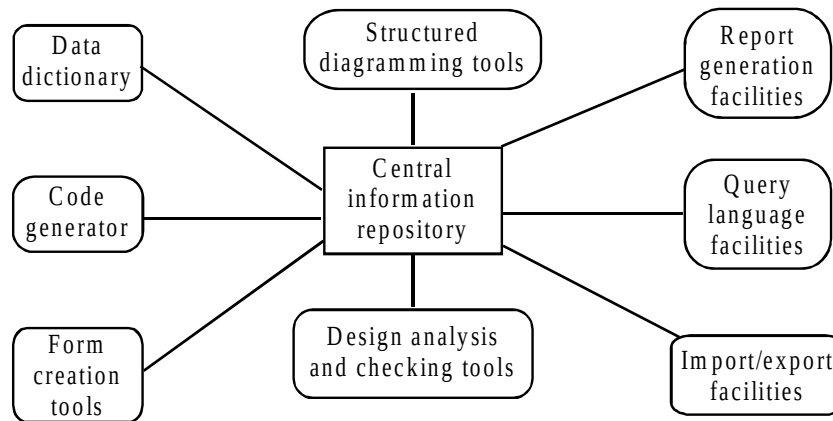
Answer any four questions from remaining six questions.

Question 1

- (a) Discuss various factors that render manual audit method ineffective in Information System audit.
- (b) Briefly explain the components of an analysis and design work bench.
- (c) Briefly discuss any five database control features.
- (d) Discuss briefly the powers of Central Government under Section 87 to make rules in respect of Information Technology Act, 2000. (5 + 5 + 5 + 5 = 20 Marks)

Answer

- (a) The audit methods that are effective for manual audits prove ineffective in many IS audits because of following factors.
 - (i) Electronic evidence: Essential evidence is not physically retrievable by most auditors and it is not readable in its original electronic form.
 - (ii) Terminology: The tools and techniques used in automated applications are described in terms that are difficult for the non-EDP auditors to understand.
 - (iii) Automated processes: The methods of processing are automated rather than manual, making it difficult for the non-EDP auditors to comprehend processing concepts and the logic of these concepts.
 - (iv) New risks and controls: Threats to computer systems and the counter measures to those threats are new to non-EDP auditors, and the magnitude of the risks and the effectiveness of the controls are not understood.
 - (v) Reliance on controls: In manual systems, the auditor can place some reliance on hard-copy evidence, regardless of the adequacy of the controls. Whereas, in automated systems, the electronic evidence is only as valid as the adequacy of controls.
- (b) Analysis and design work benches are designed to support the analysis and design stages of the software process where models of the system are created. A typical model is shown in the figure below:



The components of this model are:

- (i) Diagram editors to create data flow diagrams, structured charts, entity relationship diagram and so on.
 - (ii) Design analysis and checking tools which process the design and then submit report on errors and anomalies. These are integrated with editing system so that user errors are trapped at an early stage in the process.
 - (iii) Repository query languages which allow the designer to find the designs and associate design information in the repository.
 - (iv) A data dictionary which maintains precise and unambiguous information about all data elements used in a system design.
 - (v) Report definition and generation tools which take information from the central store and automatically generate system documentation.
 - (vi) Forms definition tools which allow screen and document formats to be specified.
 - (vii) Import-export facilities which allow the interchange of information from the central repository with other development tools.
 - (viii) Code generators which generate code or code skeletons automatically from the design captured in the central store.
- (c) Database control features include the following:
- (i) User View: The user view or subschema is a subset of the total database that defines the user's data domain and provides access to the database. Access privileges to the data, as defined in their views, should be commensurate with the users' legitimate needs. Several users may share a single user view but have different authority levels. Effective access control requires additional security measures.

