

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

QUESTIONS

1. (a) State and explain any five characteristics of a good Management Information Systems.
(b) Explain three broad categories of the planning information requirements of executives.
2. (a) Explain the four common cycles of a business activity.
(b) What are the major constraints in operating a MIS?
3. Discuss the limitation of the Management Information System.
4. Explain the role played by Financial Information Systems in making financial decisions.
5. (a) Explain Personnel Information Systems.
(b) What are the threats to operating system integrity?
6. Write a short notes on Materials Requirement Planning (MRP).
7. What is an Executive Information System? Discuss its various purposes.
8. (a) Explain the component architecture of the client / server technology.
(b) Describes the benefit of using Client / Server Architecture over other computing model.
9. (a) Define a 2-tier and a 3-tier architecture with reference to client-server architecture.
(b) What are the control techniques to be checked to ensure security for client / server technology?
10. (a) Discuss the reasons as to why organization fail to achieve their systems development objective.
(b) Distinguish between logical design and physical design. In which case is the analyst responsible for the design? What is the role of the programmer and the user?
11. Write short notes on the following:
(a) Data Dictionary.
(b) Systems Development Life Cycle.
12. What are the fact finding techniques used by a system analyst?
13. Discuss with examples, the commonly used coding schemes for data processing?
14. (a) What is an application software?
(b) Discuss the factors upon which “Make or Buy” decision of an application software depends?

- (c) Before purchasing the packaged software, on what features the software will be assessed?
- 15. Describe any five program design tools.
- 16. Detail the principles of Information Security.
- 17. (a) What do you understand by hash function with reference to electronic records?
(b) Briefly describe section 3 of Chapter II of Information Technology Act, 2000 relating to Authentication of Electronic Records.
- 18. Discuss various issues that are of primary concern for an auditor involved in Information System Audit.
- 19. What do you mean by production scheduling? Draw the information flow diagram for design of computerized production scheduling system. Also explain:
 - (i) System interface.
 - (ii) File inputs and
 - (iii) Reports required for the above system.
- 20. (a) List any five ERP vendors and briefly describe the ERP packages offered by them.
(b) What are the benefits achieved by implementing the ERP packages?
- 21. Write a short notes on the following:
 - (a) Security risks associated with personal computers.
 - (b) Personal computers controls.
 - (c) Firewalls.
- 22. (a) Write short notes on the Disc Imaging and Analysis Technique.
(b) How can computer Fraud be committed using input in four different ways?
- 23. What is a Digital Signature? How is it used? What are the duties of certifying authorities in regard to its usage?
- 24. (a) Briefly describe the various objectives to be met while performing an IS audit.
(b) How does MIS auditing enhances the control process?
- 25. (a) Explain the role played by an information security administrator.
(b) Discuss Security Management steps an Internet user should take to protect from Cyber crime and computer security threats.
- 26. (a) Write a short note on Meta-CASE workbenches.
(b) What are five different levels of integration of CASE tools.
- 27. What are the two major categories of exposures in the communication sub-system including Internet and Intranet? What control mechanisms could be used to deal with them?

SUGGESTED ANSWERS/HINTS

1. (a) Five important characteristics for a good management Information systems are briefly discussed below:
 - (i) Management Oriented: It means that effort for the development of the Information System should start from an appraisal of management needs and overall business objectives. A good management Information system is not necessarily meant for top management only, it may also meet the information requirements of middle level or operating levels of management as well.
 - (ii) Management Directed: Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts. Mere one time involvement is not enough. For system's effectiveness, it is necessary for management to devote their sufficient time not only at the stage of designing the system but for its review as well, to ensure that the implemented systems meet the specifications of the designed system. In brief, management should be responsible for setting system specifications and it must play a key role in the subsequent trade off decision that occur in system development.
 - (iii) Integrated: Development of information should be an integrated one. It means that all the functional and operational information sub-systems should be tied together into one entity. An integrated information system has the capability of generating more meaningful information to management. The word integration here means taking a comprehensive view or a complete look at the inter locking sub-systems that operate within a company.
 - (iv) Common data flows: It means that the use of common input, processing and output procedures and media whenever possible is desirable. Data is captured by systems analysts only once and as close to its original source as possible. They, then, try to utilize a minimum of data processing procedures and sub-systems to process the data and strive to minimize the number of output documents and reports produced by the system. This eliminates duplication in data collection, documents and procedures. It also simplifies operations and produces an efficient information system. However, some duplication is necessary in order to ensure effective information systems.
 - (v) Heavy Planning Element: A management information systems usually takes 3 to 5 years and sometimes even longer period to get established firmly within a company. Therefore, a heavy planning element must be present in MIS development. It means that MIS designer should keep in view future objectives and requirements of firm's information in mind. The designer must avoid the possibility of systems obsolescence before the systems gets into operation.

- (b) The planning information requirements of executives can be categorised into three broad categories:
- (i) Environment information: It comprises of the following:
 - Government Policies: Information about concessions / benefits, government policies in respect of tax concessions or any other aspects, which may be useful to the organization in the future period.
 - Factor of production: Information related with sources, cost, location, availability, accessibility and productivity of the major factors of production viz., (i) Labour, (ii) materials and parts and (iii) Capital.
 - Technological environment: Forecast of any technological changes in the industry and the probable effect of it on the firm.
 - Economic trends: It includes information relating to economic indicators like consumer disposal income, employment, productivity, capital investment etc. Such information is valuable for those firms specially whose output is a function of these important variables.
 - (ii) Competitive information: It includes the following information.
 - Industry demand: Demand forecast of the industry in respect of the product manufactured and in the area in which the firm would be operating.
 - Firm demand: Assessment of the firm's product demand in the specified market. It also includes an assessment of firm's capability to meet firm's demand.
 - The competitive data: Data of competing firms for forecasting demand and making decisions and plans to achieve the forecast.
 - (iii) Internal information: It usually includes information concerning organisations' (a) sales forecast, (b) financial plan / budget, (c) supply factor, and (d) policies, which are vital for subsidiary planning at all levels in the organization.
2. (a) (i) Revenue cycle: It comprises of events related to the distribution of goods and services to other entities and the collection of related payments. It includes application systems involving customer order entry, billing, accounts receivables and sales reporting.
- (ii) Expenditure cycle: It comprises of events related to the acquisition of goods and services from other entities and the settlement of related obligations. It include application systems involving vendor selection and requisitioning, purchasing, accounts payable and payroll.
- (iii) Production cycle: It comprises of events related to the transformation of resources into goods and services. It includes application systems involving production control and reporting, product costing, inventory control and property accounting.

- (iv) Finance cycle: It comprises of events related to the acquisition and management of capital funds, including cash. It includes application systems concerned with cash management and control, debt management and the administration of employee benefit plans.
- (b) Major constraints, which come in the way of operating a management information system, are the following:
 - (i) There is non-availability of experts who can diagnose the objectives of the organisation and provide a desired direction for installing and operating information systems. This problem may be overcome by grooming internal staff. The grooming of staff should be preceded by proper selection and training.
 - (ii) Experts usually face the problem of selecting the sub-systems of MIS to be installed and operated upon. The criteria, which should guide the experts here, may be the need and importance of a function for which MIS be installed first.
 - (iii) Due to varied objectives concerned, the approach adopted by experts for designing and implementing MIS is a non-standardised one. Though in this regard nothing can be done at the initial stage but by and by standardisation may be arrived at for the organisation in the same industry.
 - (iv) Non-availability of cooperation from staff in fact is a crucial problem. It should be handled tactfully. This problem may be solved by educating the staff. This task should be carried out by organising lectures, showing films and also explaining to them the utility of the systems. Besides this, some persons should also be involved in the development and implementation of the system.
 - (v) 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 linking managers etc. Turnover of experts can be reduced by creating better working conditions and paying at least at par with other similar concerns.
 - (vi) Difficulty in quantifying the benefits of MIS, so that it can be easily comparable with cost. This raises questions by departmental managers about the utility of MIS. They forget that MIS is a tool, which is essential to fight out competition and the state of uncertainty that surrounds business today.
- 3. Limitations of the Management Information Systems:
 - (i) MIS is not a substitute for effective management. It cannot replace managerial judgement in making decisions in different functional areas.
 - (ii) MIS may not have requisite flexibility to quickly update itself with changing needs of time.
 - (iii) MIS cannot provide tailor-made information packages suitable for the purpose of every type of decision made by executives.