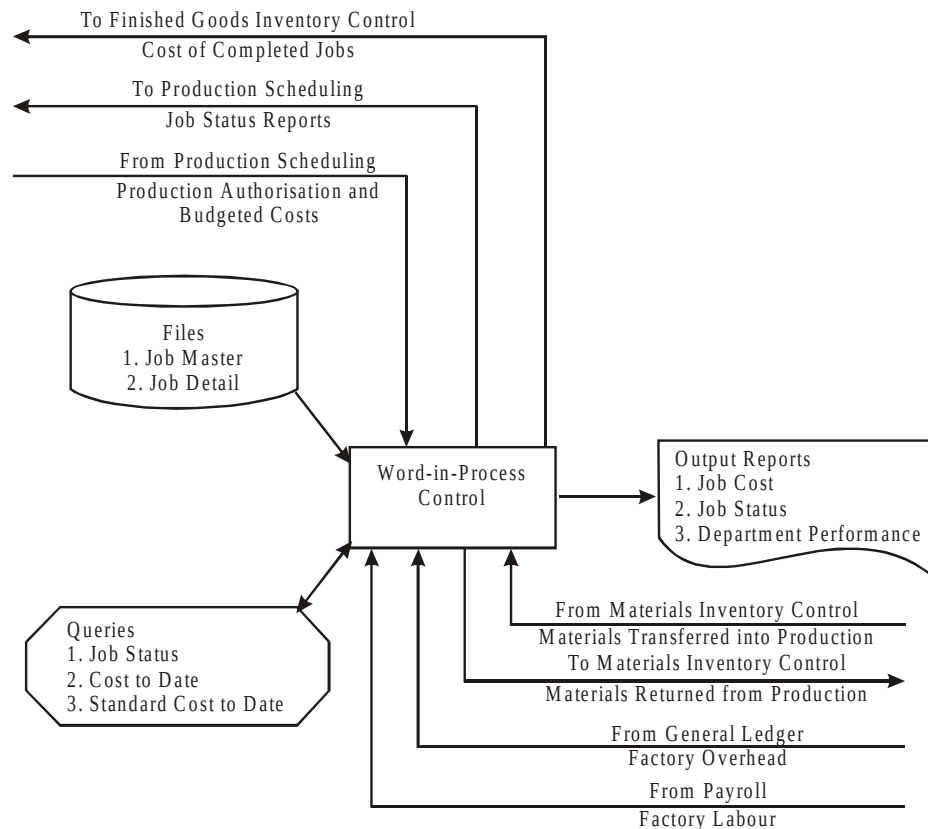
- (ii) Database Authorisation Table: The database authorization table contains rules that limit the actions that a user can take. This technique is similar to the access control list used in the operating system. Each user is granted certain privileges that are coded in the authority table, which is used to verify the user's action requests.
 - (iii) User-Defined Procedures: A user defined procedure allows the user to create a personal security program or routine to provide more positive user identification than a single password can.
 - (iv) Data Encryption: Many database systems use encryption procedures to protect highly sensitive data like password files, certain financial data, product formulae etc. Data encryption uses an algorithm to scramble selected data, thus making it unreadable to an intruder "browsing" the database. Encryption is used for protecting data that are transmitted across networks.
 - (v) Biometric Devices: User authentication procedures use biometric devices, which measure various personal characteristics, such as fingerprints, voice prints, retina prints, or signature characteristics. These user characteristics are digitized and stored permanently in a database security file or on an identification card that the user carries. When an individual attempts to access the database, a special scanning device captures his or her biometric characteristics, which is compared with the profile data stored internally or on the ID card. If the data do not match, access is denied.
- (d) Section 87 of the Act confers on the Central Government the power to make rules. These are:
- (1) The manner in which any matter may be authenticated by a digital signature.
 - (2) The manner and format in which electronic records shall be filed or issued.
 - (3) The type of digital signature, manner and format in which it may be affixed.
 - (4) The security procedure for the purpose of creating same electronic record and secure digital signature.
 - (5) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers.
 - (6) The requirements, manner and form in which application is to be made for a license to issue Digital Signature Certificates.
 - (7) The period of validity of the license.
 - (8) The qualification, experience of an adjudicating Officer, as well as other officers.
 - (9) The salary, allowances and terms and conditions of service of the Presiding Officer, etc.

Question 2

- (a) What is work-in-process control system? Describe briefly the system interfaces, files and inputs, and reports involved in this system.
- (b) Describe the main prerequisites of a MIS which makes it an effective tool. Explain the major constraints in operating it .(10 + 10 = 20 Marks)

Answer

- (a) The work-in-process control system assigns materials, labour and overhead costs to production jobs or products. In a job order system, each cost is assigned to a specific job. In a process costing system, costs are assigned to departments and then to products. The objectives of a work-in-progress system are to cost jobs through the manufacturing process and provide management with information to assist in controlling cost and measuring the performance of departments or other units within the factory. Therefore, to function properly, the system needs information concerning materials requisitioned for each job, labour employed on each job, overhead costs allocated to each job and the production status of each job. The figure given below depicts the flow of information to and from the job-order control system:



System Interfaces

The work-in-process control system interfaces directly with the payroll, general ledger, finished goods inventory control, production scheduling and materials inventory control systems. Labour cost distribution and factory overhead allocation are inputs from pay-roll and the general ledger systems respectively. Aggregate work-in-process inventory transferred to finished goods is sent from work-in-process control to the general ledger. Once manufacturing is complete, jobs are transferred from work-in-process control to finished goods inventory control.

Authorization to start production along with a bill of materials, specifications, production schedule, and budgeted standard costs are transferred from the production scheduling system. Job status reports are available to this system. Direct and indirect materials are requisitioned from the materials inventory control system.