- (iv) MIS takes into account mainly quantitative factors, thus it ignores the non-quantitative factors like morale and attitude of members of the organization.
- (v) MIS is less useful for making non-programmed decisions.
- (vi) The effectiveness of MIS decreases due to frequent changes in top management, organizational structure and operational team.
- (vii) MIS effectiveness is reduced where culture of hoarding information and not sharing it with others exists.

The quality of the outputs of MIS is basically governed by the quality of input and processes.

4. Financial Information Systems play an important role in making following financial decisions:

- (i) Estimation of requirements of funds: This is the very important and starting point of making financial decisions. A very careful estimation of funds and the time at which these funds are required is made in this stage. This can be done by forecasting all physical activities of the firm and translating them into monetary units.
- (ii) Capital structure decisions: Decisions are to be taken to select an optimum mix of different sources of capital structure. There are many options available for procuring funds. Decision maker has to decide the ratio between debt and equity, long-term and short-term funds etc. He has to ensure that overall capital structure is such that the company is able to procure funds at optimum cost.
- (iii) Capital budgeting decisions: Funds procured from various sources are required to be invested in different assets. With the help of capital budgeting, decision maker can determine feasibility of investment in long-term assets. This will help in attainment of financial objectives.
- (iv) Profit Planning: This part of profit planning is essential for the growth of the organization. The decision maker has to make decision regarding profits and dividends. He has to ensure adequate surplus in future for growth and distribution of dividends.
- (v) Tax Management: Tax planning is aimed at reducing of outflow of cash resources by way of taxes so that the same may be effectively utilized for the benefit of business. The purpose of tax planning is to take full advantage of exemptions, deductions, concessions, rebates, allowances and other relief.
- (vi) Working Capital Management: Working capital management is concerned with the investment of long-term funds into current assets. Decisions are to be taken for effective financing of current assets required for day-to-day running of the organization.
- (vii) Current Assets Management: Policy decisions are taken regarding various items of current assets. Credit policy determines the amount of sundry debtors at any

point of time. Inventory policy is to be determined jointly between finance and production department.

5. (a) Personnel Information System: The Personnel Information System (PIS) deals with the flow of information about people working in the organization as well as future personnel needs. This information system will furnish information concerning skills required by the organization and skill which are available or existing. The personnel information system consists of five sub-systems.
 - (i) Recruitment: This deals with forecasting personnel needs, skills required and recruiting the personnel at appropriate time to meet the organization needs. This sub-system also deals with job specification and other personnel data.
 - (ii) Placement: This sub-system deals with the matching of available personnel with the requirements. This sub-system will use management service as its tool to identify talent in the organization and provides suitable placements.
 - (iii) Training and Development: With changes taking place inside and outside the organization, there is every need to update and improve the skills of personnel within the organization. This sub-systems takes up the task of enhancing the appropriate skill of its personnel depending upon the needs of the organization.
 - (iv) Compensation and Remunerations: Pay and other allowances and benefits are given based on government policies, recruitments, market condition and depending upon the strength of the organization. The information included in the system is largely associated with the traditional payroll and other financial records.
 - (v) Maintenance: This sub-system is designed to ensure that proper personnel policies and procedures are achieved. It may be extended to the operation of systems control, work standards and to measure the performance against financial plans.
- (b) Threats to operating systems integrity: Operating system control objectives are sometimes not achieved because of flaws in the operating system that are exploited either accidentally or intentionally.

Accidental threats include hardware failures that cause the 'operating systems to crash. Operating system failures are also caused by errors in user application programs that the operating systems cannot interpret. Accidental system failures may cause whole segments of memory to be "dumped" to disks and printers, resulting in the unintentional disclosure of confidential information.

Intentions threats to the operating system are most commonly attempts to illegally access data or violate user privacy for financial gain. However, a growing form of threat is from destructive programs from which there is no apparent gain. These exposures come from three sources:

1. Privileged personnel who abuse their authority. Systems administrators and

systems programmers require unlimited access to the operating system to perform maintenance and to recover from system failures. Such individuals may use this authority to access users' programs and data files.

2. Individuals, both internal and external to the organization, who browse the operating system to identify and exploit security flaws.
3. An individual who intentionally (or accidentally) inserts a computer virus or other form of destructive program into the operating system.

6. **Materials Requirements Planning (MRP):**

It is eye-opening to note that a major cause of production inefficiency is a lack of integrated production planning, production scheduling, and production control information systems. One approach to improve production efficiency is materials requirement planning (MRP). MRP integrates several production related information system so that MRP system can access and extract data from these systems to accomplish production scheduling. MRP's purpose is to greatly improve both inventory management and production scheduling.

To achieve the efficiencies of which they are capable, MRP systems require high levels of discipline – such as not requisitioning materials long before they are needed, proper scrap reporting and using well-defined procedures for implementing and recording changes promptly. Accurate input data also is absolutely necessary, for example inventory quantity data must be accurate and interplant transfers must be recorded accurately and promptly.

The benefits of MRP systems are:

- (i) Significantly decreased inventory levels and corresponding decrease in inventory carrying costs.
 - (ii) Fewer stock shortage, which cause production interruption and time-consuming schedule juggling by managers.
 - (iii) Increased effectiveness of production supervisors and less production chaos.
 - (iv) Better customer service – an increased ability to meet delivery schedules and to set delivery dates earlier and more reliably.
 - (v) Greater responsiveness to change.
 - (vi) Closer coordination of the marketing, engineering and finance activities with the manufacturing activities.
7. An Executive Information System (EIS) is a tool that provides direct online access to relevant information in useful and navigable format. Relevant information is timely, accurate, and actionable information about aspects of a business that are of particular interest to the senior manager. The useful and navigable format of the system means that it is specifically designed to be used by individuals with limited time, limited key boarding skills and little direct experience with computers. An EIS is quite easy to navigate so that managers can identify broad strategic issues and

then explore the information to find the root causes of those issues. Executive information systems can be used for wide range of applications. In government, EIS have been constructed to track data about ministerial correspondences, case management, workers productivity, finances and human resources etc. EIS have also been used to monitor information about competitors in the news media and data bases of public information etc.

EIS requires large amounts of capacity and processing power within both the system and the network since information is in summary format by pictorial or graphical means. However, EIS has the facility to “drill down” to other levels of information to see the details. The ability to manipulate data, to project “what if” outcomes and to work with modeling tools within the system are also evident in EIS.

Purposes of EIS:

- (i) The primary purpose of an EIS is to support managerial learning about an organization, its work processes and its interaction with the external environment. Informed managers can ask better questions and make better decisions.
 - (ii) Second purpose for an EIS is to allow timely access to information. All of the information contained in an EIS can typically be obtained by a manager through traditional methods. However, the resources and time required to manually compile information in a wide variety of formats and in response to ever changing requirements often inhibit managers from obtaining this information. Often, by the time a useful report can be compiled, the strategic issues facing the manager change, and the report cannot be used. Timely access also influences learning. When a manager obtains the answers to a question, that answer typically sparks other related questions in the manager's mind. This way learning cycle continues unbroken.
 - (iii) Third purpose of an EIS is commonly misperceived. An EIS has a powerful ability to direct management attention to specific areas of the organization or specific business problems. Some managers look upon this as an opportunity to discipline subordinates.
 - (iv) Sometimes misaligned reporting systems can result in inordinate management attention to things that are not so important. An EIS system can provide information that is actually important and represents a balanced view of the organization's objectives.
8. (a) Client / Server (C/S) 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 databases – oriented C/S technology, as well as more recent general distributed computing technologies.