Files and Inputs

A typical work-in-process system in a manufacturing firm contains a job file that has one record for each job in the manufacturing process. The record contains information regarding job identification number, customer identification, promised completion date, estimated shipping date, promised shipping date, total estimated material cost, total standard labour cost and total standard overhead cost etc.

The job detail file contains in-depth information about each job. When authorization to start a job is received from production scheduling, a record is created for the job. A bill of materials, a machine schedule and a labour schedule are entered into the file.

Reports

The work-in-process control system produces job cost, job status and department performance reports periodically. A job cost report contains a detailed summary of the costs incurred to date, the budgeted cost, and estimated completion dates for each job in this system. Reports are helpful in saving time because we get all the information in summarized form.

(b) The main pre-requisites of an effective MIS are as follows:

- (i) Database: It can be defined as a "superfile" which consolidates data records formerly stored in many data files. The data in a database is organized in such a way that access to the data is improved and redundancy is reduced. The characteristics of database are:
 - ◆ The database is sub-divided into major information subsets needed to run a business wherein each subsystem utilizes same data and information kept in same file to satisfy its information needs.
 - ◆ It is user-oriented.
 - ◆ It is capable of being used as a common data source, to various users, helps in avoiding duplication of efforts in storage and retrieval of data and information.

- ◆ It is available to authorized persons only.
 - ◆ It is controlled by a separate authority established for the purpose, known as Data Base Management System (DBMS).
 - ◆ The maintenance of data in database requires computer hardware, software and experienced computer professionals.
- (ii) Qualified system and management staff: The second pre-requisite is that it should be manned by qualified officers. For this, the organisational management base should comprise of two categories of officers.
- ◆ Systems and Computer experts: They, in addition to their expertise in their subject area should be capable of understanding management concepts to facilitate the understanding of problems faced by the concern. They should also be clear about the process of decision making and information requirements for planning and control functions.
 - ◆ Management experts: They should understand quite clearly the concepts and operations of a computer.
- (iii) Support of Top Management: The management information system to be effective, should receive the full support of the top management. The reasons for this are as follows:
- ◆ Subordinate managers are usually lethargic about activities which do not receive the support of their superiors.
 - ◆ The resources involved in computer-based information systems are large and are growing larger in view of importance gained by management information system.
- Their whole hearted support and cooperation will help in making MIS an effective one.
- (iv) Control and Maintenance of MIS: Control of the MIS means the operation of the system as it was designed to operate. Sometimes users develop their own procedures or short cut methods to use the system, which reduce its effectiveness. To check such habits of users, the management at each level in the organization should device checks for the information system control. At times, there may be the need for improvements to the system. Formal method and documenting always must be provided. Maintenance is closely related to control.
- (v) Evaluation of MIS: The evaluation of MIS should take into account the following points:
- ◆ Examining whether enough flexibility exists in the system, to cope with any expected or unexpected information requirement in future.
 - ◆ Ascertaining the views of users and the designers about the capabilities and deficiencies of the system.

- ◆ Guiding the appropriate authority about the steps to be taken to maintain effectiveness of MIS.

Constraints in operating MIS

Major constraints which come in the way of operating an information system are:

- (1) Non-availability of experts, who can diagnose the objectives of the organization and provide a desired direction for installing an operating system.
- (2) Experts usually face the problem of selecting the sub-system of MIS to be installed and operated upon.
- (3) Due to varied objectives of business concerns, the approach adopted by experts for designing and implementing MIS is a non-standardised one.
- (4) Non-availability of cooperation from staff in fact is a crucial problem. It should be handled tactfully. Educating the staff by organizing lectures, showing films, training on system and utility of the system may solve this problem.
- (5) There is high turnover of experts in MIS. Turnover in fact arises due to several factors like pay packet, promotion chances, future prospects, behaviour of top ranking managers etc.
- (6) Difficulty in quantifying the benefits of MIS, so that it is easily comparable with cost.

Question 3

- (a) Discuss in detail, how the investigation of present system is conducted by the system analyst.
- (b) Briefly explain various kinds of controls that can be incorporated in the system to make frauds difficult to perpetrate. (10 + 10 = 20 Marks)

Answer

- (a) Detailed investigation of the present system involves collecting, organizing and evaluating facts about the system and the environment in which it operates. Survey of existing methods, procedures, data flow, output, files, input and internal controls should be intensive in order to fully understand the present system and its related problems.

The following areas should be studied in depth:

- (1) Review historical aspects: A brief history of the organization is a logical starting point for an analysis of the present system. The historical facts should identify the major turning points and milestones that have influenced its growth. A review of annual reports provides historical perspective. Organisation chart can identify the growth of management levels as well as the development of various functional areas and departments. The system analyst should investigate what system changes have occurred in the past.
- (2) Analyse inputs: A detailed analysis of 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. The system analyst should be aware of the various sources from where the data are initially captured. The system analyst must understand the nature of each form, what is contained in it, who prepared it, from where the form is initiated, where it is completed, the distribution of the form and other similar considerations.

- (3) 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. The system analyst should also review all on-line and off-line files which are maintained in the organization as it will reveal information about data that are not contained in any outputs.
- (4) Review methods, procedures and data communications: A procedure review is an intensive survey of the methods by which each job is accomplished, the equipment utilized and the actual location of the operations. Its basic objective is to eliminate unnecessary tasks or to perceive improvement opportunities in the present information system. He must review the types of data communication equipments including data interface, data links, modems, dial-up and leased lines and multiplexers. The system analyst must understand how the data communication network is used in the present system so as to identify the need to revamp the network when the new system is installed.
- (5) Analyse outputs: The outputs or reports should be scrutinized carefully by the system analysts in order to determine how well they meet the organization's needs. The analysts must understand what information is needed and why, who needs it and when and where it is needed. Additional questions concerning the sequence of the data, how often the form reporting it is used, how long it is kept on file, etc., must be investigated.
- (6) Review internal controls: Locating the control points helps the analyst to visualize the essential parts and framework of a system. An examination of the present system of internal controls may indicate weaknesses that should be removed in the new system.
- (7) Model the existing physical system and logical system: The logical flow of the present information system may be depicted with the help of system flow charts. The physical-flow of the existing system may be shown by employing data flow diagrams. The data elements needed in the new system will be found in the present system only.
- (8) Undertake overall analysis of present system: The final phase of the detailed investigation includes the analysis of:
 - (a) the present work volume
 - (b) the current personnel requirements
 - (a) the present benefits and costs.

- (b) One way to deter fraud is to design a system with sufficient controls to make fraud difficult to perpetrate. These controls help to ensure the accuracy, integrity and safety of system resources.
- (i) **Develop a strong system of Internal Controls:** The overall responsibility for a secure and adequately controlled system lies with top management. Managers typically delegate the design of adequate control systems to systems analysts, designers, and end users. The corporate information security officer and the operations staff are typically responsible for ensuring that control procedures are followed.
 - (ii) **Segregate Duties:** There must be an adequate segregation of duties to prevent individuals from stealing assets and covering up their tracks.
 - (iii) **Require vacations and Rotate Duties:** Many fraud schemes, such as lapping and kiting, require the ongoing attention of the perpetrator. If mandatory vacations were coupled with a temporary rotation of duties, such ongoing fraud schemes would fall apart.
 - (iv) **Restrict Access to Computer Equipment and Data Files:** Computer frauds can be reduced significantly if access to computer equipment and data files is restricted. Physical access to computer equipment should be restricted, and legitimate users should be authenticated before they are allowed to use the system.
 - (v) **Encrypt Data and Programs:** Another way to protect data is to translate it into a secret code, thereby making it meaningless to anyone without the means to decipher it.
 - (vi) **Protect Telephone Lines:** Computer hackers use telephone lines to transmit viruses and to access, steal, and destroy data. One effective method to protect telephone lines is to attach an electronic lock and key to them.
 - (vii) **Protect the System from Viruses:** There are hundreds of thousands of virus attacks every year, and estimated 90% of the PCs that suffer a virus attack are re-infected within 30 days by the same virus or some other virus. A system can be protected from viruses by ensuring that the latest versions of the anti-virus programs are used.
 - (viii) **Control Sensitive Data:** Controls can be placed over data files to prevent or discourage copying. Employees should be informed of the consequences of using illegal copies of software, and the company should institute controls to see that illegal copies are not in use. Backup tapes, and system documentation should be locked up. Servers and PCs should also be locked when not in use. Companies should never store all of their data in one place or give an employee access to all of it. Closed-circuit televisions can be used to monitor areas where sensitive data or easily stolen assets are handled.
 - (ix) **Control Laptop Computers:** To control laptops, companies should take following measures:

- ◆ Establish laptop security policies to require employees to back up data before travelling and to a separate source when on the road, and to never leave a laptop unattended.
- ◆ Install software that makes it impossible for the computer to boot up without a password.
- ◆ Password protect and encrypt data on the hard disk so that if a laptop is stolen, the data cannot be used.
- ◆ Employees should be asked to store confidential data on a disk, rather than the hard drive, and always keep the diskette in their possession.