Components of Client Server Architecture:

Client: Clients, which are typically PCS, are the “users” of the services offered by the servers. There are basically three types of clients:

- ◆ Non-graphical User Interface (NGUI)
- ◆ GUI – clients
- ◆ Objects – Oriented User Interface (OOUI)

Server: Servers await requests from the clients and regulate access to shared resources. File servers make it possible to share files across a network by maintaining a shared library of documents, data and images.

Middleware: The network systems implemented within the client / server technology is commonly called by the computer industry as middleware. Middleware is all the distributed software needed to allow clients and servers to interact.

Network: The network hardware is the cabling, the communication cords, and the devices that link the servers and the clients. The communication and data flow over the network is managed and maintained by network software.

- (b) Client / Server is described as a ‘Cost-reduction’ technology. This technology allows doing what one may be currently doing with computers much less expensively. These technologies include client / server computing, open systems, fourth generation languages, and relational databases. Cost reductions are usually quoted as the chief reasons for changing to client / server.

Benefits of the client / server technology:

- ◆ Users are more productive today because they have easy access to data and because applications can be divided among many different users so efficiency is at its highest.
- ◆ Client / Server applications make organisations more effective by allowing them to develop applications simply and efficiently.
- ◆ Reduce the cost of the client's computer, the server stores data for the clients rather than clients needing large amounts of disk space. Therefore, the less expensive network computers can be used instead.
- ◆ Reduce the cost of purchasing, installing and upgrading software programs and applications on each client's machine: delivery and maintenance would be from one central point, the server.
- ◆ The management control over the organization would be increased.
- ◆ Many times easier to implement Client / Server than change a legacy application.

- ◆ Leads to new technology and the move to rapid application development such as object oriented technology.
 - ◆ Long term cost benefits for development and support.
 - ◆ Easy to add new hardware to support new systems such as document imaging and video teleconferencing which would not be feasible or cost efficient in a mainframe environment.
 - ◆ Can implement multiple vendor software tools for each application.
9. (a) 2-tier refers to fat clients and 3-tier refers to fat servers in a Client / Server architecture. Fat client and fat-server serve as vivid descriptions of the type of Client / Server systems in place. In a fat client systems, more of the processing takes place on the client, like with a file server or database server. Fat-servers place more emphasis on the server and try to minimize the processing done by the clients. Examples of fat-servers are transaction, groupware and the web-servers.
- (b) To increase the security for client / server technology, an IS auditor should ensure that the following control techniques are in place:
- ◆ Access to data and application is secured by disabling the floppy disk drive.
 - ◆ Diskless workstation prevents unauthorized access.
 - ◆ Unauthorised users may be prevented from overriding login scripts and access by securing automatic boot or start up batch files.
 - ◆ Network monitoring can be done to know about the client so that it will be helpful for later investigation, if it is monitored properly. Various network-monitoring devices are used for this purposes. Since this is a detective control technique, the network administrator must continuously monitor the activities and maintain the devices, otherwise these tools becomes useless.
 - ◆ Data encryption techniques are used to protect data from unauthorized access.
 - ◆ Authentication systems can be provided to a client, so that they can enter into system, only by entering login name and password.
 - ◆ Smart cards can be used. It uses intelligent hand-held devices and encryption techniques to decipher random codes provided by client-server based operating systems. A smart card displays a temporary password based on an algorithm and must be re-entered by the user during the login session for access onto the client-server system.
 - ◆ Application controls may be used and users will be limited to access only those functions in the systems that are required to perform their duties.
10. (a) There are many reasons why organisations fail to achieve their systems development objectives. Some of these are discussed below:
- (i) Lack of senior management support for and involvement in information systems developments: Developers and users of information systems will

watch senior management to determine which systems development projects are important and will act accordingly by shifting their efforts away from any project not receiving management attention.

In addition, management can see that adequate resources, as well as budgetary control over use of those resources, are dedicated to the project.

- (ii) Shifting user needs: User requirements for information technology are constantly changing. As these changes accelerate, there will be more requests for systems development and more development projects. When these changes occur during development process, the development teams may be faced with the challenge of developing systems whose very purpose have changed since the development process began.
- (iii) Development of strategic systems: Because strategic decision making is unstructured, the requirements, specifications and objectives for such development projects are difficult to define; and determining "successful" development will be elusive.
- (iv) New technologies: When an organization tries to create a competitive advantage by applying advanced information technology, it generally finds that attaining systems development objectives is more difficult because personnel are not so familiar with the technology.
- (v) Lack of standard project management and systems development methodologies: Some organisations do not formalize their project management and systems development methodologies, thereby making it very difficult to consistently complete projects on time or within budgets.
- (vi) Overworked or under-trained development staff: In addition to being overworked, systems developers often lack sufficient education background. Furthermore, many companies do little to help their development personnel stay technically updated; in these organisations, a training plan and training budget do not exist.
- (vii) Resistance to change: People have a natural tendency to resist change and information systems development projects signal changes often radical in the workplace. Business process reengineering is often the catalyst for the system's development project. When personnel perceive that the project will result in personnel cutbacks, threatened personnel will dig in their heels, and the development project is doomed to failure. Personnel cutbacks often result when reengineering projects really attempt at downsizing.
- (viii) Lack of user participation: Users must participate in the development effort to define their requirements, feel ownership for project success, and work to resolve development problems. User participation also helps to reduce user resistance to change.

- (ix) Inadequate testing and user training: New systems must be tested before installation to determine that they will operate correctly. Users must be given training to effectively utilize the new systems.
- (b) Design is concerned with translating systems requirements into ways of meeting these requirements. Logical design is the blueprint containing all the detailed specifications of the new systems to meet system requirements. It contains the features of the new system, its outputs, inputs, files and databases and procedures.

In contrast, physical design is the activity that follows logical design. It involves programmers who translate the design specifications formulated by analysts in the logical design phase into program software, files and a working systems.

Analysts are responsible for the following:

- (i) To translate requirements data into detailed specifications (the means of meeting what the new or modified system must do). This activity should include output and input design.
- (ii) To act as a liaison (to clarify what the specific actions are) between the logical design phase and the programmers involved in the physical design phase.

Programmer are responsible for translating the specifications produced in the logical design phase into program software, files and databases and a working system.

Users are responsible for providing essential feedback to analysts, including that obtained from reviewing mock-up reports, input formats, systems procedures and system controls. Users involvement not only paves the way for a smoother introduction of the new system, but also acquaints the user with the capabilities and limitations of the new systems.

11. (a) Data Dictionary: It is a computer file that contains descriptive information about the data items in the files of a business information system. In other words, it is a computer file about data. The information included in each record of a Data Dictionary may include the following about an item.
 - (i) Codes describing the data item's length, data type and range.
 - (ii) Identity of the source documents used to create the data.
 - (iii) Names of the computer files storing the data item.
 - (iv) Identify of individuals / programs permitted to access the data item for the purpose of file maintenance, upkeep or inquiry.
 - (v) Identify of programs / individuals not permitted to access the data item.
 - (vi) Names of the computer programs that modify the data items.

It has variety of uses. It serves as an aid to documentation and is also useful for securities. It helps accountants and auditors in establishing audit trails and

in planning the flow of transaction data through the system. Finally, it serves as an important aid in investigating or documenting internal control procedures.

- (b) **System Development Life Cycle:** The process of system development starts when management realizes that a particular business needs improvement. The system development life cycle method can be thought of as a set of activities that analysts, designers and users carry out to develop and implement an information system.