Question 4

- (a) Briefly explain the characteristics and features of an Enterprise Resource Planning.
- (b) Briefly discuss four basic components of Decision Support System.
- (c) Define the following computer fraud and abuse technique:
 - (i) War dialing
 - (ii) Scavenging
 - (iii) Cracking
 - (iv) Internet terrorism
 - (v) Masquerading. (5 + 5 + 10 = 20 Marks)

Answer

- (a) Characteristics of ERP are briefly explained below:
 - (i) Flexibility: An ERP system should be flexible to respond to the changing needs of an enterprise. The client-serves technology enables ERP to run across various database backend through Open Database Connectivity (ODBC).
 - (ii) Modular and Open: EPR system has to have open system architecture. This means that any module can be interfaced or detached whenever required without affecting the other modules. It should support multiple hardware platforms for the companies having heterogeneous collection of systems. It must support some third party add-ons also.
 - (iii) Comprehensive: It should be able to support variety of organizational functions and must be suitable for a wide range of business organizations.
 - (iv) Beyond the Company: It should not be confined to the organizational boundaries, rather it should support the on-line connectivity to the other business entities of the organization.
 - (v) Best Business Practices: It must have a collection of the best business processes applicable worldwide. An ERP package imposes its own logic on a company's strategy, culture and organization.

Some of the major features of ERP are:

- ◆ ERP 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, creation of Materials and Resources.
- ◆ It has end-to-end supply Chain Management to optimize the overall Demand and Supply Data.
- ◆ ERP facilitates company-wide Integrated Information system covering all functional areas like manufacturing, selling and distribution, payables, receivables, inventory accounts, human resources, purchases etc.
- ◆ ERP performs core activities and increases customer service, thereby augmenting the corporate image.
- ◆ ERP bridges the information gap across organizations.
- ◆ ERP provides complete integration of systems not only across departments but also across companies under the same management.
- ◆ ERP is the solution for better project management.
- ◆ ERP allows automatic introduction of the latest technologies like Electronic Fund Transfer (EFT), Electronic Data Interchange (EDI), Internet, Intranet, Video conferencing and E-Commerce etc.
- ◆ ERP eliminates most business problems like material shortages, productivity enhancements, customer service, cash management, inventory problems, quality problems, prompt delivery etc.
- ◆ ERP provides intelligent business tools like Decision Support System (DSS), Executive Information System (EIS), Data mining and easy working systems to enable better decisions.

(b) A decision support system has the following components:

- (i) The User: The user of a decision support system is usually a manager with an unstructured or semi-structured problem to solve. Users do not need a computer background to use a decision support system for problem solving. The most important knowledge is a thorough understanding of the problem and the factors to be considered in finding a solution. A user does not need extensive education in computer programming in part because a special planning language performs the communication function within the decision support system.
- (ii) One or more databases: Decision support systems include one or more databases which contain both routine and non-routine data from both internal and external sources. The data from external sources include data about the operating environment surrounding an organization. Decision support system users may

construct additional database themselves. Some of the data may come from internal source.

- (iii) A planning language: Two types of planning languages that are commonly used in decision support system are (1) general purpose planning languages and (2) special purpose planning languages. General purpose planning languages allow users to perform many routine tasks like-retrieving various data from a database or performing statistical analysis. The languages in most electronic spreadsheets are good example of general purpose planning languages. These languages enable the user to tackle a broad range of budgeting, forecasting and other worksheet oriented problems. Special purpose planning languages are more limited. Some statistical languages, such as SAS, SPSS and Minitab are examples of special purpose planning languages.
- (iv) Model Base: The model base is the “brain” of the decision support system because it performs data manipulation and computations with the data provided to it by the user and the database. There are many types of model bases but most of them are custom-developed models that do some type of mathematical functions. The analysis provided by the routine in the model base is the key to supporting the user’s decision.
- (c) (i) War dialing: It relates to programming a computer search for an idle modem by dialing thousands of phone lines. Perpetrator enters the system through idle modem, captures the personal computer attached to the modem, and gain access to the network to which the personal computer is attached.
- (ii) Scavenging: Gaining access to confidential information by searching corporate records is termed as scavenging. Scavenging methods range from searching for printouts or carbon copies of confidential information to scanning the contents of computer memory.
- (iii) Cracking: Unauthorized access to and use of computer systems, usually by means of a personal computer and a telecommunications network is called cracking. Crackers are hackers with malicious intentions.
- (iv) Internet terrorism: Using internet to disrupt electronic commerce and to destroy company and individual communications is referred as internet terrorism.
- (v) Masquerading: Under this technique, perpetrator gains access to the system by pretending to be an authorized user and enjoys same privileges as the legitimate user. Fraud messages can be sent to the receiver by using legitimate users identity and thus can prove to be harmful.

Question 5

- (a) Discuss various issues that should be considered while designing system input.
- (b) Briefly explain the risks associated with client / server model.
- (c) “Personnel information system deals with flow of information relating to people.” Explain.

- (d) Briefly describe various steps involved in system testing. (5 + 5 + 5 + 5 = 20 Marks)

Answer

- (a) Various issues involved in designing systems input are discussed below:
- (i) Content: The analyst is required to consider the types of data that are needed to be gathered to generate the desired user outputs. Sometimes, the data needed for a new system are not available within the organization. Hence, the system designer has to prepare new documents for collecting such information.
 - (ii) Timeliness: In data processing, it is very important that data is inputted to computer in time because output cannot be produced until certain inputs are available. Hence, a plan must be established regarding when different types of inputs will enter the system. In transaction data processing, the people requiring output are not the same who input most of the data. Hence, timeliness of input becomes more relevant for such systems.
 - (iii) Media: Input consideration includes the choice of input media and subsequently the devices on which to enter the data. Various user input alternatives available in the market include display workstations, magnetic tapes, magnetic disks, key-boards, optical character recognition, pen-based computers and voice input etc. A suitable medium may be selected depending on the application to be computerized.
 - (iv) Format: While specifying the record formats, the type and length of each data field as well as any other special characteristics must be defined. Designing input formats in mainframe and mini computer database environments often require the assistance of a professional programmer or database administrator. Format is different for different type of operating system.
 - (v) Input volume: Input volume refers to the amount of data that has to be entered in the computer system at any one time.
- (b) The four categories of risks associated with client / server model are briefly discussed below:
- (i) Technological Risks: The technological risk is quite simple. The first risk is – Will the new system work? But more important is the risk that in the long run the system may become obsolete. To resolve this issue, the firm and the IT consultant / division should understand system standards and market trends and use them in their decision making processes while deciding what system to incorporate into their organization.
 - (ii) Operational Risk: These risks parallel the technological risks in both the short and long run. Respectively, they are – Will you achieve the performance you need from the new technology and will the software that you chose be able to grow or adapt to the changing needs of the business.
 - (iii) Economic Risk: In the short run, firms are susceptible to hidden costs associated with the initial implementation of new client / server system. Cost will rise in the

short term since one needs to maintain the old system (mainframe) and the new client server architecture development. In the long run, the concern centres around the support costs of the new system.

- (iv) Political Risks: Finally, political (people) risks involved in this transition are addressed. Here, the short-term question is – will end users and management be satisfied? The answer to this is definitely not if the system is difficult to use or is plagued with problems.
- (c) Personnel Information system deals with the flow of information relating to people working in the organization and future personnel needs. It is concerned with six basic sub-systems of the personnel functions as discussed below:
 - (1) Recruitment: Properly managed recruitment sub-system may forecast personnel needs and skills required for recruiting personnel at the proper time to meet organizational manpower needs.
 - (2) Placement: This sub-system is concerned with the task of matching the available persons with the requirements. A good placement sub-system makes use of latest behavioural tools and techniques.
 - (3) Training and Development: As technological changes and demands for new skills accelerate, many companies find that they must develop much of their requirements from internal sources. In addition, a large part of the work force must constantly be updated in new techniques and developments.
 - (4) Compensation: This sub-system is concerned with the task of determining pay and other benefits for the workers of the concern. It makes use of traditional payroll and other financial records, government reports and unions expectation before arriving at the final figure of pay and other benefits for each category of workers.
 - (5) Maintenance: This sub-system is designed to ensure that personnel policies and procedures are achieved. It may be extended to the operation of systems control, work standards which are required to measure performance against financial plans or other programs and the many subsidiary records normally associated with the collection, maintenance and discrimination of personnel data.
 - (6) Health and Safety: This sub-system is concerned with the health of personnel and the safety of jobs in the organization.
- (d) Steps involved in system testing: System level testing must be conducted prior to installation of an information system. It involves (a) preparation of realistic test data in accordance with the system test plan, (b) processing the test data using the new equipment (c) thorough checking of the results in all system tests and (d) reviewing the results with future users, operators and support personnel. System level testing is an excellent time for training employees in the preparation of the IS as well as maintaining it. One of the most effective ways to perform system-level testing is to perform parallel operations with the existing system. Parallel operations consist of feeding both systems the same input data and comparing data files and output results. Despite the fact that

the individual programs were tested, related conditions and combinations of conditions that have not envisioned are likely to occur. Last minute changes to computer programs are necessary to accommodate the new conditions.

One procedure for testing the new interactive system is to have several remote input terminals connected on line, which are operated by supervisory personnel backed up by other personnel operating in the old system. The outputs are checked for compatibility and appropriate corrections are made to the on-line computer programs. Once this segment of the new system has proved satisfactory, the entire terminal network can be placed into operation for this one work. Additional sections of the system can be added by testing in this manner until all programs are operational.