The system development life cycle method consists of the following activities:

- (i) **Preliminary investigation:** It is undertaken when users come across a problem or opportunity and submit a formal request for a new system for the MIS department. This activity consists of three parts: request clarification, feasibility study and request approval.
- (ii) **Requirements analysis or system analysis:** In this stage, the analysts work closely with employees and managers of the organization for determining the information requirements of the users. Several fact-finding techniques and tools such as questionnaire, interviews, observing decision-maker behaviour and office environment etc., are used for understanding the requirements of the users. As details are gathered, the analysts study the present systems to identify its problems and shortcomings and identify the features which the new system should include to satisfy the new or changed user application environment.
- (iii) **Design of the system:** It produces the details that state how a system will meet the requirements identified in the previous step. The analyst designs various reports / outputs, data entry procedures, input files and database. He also selects file structures and data storage devices. These detailed design specifications are then passed on to the programming staff for software development.
- (iv) **Acquisition and development of software:** In this stage, resource requirements such as specific type of hardware, software and services are determined. Subsequently, choices are made regarding which products to buy or lease from which vendors. Software developers may modify and then install purchased software or they may write new custom designed programs.
- (v) **System testing:** Before the information system can be used, it must be tested. Special test data are input for processing, and results are examined. If it is found satisfactory, it is eventually tested with actual data from the current system.
- (vi) **Implementation and maintenance:** After system is found to be fit, it is implemented with actual data. After implementation, the system is maintained, it is modified to adapt to changing users and business needs.

12. Fact Finding Techniques: Various fact-finding techniques which are used by the system analyst for determining users' needs are discussed below:

- (i) Documents: Document means manuals, input forms, output forms, diagrams of how the current system works, organization charts showing hierarchy of users and managers responsibilities, job descriptions for the people who work with the current systems, procedure manuals, program codes for the applications associated with the current system etc. Documents are a very good source of information about user needs and the current systems. They are easy to collect, convey a lot of information and provide relatively objective data. The analyst should ensure that the documents which he is collecting are current, accurate and contain up-to-date information.
- (ii) Questionnaires: Users and managers are asked to complete questionnaire about the information system when the traditional systems development approach is chosen. The main strength of questionnaires is that a large amount of data can be collected through a variety of users quickly. Also, if the questionnaire is skillfully drafted, responses can be analysed rapidly with the help of a computer.
- (iii) Interviews: Users and managers may also be interviewed to extract information in depth. The data gathered through interviews often provide system developer with a complete picture of the problems and opportunities. Interviews also give analyst the opportunity to note user reaction first-hand and to probe for further information.
- (iv) Observation: In prototyping approach, observation plays a central role in requirement analysis. Only by observing how users react to prototype of a new system, the system can be successfully developed. In traditional approach, the analyst should visit the user site to watch how the work was taking place. Such a surprise visit often helps the analyst in getting a clean picture of the user's environment and to determine why a request for a new system was submitted.

13. The commonly used coding schemes for data processing are briefly discussed below:

- (1) Classification Codes: Classification codes place separate entities, such as events, people, or objects into distinct groups called classes. A code is used to distinguish one class from another. The code is recorded on the source document by the user. In an online system, it can be keyed directly into the system through a terminal. The user classifies the event into one of the several possible categories and records the code.

For example, on a toll bridge, the number of each type of vehicles traveling on the bridge is counted to monitor its use. Toll charges are based on the type of vehicle. Since many types of vehicles travel the bridge, using common attributes of size, weight and the state to which it belongs would make its description difficult. Therefore, classification codes are established to group the vehicles in various classes. For example, a passenger car traveling the bridge is

categorized as class 1 vehicle and charged the lowest rate. However, a passenger car traveling a two-wheeler trailer is coded as class 2 and the one having a four-wheeler trailer is classified as class 3.

Classification codes vastly simplify the input process because only a single digit code is required. The need for writing lengthy descriptions or making judgements is eliminated and hence the process is made simpler.

- (2) **Function Codes:** Function Codes state the activities or work to be performed without spelling out all of the details in narrative statements. Analysts use this type of code frequently. The figure below shows a list of function codes for updating inventory. Data required for input vary depending on what function is needed. For example, appending or updating a record in a transaction processing system would require only the identification key of the record and the function code. On the other hand, adding a new record would require all data elements to be input, including the function code.

Code	Function
1	Delivered
2	Sold
3	Spoiled
4	Lost or stolen
5	Returned
6	Transferred out
7	Transferred in
8	Journal entry (add)
9	Journal entry (subtract)

- (3) **Significant-digit Subset Codes:** A well-conceived coding scheme, using significant-digit subset codes, can provide a wealth of information to users and management. Suppose item numbers are to be assigned to the different materials and products that a firm stocks or sells. One way to accomplish this is to assign numbers in sequence, starting with the first and going through to the last. Or a prefix can be added to the identification numbers to further describe the type of item: steel has an S-prefix, plastic a P, and so on.

Codes can be divided into subsets or sub-codes, characters that are part of the identification number and that have special meaning. The sub-codes give the user additional information about the item. In the inventory example, the most important information is the class of product, the item within that class, and the supplier. Therefore, the analyst develops an identification number carrying this information through significant digits in several subsets of the overall item.

123	456	78
Product class	Item number	Vendor number

If management wants to know how sales are in the waterwheel line, #323, the data can be sorted on that subset and a report produced. Similarly, if information is wanted about all products supplied by vendor 28, a quick examination of this subset of products will provide the information.

Using digits in an identification number to convey additional information does not add to the length of the data or, to processing time. However, the extra information sub-codes provide can be invaluable to management.

- (4) Mnemonic codes: These are suitable where the codes have to be remembered by people e.g. BL may stand for bolts. Universities frequently use mnemonics to code information. MBA for Master of Business Administrator or CS for Computer science. Mnemonic coding is particularly suited to tool stores since tools can be divided into four categories and each category may be assigned a mnemonic code e.g.

DR for drills

SW for saw blades

GR for grinding wheels etc.

The prefix (e.g. DR) may be followed by size e.g. 0.2 meaning 2 centimeter drill.

14. (a) Application software: Application software is aimed at a solution to a particular problem of the user of a computer system. It has direct interface with the computer system and provides standard processing utilities to solve the specific application problems of the user. For example, number of application software exists in the area of accounting and financial management.

Application software can be sub-divided into two categories viz., general purpose and application-specific. General purpose application software are programs that perform common information processing jobs for end users such as word processing programs, spread sheet programs and database management programs etc. Application specific programs support specific applications of end users e.g. accounting package, inventory control, scientific analysis, computer assisted instruction programs in education etc.

- (b) Factors affecting the “make or buy” decision of application software are as follows:
- ◆ Availability of skilled manpower: If sufficient number of programmers are not available, the organization may be forced to purchase packages that it otherwise would develop.
 - ◆ Cost of programming: In case the cost of developing the software is more than the price of pre-written software, the organization may decide to buy the software.

- ◆ Backlog of program: The in-house software development takes long time. If there is lot of backlog of programs awaiting development, the organization may choose to buy the software.
 - ◆ Suitability of software: Sometimes the available software may not be suitable for specific needs of the organization. Hence, it may be better to develop software in such instances.
 - ◆ Time frame available for implementation: If the time available for implementation of the new computerized system is very short, the organization may decide to buy the software.
 - ◆ Availability of sophisticated software: In many instances, the programs available for purchase are more sophisticated than the organization would probably develop. For example, many of the applications programs are fully integrated with other application programs. This integration is a powerful incentive for purchasing rather than developing programs.
- (c) Before purchasing the packaged software, the following features of the software should be assessed:
- (a) Is the package really available, or is it just another example of vaporware product announced well in advance of the time when it will be actually ready for use?
 - (b) Is the output produced by the package suitable in form and content to the user?
 - (c) Can the package accept the input data that the user needs to process in the form that he needs to use?
 - (d) Does the package support an acceptable range of I/O devices?
 - (e) Are the files created and / or processed by the software acceptable in terms of such contents, storage media, record format, access restrictions, etc?
 - (f) Does the package have an adequate response time, or the user must wait for lengthy periods while the program processes the last data entry?
 - (g) Is the package "user friendly" – is it easy to learn and use?
 - (h) What is the quality of the documentation? Are the manuals and other documents in the package complete, clearly written and well organized?
 - (i) Does the package have good error – handling controls? Are system errors reported to the users in clear messages or cryptic codes?
 - (j) What is the warranty period for the package? What is the level of support users are expected to receive from the vendor?
 - (k) Does the package represent a good value for money? Can an attractive, acceptable package be obtained for a significantly lower outlay?

15. Five programs design tools are briefly discussed below:

- (1) **Program flow chart:** Program flow chart is among the most common program design tools that managers and users encounter when reviewing the design work of the system development project. These flow charts depict the logical steps through which a computer program must proceed when solving a problem. At one time, program flow charts were considered the premier program design tool. Although they are still widely used, sometimes it is difficult for programmers to translate a program flow chart directly into a structured code.

A program flow chart depicts the logical processing steps followed by a program quite well. However, unlike some of the other program design tools, they often do not provide a broad view of how the program is organized. However, they are useful for problems involving mathematical or scientific formulae.

- (2) **Pseudo Code:** When reviewing the work done by a program designer, users may also need to review narrative descriptions of a program logic. Pseudo code, like program flow charts, also represents program logic. However, instead of using graphical symbols and flow lines, pseudo code presents program logic in English-like statements. Pseudo code is generally preferred by programmers over flowcharts because it represents program code more closely. Many users also find pseudo code more understandable than program flow charts.

Pseudo code is used in a variety of ways. For examples, many fourth-generation language use pseudo code-like statements. Besides using pseudo code to design program code in a 3GL, it can be embedded into a completed 3GL program as non-executable 'comment' statements that serve as a documentation to indicate what the program is doing. Pseudo code is particularly useful when designing transaction processing and information retrieval programs.

- (3) **Structure Chart:** Another type of program design tool that a user may review is the program structure chart. Structure charts, which look similar to corporate organization charts, are useful for organizing problems. The structure chart organizes each of the program tasks into well-defined modules. The higher-level modules represent control portions of the program; the lowest level modules do the actual tasks of the program. Unlike either flow charts or pseudo code, the structure chart does not give any detail of the actual program logic and the order in which various tasks are executed. Instead they show how all the logical functions of the program fit together as a whole.
- (4) **4GL Tools:** The various tools described above were developed as manually applied methods for designing programs or systems. The main drawback of manually applied tools is that they take a lot of time to prepare. Also, when a program flow chart is prepared or a structure chart is drawn, the programmer is not sure if it is internally consistent. Fourth-generation languages provide a way out to remove these obstacles by automating many of these manual tasks by using 4GL tools. These tools ensure that the work done with them is consistent

with the other work performed by the system team. The automation of manual task and internal consistency checks are two reasons due to which productivity gains result from using 4GL tools.

- (5) Object oriented programming and design tools: These tools provide a means of enhancing programme productivity and of reducing the application backlogs common in many organisations. Object oriented software design results in a model that describes objects, classes and their relationships to one another. The object-oriented design is often taken from a data flow diagram (DFD). In fact, every input and output screen, every process and data store found in a fully decomposed DFD may be a candidate for an object in an object oriented design. There is a wide variety of object oriented development tool kits available in the market.

By adopting 4GL and object-oriented programming tools, the organisations can decrease their application development time substantially.

16. The eight core principles of information security are discussed below:

- (1) Accountability: Security of information requires timely apportionment of responsibility and accountability among data owners, process owners, technology providers and users. This accountability should be formalized and communicated. Issues relating to specification of ownership of data and information, identification of users and others who access the system, recording of activities and assignment of responsibility for maintenance of data and information etc. should be considered.
- (2) Awareness: In order to foster confidence in information, data owners, process owners, technology providers and users must be able to gain knowledge of the existence and general extent of the risks facing the organizations and its system and the organisation's security initiatives and requirements. Security measures are only effective if all involved are aware of their proper functioning and of the risks they address.
- (3) Multidisciplinary: Security covers technological, administrative organizational, operational and legal issues. Technical standards should be developed with and be enforced by codes of practice, audit, legislative, legal and regulatory requirements and awareness, education and training.
- (4) Cost effectiveness: Different levels and types of security may be required to address the risks to information. Security level and associated costs must be compatible with the value of the information. Following issues must be considered.
 - ◆ Value to and dependence of the organization on particular information assets.
 - ◆ Value of the data or information itself, based on a pre-defined level of confidentiality or sensitivity.

- ◆ Threats to the information, including the severity and probability of such threats.
 - ◆ Safeguards that will minimize or eliminate the threats, including the cost of implementing the safeguards.
 - ◆ Costs and benefits of incremental increases to the level of security.
 - ◆ Safeguards that will provide an optimum balance between the harm arising from a security breach and the costs associated with the safeguards.
 - ◆ Where available and appropriate, the benefit of adopting established minimum security safeguards as a cost-effective alternative in balancing costs and risks.
- (5) Integration: Measures, practices and procedures for security must be coordinated and integrated with each other and with other measures, practices and procedures of the organization, so as to create a coherent system of security. This requires that all levels of the information cycle are covered.
- (6) Reassessment: The security of information system should be reassessed periodically, as information systems and the requirements for their security vary over time.
- (7) Timeliness: Security procedures must provide for monitoring and timely response to real or attempted breaches in security in proportion with the risk.

Following issues must be considered:

- ◆ Instantaneous and irrevocable character of business transactions.
 - ◆ Volume of information generated from the increasingly inter connected and complex information systems.
 - ◆ Automated tools to support real-time and after-the-fact monitoring and
 - ◆ Expediency of escalating breaches to the appropriate decision making level.
- (8) Social factors: Information and the security of information should be provided and used in such a manner that the rights and interest of others are respected. Level of security must be consistent with the use and flow of information.
17. (a) Hash function means an algorithm mapping or translation of one sequence of bits into another, generally smaller set known as “hash result” such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its inputs making it computationally infeasible—
- (i) to derive or reconstruct the original electronic record from the hash result produced by the algorithm.
 - (ii) that two electronic records can produce the same hash result using the algorithm.

- (b) Authentication of electronic records using Digital Signature: Section 3 of Chapter II of Information Technology Act 2000 gives legal recognition to electronic records and digital signatures.

The section provides the conditions subjects to which an electronic record may be authenticated by means of affixing digital signature. The digital signature is created in two distinct steps. First the electronic record is converted into a message digest by using a mathematical function known as "hash function" which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tampering with the contents of the electronic record will immediately invalidate the digital signature. Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the public key corresponding to such private key. This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature.

18. Auditors involved in reviewing an information system should focus their concern on the system's control aspects. They must look at the total systems environment not just the computerized systems. This requires their involvement from the time that a transaction is initiated while it is posted to the organisation's general ledger. Specifically, auditors must ensure that provisions are made for:
- ◆ An adequate audit trail so that transactions can be traced forward and backward through the system.
 - ◆ Controls over the accounting for all data entered with the systems and controls to ensure the integrity of these transactions throughout the computerized segment of the system.
 - ◆ Handling exceptions to and rejections from the computer system.
 - ◆ Testing to determine whether the systems perform as stated.
 - ◆ Control over the changes to the computer system to determine whether the proper authorization has been given.
 - ◆ Authorisation procedures for system overrides.
 - ◆ Determining whether organization and government policies and procedures are adhered to in system implementation.
 - ◆ Training user personnel in the operation of the system.
 - ◆ Adequate controls between interconnected computer systems.
 - ◆ Adequate security procedures to protect the user's data.
 - ◆ Backup and recovery procedures for the operation of the system.
 - ◆ Technology provided by different vendors are compatible and controlled.