During parallel operations, the mistakes detected are often not those of the new system but of the old one. These differences should be reconciled as far as it is feasible economically.

Question 6

- (a) Briefly explain the best approach to implement information security policy?
- (b) What is the purpose of the system evaluation? How is it performed?
- (c) Discuss, how a controlled source program library environment can help to deter unauthorized changes to program.
- (d) Briefly explain the role of Information Security Administrator. (5 + 5 + 5 + 5 = 20 Marks)

Answer

- (a) To meet the security objective, develop and maintain adequate controls in compliance with generally accepted core principles, an ongoing and integrated approach is necessary. Executive management and especially chief executive officer support is essential for the successful development, design, implementation, and monitoring of security controls.
 - (i) Security Policies: Every organization should have a security policy that defines acceptable behaviours and the reaction of the organisation when such behaviours are violated.
 - (ii) Policy Development: The security objectives and core principles provide a framework for the first critical step for any organization developing a security policy. The security policy should support and complement existing organizational policies.
 - (iii) Roles and Responsibilities: For security to be effective, it is imperative that individual roles, responsibilities and authority are clearly communicated and understood by all.
 - (iv) Design: Once a policy has been approved by the governing body of the organization and related roles and responsibilities assigned, it is necessary to develop a security and control framework.

- (v) **Implementation:** Once the design of the security standards, measures, practices and procedures has been approved, the solution should be implemented on a timely basis, and then maintained.
 - (vi) **Monitoring:** Information systems are subject to a wide range of disruptive incidence. Hence, there is a need to institute monitoring measures and procedures over systems, processes and their environment to promptly identify, contain damage and expedite recovery.
 - (vii) **Awareness, Training and Education:** People are often the weakest link in securing information. Awareness of the need to protect information, training in the skills needed to operate them securely, and education in security measures and practices are of critical importance for the success of an organization's security program.
- (b) **System evaluation** provides the feedback necessary to assess the value of information and the performance of personnel and technology in the newly designed system. The feedback provides information regarding adjustments required in the Information system. There are two basic dimensions of information systems that should be evaluated. The first dimension is concerned with whether the newly developed system is operating properly. The other dimension is concerned with whether the user is satisfied with the information system with regard to the reports supplied by it.
- (1) **Development evaluation:** Evaluation of the development process is primarily concerned with whether the system was developed on schedule and within budget. It requires schedules and budgets to be established in advance and that records of actual performance and cost be maintained. Due to the uncertainty and mystique associated with system development, they are not subject to traditional management control procedures.
 - (2) **Operation evaluation:** The evaluation of the information system's operation pertains to whether the hardware, software and personnel are capable to perform their duties and they do actually perform them so. Operation evaluation answers such questions.
 - 1. Are all transactions processed on time?
 - 2. Are all values computed accurately?
 - 3. Is the system easy to work with and understand?
 - 4. Is terminal response time within acceptable limits?
 - 5. Are reports processed on time?
 - 6. Is there adequate storage capacity for data?
 - (3) **Information evaluation:** An information system should also be evaluated in terms of information it provides. Satisfaction can be used as a measure to evaluate the information provided by an information system. Measurement of user satisfaction can be accomplished using the interview and questionnaire technique. If

management is generally satisfied with an information system, it is assumed that the system is meeting the requirements of the organization. If management is not satisfied, modifications ranging from minor adjustments to complete redesign may be required.

- (c) A Controlled Source program library environment helps to deter unauthorized changes to program which are discussed below:

Password Control: One form of access control over the SPL (Source Program Library) is provided by assigning passwords. Every financially significant program stored in the SPL can be assigned a separate password.

Separation of Test Libraries: A strict separation is maintained between the production programs that are subject to maintenance in the SPL and those being developed. Production programs are copied into the programmer's library for maintenance and testing purposes only. Passwords for production programs can be changed regularly disclosed only on a need-to-know basis.

Audit trail and Management Report: Important feature of SPL Management software is the creation of reports that enhance management control and the audit function. Program modification reports, which describe in detail all program changes to each module are most useful. During an audit, these reports can be reconciled against program maintenance requests to verify that only the required changes were actually implemented. These reports can be produced as hard copy and also on disk.

Program Version Number: The SPLMS assigns a version number automatically to each program stored on the SPL. When programs are first placed in the libraries, they are assigned a version numbers of zero. With each modification to the program, the version number is increased by one. This feature, when combined with audit trail reports, provides evidence for identifying unauthorized changes to program modules.

Controlling Access to Maintenance Commands: Powerful maintenance commands are available for most library systems that can be used to alter or eliminate program passwords, alter the program version number and temporarily modify a program without generating a record of the modification. Access to the maintenance commands themselves should be password controlled and the authority to use them should be controlled by management or the security group.