- ◆ Databases are adequately designed and controlled to ensure that common definitions of data are used throughout the organization.
- ◆ Developing detailed evaluation criteria so that it is possible to determine whether the implemented system has met predetermined specifications.

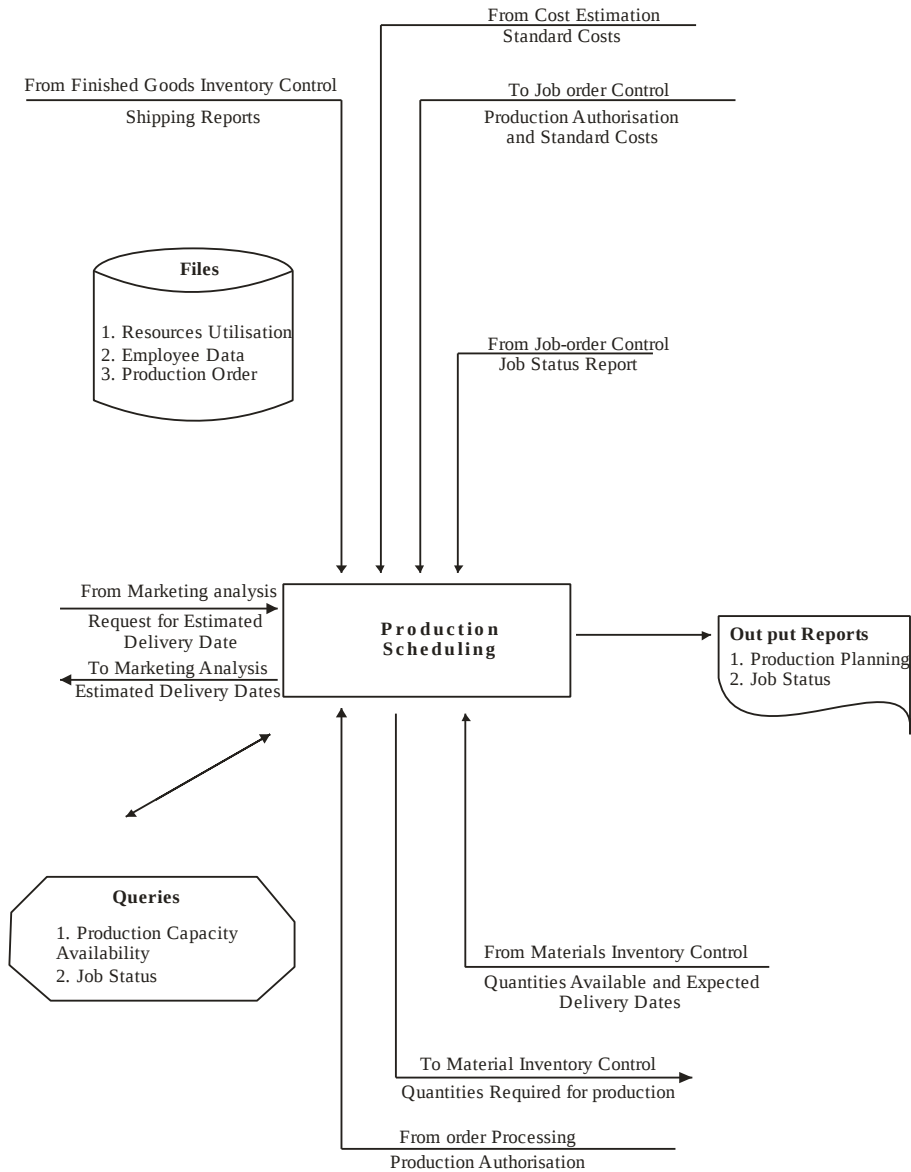
19. Production scheduling: It schedules production of components and monitors their progress throughout. It is nerve centre of the production management system. The information flow involving the production scheduling is given on the next page.

System Interfaces: The production scheduling system interacts with various other systems of the organization. The sales order processing system authorized production scheduling to start work on a job. Production scheduling then provides with estimated delivery dates and receives shipping reports from the finished goods inventory control system. Production scheduling informs material inventory control of the items and quantity required to schedule production and inventory control indicates the quantities available. Work in progress (WIP) control receives production authorization from the scheduling system. This authorization creates a new record for a job and production costs can be charged on the job. At the same time, the work-in-process control system receives the standard cost for the job and provides status reports to the scheduling system. Cost estimation provides production scheduling with budgeted standard costs for all jobs production.

Files and Inputs: Three files are required in the production scheduling systems. The resources utilization file contains a record for each machine and production process in the factory and maintains work schedules for them. The employee data file contains data concerning employee skills and scheduled work assignments. The production order file maintains completion date and schedule information for each job.

Reports: The scheduling system produces periodic production planning reports. They indicate the available capacity and scheduled future utilization of labour and machinery. Job status reports concern the status of jobs in the production process. They compare scheduled and actual completion time in the production process.

20. (a) There are quite a few ERP packages available in the market these days. Some of these are developed indigenously also. However, these indigenous packages may not be able to compete with the global ERP packages in terms of functionality and coverage of business segments and scale. Some of the global packages along with the vendors are listed below:
- ◆ Baan (The Baan Company): Initially developed for an aircraft company, it was subsequently launched as a generalised package in 1994. It offers sound technology and coverage of broad functional scope.
 - ◆ Business Planning and Control Systems (BPCS): It targets only manufacturing companies. It offers strong functionality for discrete and kanban manufacturing. However, it lags in process oriented implementation tools and workflow.



- ◆ Mapics XA (Marcam Corporation): It is viewed by many as a legacy application.
- ◆ MFG / Pro (QAD): Strong in repetitive manufacturing, originally designed to meet MRP II standards, it offers reliable manufacturing functionality and straight forward implementation.

- ◆ Oracle Applications (Oracle): It gives Internet – enabled, network – centric computing. It also offers database, tools, implementation, applications and UNIX operating systems under one stop-shop umbrella. It is currently running on wide choice of hardware.
 - ◆ R / 3 (SAP): It is a market leader with excellent philosophy of matching business processes with its modules. It covers almost all business segments.
 - ◆ Systems 21 (JBA): Its software license revenues are small compared to other major ERP vendors. It offers a rugged, reliable and manufacturing solution.
- (b) The benefits accruing to any business enterprise by implementing an ERP are unlimited. Following are some of the benefits achieved by implementing the ERP package:
- (i) gives accounts payable personnel increased control of invoicing and payment processing and thereby boosting their productivity and eliminating their reliance on computer personnel for these operations,
 - (ii) reduces paper documents by providing on-line formats for quickly entering and retrieving information,
 - (iii) improves timeliness of information by permitting posting daily instead of monthly,
 - (iv) greater accuracy of information with detailed content, better presentation, satisfactory for the auditors,
 - (v) improved cost control,
 - (vi) faster response and follow-up on customers,
 - (vii) more efficient cash collection, say, material reduction in delay in payments by customers,
 - (viii) better monitoring and quicker resolution of queries,
 - (ix) enables quick response to changes in business operations and market conditions,
 - (x) helps to achieve competitive advantages by improving its business process,
 - (xi) Improves supply-demand linkage with remote locations and branches in different countries,
 - (xii) provides a unified customer database usable by all applications,
 - (xiii) improves international operations by supporting a variety of tax structures, invoicing schemes, multiple currencies, multiple period accounting and languages,
 - (xiv) improves information access and management through the enterprise,
 - (xv) provides solution for problems like Y2K and single monetary unit or Euro currency.

21. (a) Security risk associated with personal computers are discussed below:
- (i) Personal computers are small in size and easy to connect and disconnect, they are likely to be shifted from one location to another or even taken outside the organization for theft, or for theft of information, leaving no trace.
 - (ii) Decentralised purchasing of PCs can result in hardware / software incompatibility in the long run. There is also the risk of multiple purchases of same hardware and software.
 - (iii) Floppies can be very conveniently transported from one place to another, as a result of which data corruption and theft of information may occur. Even hard disks can be ported easily these days.
 - (iv) PC is basically a single user oriented machine and hence, does not provide inherent data safeguards. Problems can be caused by computer viruses and pirated software, namely, data corruption, slow operations and system break down etc.
 - (v) Segregation of duty is not possible, owing to limited number of staff.
 - (vi) Due to vast number of installation, the staff mobility is higher and hence becomes a source of leakage of information.
 - (vii) The operating staff may not be adequately trained.
- (b) Personal computer controls: The capabilities, adaptability and user friendliness of personal computers are posing a serious challenge to auditors. PCs have the following special characteristics, which give rise to new risks that need to be controlled.
- ◆ They are small, fast and powerful, some of them even approach the power of minis and mainframes.
 - ◆ They are available in many makes and models.
 - ◆ Floppies provide a convenient way of data storage.
 - ◆ Their user-friendliness has resulted in end-user computing.
 - ◆ They act as inexpensive front-ends to large computers.
 - ◆ There is a tendency to buy off the shelf application packages.

Some other inherent problems of personal computers and the controls to be exercised are discussed below:

- (i) Weak Access Control: Security software that provides log-on procedures is available for PCs. Most of these programmes, however, become active only when the computer is booted from the hard drive. Disk locks are devices that prevent unauthorised individuals from accessing the floppy disk drive of a computer.

- (ii) Multi-level Password Control: To preserve the integrity of mission – critical data and programmes, organisations need formal back up procedures.
 - (iii) Floppy Disc Backup: Files can be backed up to floppy disks at routine periods during processing and stored away from the computer.
 - (iv) Dual Internal Hard Drives: PC can be configured with two physical internal hard drives. One disk can be used to store production data while the other stores the back-up file.
 - (v) External Hard Drive with removable disk cartridge can be used. This can provide an effective and simple back-up technique.
- (c) Firewalls: Organisations connected to the Internet or other public network often implement an electronic “firewall” to insulate their Intranet from outside intruders. A firewall is a system that enforces access control between two networks. To accomplish this, all traffic between the outside network and the organisation'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.

Firewall can be used to authenticate an outside user of the network, verify his or her level of access authority and then direct the user to the program, data, or service requested. In addition to insulating the organisation network from external networks, firewalls can also be used to insulate portions of the organisation's intranet from internal access. There are a number of firewall products on the market. Firewalls can be grouped into two general types: network-level firewalls and application-level firewalls.

Network-level firewalls provides low cost and low security access control. This type of firewall consists of screening router that examines the source and destination addresses that are attached to incoming message packets. The firewall accepts or denies access requests based on filtering rules that have been programmed into it.

Application-level firewalls provides a high level of customizable network security, but can be extremely expensive. These systems are configured to run security applications called proxies that permit routine services such as e-mail to pass through the firewall, but can perform sophisticated functions such as logging or user authentication for specific tasks. If an outside user attempts to connect to an unauthorized service or file, the network administrator or security group can be notified immediately.

22. (a) Disc Imaging and Analysis Technique: To reduce the risk to business from computer fraud, computer forensic tools can be used. Disk imaging and analysis technique is also one such tool. It enables the fraud investigator to discover evidence of transactions that the fraudster thought were inaccessible or had been destroyed. They can be used where evidence of the commission of a fraud may

have been retained in a computer. For example such evidence may be in the form of word processing documents showing the stages in creation of a forged invoice or a blackmail letter; or files which demonstrate that an employee has been sending confidential information by e-mail to a competitor or copies of passwords of other members of staff or users of other computers or pornographic material. This technique can equally well be applied to a network or any other storage medium.

This technique involves work carried out in following stages:

- (i) using special hardware and software to take an exact copy of the computer hard disk, leaving the original copy intact, and leaving no trace of the copying process.
 - (ii) The image copy of the disk is processed and areas of storage containing partially overwritten files and files which have been marked deleted but not overwritten are recovered.
 - (iii) The processed image is then analysed using search software to find references to suspected transactions.
- (b) The simplest and most common way to commit a fraud is to alter computer input. In collusive fraud, one perpetrator, for example, opened an account at a bank and then prepared blank deposit slip. The slips were similar to those available in bank lobby, with his account number encoded. One morning he replaced all the deposit slips in the bank lobby with his forged ones. For three days all bank deposits using the forged slips went directly into his account. Then he withdrew the money and disappeared.

In disbursement frauds, the perpetrator can cause a company to either pay too much for ordered goods or to pay for goods that are never ordered. He may keep the amount low enough so that most companies may not bother for purchase orders or approvals for such small amounts.

To commit payroll frauds, perpetrator can enter data to increase the salary, create a fictitious employee or retain a terminated employee on records and proceeds to intercept and cash the illegal cheques.

In a cash receipt fraud, the perpetrator may hide the theft by falsifying system input e.g. he may sell full-price tickets but enter the sale as half-price tickets and pocket the difference.

23. Digital signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure.

The digital signature is created in two distinct steps. First the electronic record is converted into a message digest by using a mathematical function known as "hash function" which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tempering of the contents of the electronic record will immediately invalidate the digital signature. Secondly, the identification of the person affixing the digital

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

Section 5 of the Chapter III provides for legal recognition of Digital signatures where any law requires that any information or document should be authenticated by affixing the signature of any person, then such a requirement can be satisfied if it is authenticated by means of digital signatures affixed in such manner as may be prescribed by the central government.

Duties of certifying authority:

1. According to Section 30 of the Information Technology Act, 2000, certifying authority shall follow certain procedures in respect of digital signatures as given below:
 - ◆ Make use of hardware, software and procedures that are secure from intrusion and misuse.
 - ◆ Provide a reasonable level of reliability in its services, which are reasonably suited to the performance of intended functions.
 - ◆ Adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured and
 - ◆ Observe such other standards, as specified by the regulation.
 2. Every certifying authority shall ensure that every person employed by him complies with the provisions of the Act, or rules, regulations or orders made thereunder.
 3. A certifying Authority must display its licence at a conspicuous place of the premises in which it carries on its business. A certifying authority whose licence is suspended or revoked shall immediately surrender the license to the controller.
 4. Every certifying authority shall display its digital signature certificate, which contains the public key corresponding to the private key used by that certifying authority and other relevant facts.
24. (a) While performing an IS audit, auditors should ascertain that the following objectives are met:
- (i) Security provisions protect computer equipments, programs, communications and data from unauthorized access, modifications or destruction.
 - (ii) Program development and acquisition is performed in accordance with management's general and specific authorization.

- (iii) Program modifications have the authorization and approval of the management.
 - (iv) Processing of transactions, files, reports and other computer records is accurate and complete.
 - (v) Source data that is inaccurate or improperly authorized is identified and handled according to prescribed managerial policies.
 - (vi) Computer data files are accurate, complete and confidential.
- (b) Comprehensive and systematic MIS auditing can help organisations to determine the effectiveness of the controls in their information systems. Regular data quality audits should be conducted to help organization ensure a high level of completeness and accuracy of the data stored in their systems. Data cleaning should also be performed to create consistent and accurate data for company wide use in e-commerce and e-business.

An MIS audit identifies all of the controls that govern individual information systems and assesses their effectiveness. To accomplish this, the auditors must acquire a thorough understanding of operations, physical facilities, telecommunications, control systems, data security objectives, organisations structure, manual procedures and individual applications.

The auditor usually interviews key individuals who use and operate specific information system concerning their activities and procedures. Application controls, overall integrity controls and control discipline are examined. The auditor should trace the flow of sample transactions through the system and perform tests using if appropriate, automated audit software.

The auditor lists and ranks all control weaknesses and estimates the probability of their occurrences. He then assesses the financial and organizational impact of each threat. Management is expected to device a plan for countering significant weaknesses in controls.