Message sequence numbering: An intruder in the communications channel may attempt to delete a message from a stream of messages, change the order of messages received, or duplicate a message. A sequence numbers is inserted in each message and any such attempt will become apparent at the receiving end.

- (d) Role of an Information Security Administrator

An Information Security Administrator (ISA) is a person who is solely responsible for controlling and coordinating the activities pertaining to all security aspects of the

organization. The roles of an ISA are:

- ◆ A security administrator attempts to ensure that the facilities in which systems are developed, implemented, maintained and operated are safe from threats that affect the continuity of installation and or result in loss of security.
- ◆ The security administrator sets policy, subject to board approval.
- ◆ He also investigates, monitors, advise employees, counsels management on matters pertaining to security.
- ◆ He is responsible for establishing the minimal fixed requirements for classification of information based on the physical, procedural and logical security elements. He assigns responsibilities to job classifications and formulates what to be done in case of exceptions.
- ◆ The security administrator guides other information security administrators and users on the selection and application of security measures.
- ◆ Investigates all security violations.
- ◆ Advises senior management on matters of information resource control.
- ◆ Consults on matters of information security.
- ◆ A security administrator also has the responsibility of conducting a security program, which is a series of ongoing, regular, periodic evaluation of the facilities available.
- ◆ A security administrator has to consider an extensive list of possible threats to the organization, prepare an inventory of assets, evaluate the existing controls, implement new controls etc.

The security administrator requires the assistance of many individuals because of their expertise in that particular field. The auditor should see that these steps are performed on a regular basis, the results of the reviews are analysed and documented and advises the management of appropriate action in light of the results.

Question 7

Write short notes on the following:

- (a) Closed and open systems
- (b) Programmed decisions
- (c) Program documentation
- (d) Firewalls.

(4 × 5 = 20 Marks)

Answer

- (a) Closed Systems: A closed system is self contained and does not interact or make exchange across its boundaries with its environment. Closed systems do not get the

feed back they need from the external environment and tend to deteriorate eventually. For example, if a marketing system does not get feed back from the market, its efficiency will gradually continue to decrease.

A relatively closed system is one that has only controlled and well defined inputs and outputs. It is not subject to disturbances from its environment. A computer program can be taken as an example of relatively closed system because it accepts only previously defined inputs, processes them and provides previously defined outputs.

Open Systems: Open systems actively interact with their environment. Such systems regularly get inputs and give outputs to its environment. These systems are also subject to unknown inputs and environmental disturbances. Open systems are also able to adapt to environmental changes for their survival and growth. Business organization is an example of such system.

- (b) Programmed Decisions: Such decision procedures are applicable to situations and problems which are routinely recurring, are more familiar and can be structured. Programmed decisions have built-in pre-decided rules or procedures which are well-structured in advance and are time tested for their validity. Thus, programmed decisions are said to refer to decisions made on problems and situations by reference to a predetermined set of precedents, procedures, techniques and rules. As a consequence, by applying these rules to a problem, a decision emerges. Manager's judgement or discretion is not required. Thus, decision making is simplified.

Organisations evolve a repertory of procedures, rules, processes and techniques for handling routine and recurring problem situations. For example, for many organisations there is a set procedure for receipt of materials, payment of bills etc. These are examples of programmed decisions which tend to be consistent over situations and time.

- (c) Program documentation: The writing of narrative procedures and instructions for people who will use software is done throughout the program life cycle. User documentation should also be reviewed for understandability. Program design and a set of technical design specifications must include the following:
1. A brief narrative description of what the program should do.
 2. A description of the outputs, inputs and processing to be performed by the program.
 3. A deadline for finishing the program.
 4. The identity of the programming language to use and the coding standards to follow.
 5. A description of the system environment into which the program should fit.
 6. A description of the testing required to certify the program for use.
 7. A description of documentation that must be generated for users, maintenance programmers and operational personnel.

- (d) A firewall is a system that enforces access control between networks. To accomplish this:
- ◆ All traffic between the outside network and the organization's intranet must pass through the firewall.
 - ◆ Only authorized traffic between the organization and the outside, as specified by formal security policy, is allowed to pass through the firewall.
 - ◆ The firewall must be immune to penetration from both outside and inside the organization.

Firewalls are of two types as discussed below:

- ◆ Network level firewall: This type of firewall consists of screening router that examines the source and destination addresses that are attached to incoming messages. The firewall accepts or denies access requests based on filtering rules that have been programmed into it.
- ◆ Application level firewall: It provides a high level of customized network security, but can be highly expensive. These systems are configured to run security applications called proxies that permit routine services to pass through firewall. It can also perform functions such as logging or user authentication for specific task. If an outside user attempts to connect to an unauthorized service or file, the network administrator can be notified immediately.