25. (a) Role of Information Security Administrator: An information security administrator is a person who is solely responsible for controlling and coordinating the activities pertaining to all security aspects of the organization.
- (i) A security administrator attempts to ensure that the facilities in which systems are developed, implemented, maintained and operations are safe from threats that affect the continuity of installation and or result in loss of security.
 - (ii) The security administrator sets policy, subject to board approval.
 - (iii) He also investigates, monitors, advises employees, counsels management on matters pertaining to security.
 - (iv) The security administrator is responsible for establishing the minimal fixed requirements for classification of information based on the physical, procedural and logical security elements. The need to protect these securities is also

stressed. He assigns responsibilities to job classification and formulates what is to be done in case of exceptions.

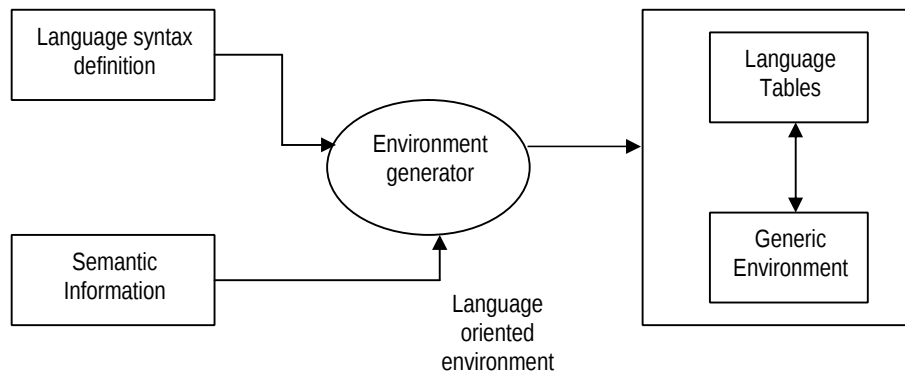
- (v) The security administrator guides other information security administrators and users on the selection and application of security measures. He trains them on how to mark and handle processes, train security coordinates, select software security packages and solve problems.
- (vi) Investigates all security violations.
- (vii) Advises senior management on matters of information resource control.
- (viii) Consults on matters of information security.
- (ix) He is responsible of conducting security program, which is a series of ongoing, regular periodic evaluations of the facilities available.
- (x) He has to consider an extensive list of possible threats to the organization. Also, he prepares an inventory of assets, evaluates the existing controls and implements new controls.

The information security administrator requires assistance from many experts in that particular field. He should see that whether these steps are performed on a regular basis. The results of the reviews are analysed and documented by him and he advises the management on appropriate action in the light of the result.

- (b) The following security management steps may be taken by an Internet user to protect from Cyber crimes and other computer security threats.
 - (i) Use antivirus and firewall software and update it often to keep destructive programmes off the computers.
 - (ii) Do not allow online merchants to store the credit card information for further purchases.
 - (iii) Use a hard-to-guess password that contains a mix of numbers and letters and change it frequently.
 - (iv) Use different passwords for different websites and applications to keep hackers guessing.
 - (v) Use the most up-to-date version of the web browser, e-mail software and other programmes.
 - (vi) Send credit card numbers only to secure sites; look for a padlock or key icon at the bottom of the browser.
 - (vii) Use a security programme that gives you control over “cookies” that send information back to website.
 - (viii) Install firewall software to screen traffic if you use digital subscriber line (DSL) or a cable modem to connect to the Internet.

- (ix) Do not open e-mail attachments unless you know that the source of the incoming message is trustworthy.
26. (a) Meta CASE work benches: Meta-CASE workbenches are CASE tools, which are used to generate other CASE tools. They are based on a description of the rules and notifications of design or analysis methods. The general principles will be based on the diagram given below:

Environment generator for Meta CASE tools



There are five different aspects, which are to be considered in Meta CASE workbench.

- (i) A data model for data capture and output generation.
 - (ii) A frame model, which defines the views of the data model to be generated. Each possible view of the data model is termed as frame. Links between frames, which allow navigation from one representation to another are defined in the model.
 - (iii) Diagrammatic notation for each diagram frame.
 - (iv) Textual presentation for each text frame.
 - (v) Report structures.
- (b) There are five different levels of integration of CASE tools as stated below:
- (i) Platform integration: Here the tools to be implemented run on the same platform where platform means either a single computer / operating system or a network of systems.
 - (ii) Data integration: It is the process of exchange of data by CASE tools. The result from one tool can be passed on as input to other tools.
 - (iii) Presentation integration: It means that the tools in the system use a common metaphor or style and a set of common standards for user interaction.

- (iv) Control Integration: It is the mechanism of one tool in a workbench or environment to control the activation of other tools in the CASE system.
- (v) Process integration: This means that the CASE system has embedded knowledge about the process activities, their phasing, their constraints and the tools needed to support their activities.

27. There are two major exposures in the communication sub-system including Internet and Intranet.

- ◆ Data may be lost or corrupted through component failure.
- ◆ An intruder may subvert data being transmitted through the sub-system.
- (i) Component failure: The primary components in the communication sub-systems are:
 - (a) Communication lines viz., twisted pair, coaxial cables, fiber optics, microwave and satellite etc.
 - (b) Hardware- ports, modems, multi-plexers, switches and concentrators etc.
 - (c) Software – Packet switching software, polling software, data compression software etc.

Due to component failure, transmission between sender and receiver can be disrupted, destroyed or corrupted in the communication system. There may be loss of databases and program stored on the network server due to equipment failure.

- (ii) Subversive threats: An intruder attempts to violate the integrity of some components in the sub-system.
 - (a) Invasive tap: By installing it on communication line, he can read and modify data.
 - (b) Inductive tap: It monitors electromagnetic transmissions and allows the data to be read only.

Subversive attacks can provide intruders with important information about messages being transmitted and the intruder can manipulate these messages in many ways.

Following mechanism can be used to control risks:

- (i) Firewall: Organisations connected to the Internet and Intranet often implement an electronic firewall to insulate their network from outside intruder. A firewall is a system that enforces access control between two networks. To accomplish this:
 - ◆ All traffic between the outside network and the organisations Internet must pass through the firewall.

- ◆ Only authorized traffic between the organization and the outside is allowed to pass through the firewall.
- ◆ The firewall must be immune to penetration from both outside and inside the organization.

In addition to insulating the organisation's network from external networks, firewalls can be used to insulate portions of the organisation's Intranet from internal access also.

- (ii) Controlling Denial of service attacks: When a user establishes a connection on the internet through TCP / IP, a three way handshake takes place between SYN packets to the receiver but never responds with an ACK to complete the connection. As a result, the ports of the receiver's server are clogged with incomplete communication requests and legitimate transactions are prevented from processing. Organisations under attack have been prevented from receiving internet messages for days in the past. If target organization could identify the server that is launching the attack, the firewall could be programmed to ignore all communication from that site.
- (iii) Encryption: Encryption is the conversion of data into a secret code for storage in databases and transmission over networks. The sender uses an encryption algorithm and the original message called the clear text is converted into cipher text. This is decoded at the receiving end. The encryption algorithm uses a key which is of 56 to 128 bits in length. The more bits in the key, the stronger is the encryption method. Two general approaches to encryption are use of private key and public key encryption.
- (iv) Message Transaction Log: An intruder may penetrate the system by trying different passwords and user ID combinations. All incoming and outgoing message along with attempted access should be recorded in a Message Transaction Log. The log should record the user ID, the time of the access and the terminal location and telephone number from which the request originated.
- (v) Call Back Devices: It is based on the principle that the key to network security is to keep the intruder off the LAN rather than imposing security measures after the criminal has connected to the LAN server. The call-back device requires the user to enter a password and then the system breaks the connection. If the caller is authorized, the call back device dials the caller's number to establish a new connection. This limits access only from authorized terminals or telephones numbers and prevents an intruder masquerading as a legitimate user.