

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

QUESTIONS

1. (a) What is Management Information System? With the help of a figure explain the functions of MIS of an organization.
(b) What are the characteristics of an effective MIS?
2. (a) Discuss the source and nature of accounting / financial information which a personnel department would require in an organization.
(b) What are the five characteristics of the types of information used in executive decision making.
3. How the systems approach to problem solving is applied?
Explain with the help of a flowchart how the system approach to problem solving is applied, by considering the problem of long delays between receipts of order and delivery in some hypothetical system.
4. (a) What is client server architecture? What are the characteristics of Client/Server technology?
(b) What are the risks involved in client /server model?
5. What are the control techniques ensured by an IS auditor for the security of the client/server environment ?
6. (a) Discuss the reasons as to why organizations fail to achieve their system development objectives.
(b) Describe in detail the steps involved in the selection of a computer system.
7. (a) Discuss the fourth viz. the system acquisition and development stage of system development life cycle in detail.
(b) Briefly discuss some of the program design tools which are commonly used.
(c) Why is personnel training important for the success of systems implementation? What type of training should be imparted to (i) system operators (ii) users.
8. (a) Give a detailed description on general controls of computer, highlighting personal computer controls ?
(b) What do you understand by the term “Disaster Recover Plan”? Discuss its various components.
9. (a) What are the fundamental control objectives an operating system must achieve to perform its tasks consistently and reliably ?
(b) What are the threats to operating system integrity ?
10. Draw the system flow chart for a materials inventory control system and explain the factors involved in its design.
11. What are the different types of securities required for the computer system? Explain briefly the different components of physical security of a computer installation.
12. (a) “Implementing an ERP system has more to do with changing the way an organization does business than it does with technology”. Give your comments on the given statement.
(b) What are the steps involved in the implementation of a typical ERP package ?
13. Discuss various issues that are of primary concern for an auditor involved in information system audit.

14. What kind of information is considered sensitive by a business organization? Discuss the factors that should be considered while deciding about the level of protection needed for information.
15. (a) Why is information security important?
(b) What is the role of security administrator?
16. (a) Describe the major techniques of Concurrent Audit of Information systems. Bring out the relevance of such Audit.
(b) What are the two major categories of exposures in the Communication subsystems including Internet and Intranet? What control mechanisms could be used to deal with them?
17. What is E-Governance? Discuss the different sections associated with this Chapter (i.e. Chapter III).
18. Write short-notes on the following:
 - (a) Strategic Decision Making
 - (b) Software Tools for Decision Support Systems
 - (c) Systems Design Phase
 - (d) Implementation Guidelines for ERP.
19. Write short-notes on the following:
 - (a) Middleware
 - (b) Torjon Horse
 - (c) 4GL Work benches
 - (d) Program maintenance

SUGGESTED HINTS / ANSWERS

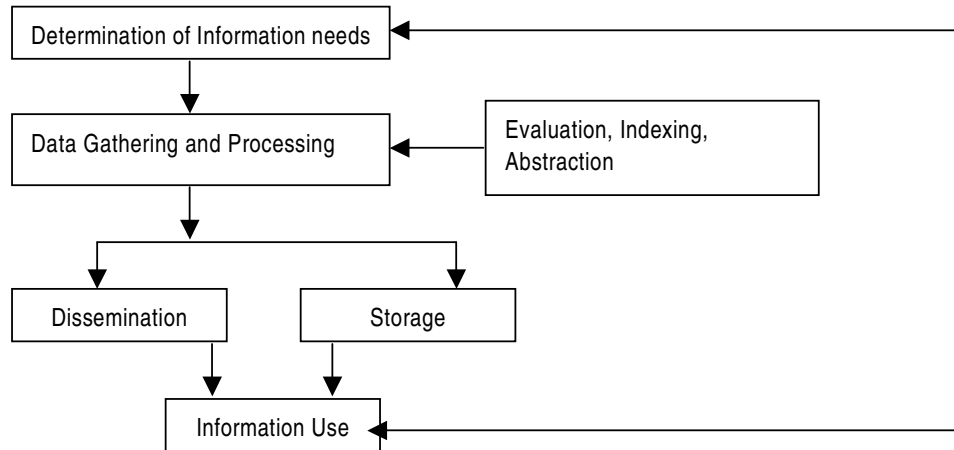
1. (a) Management Information System

Today Information is critical to the success of any business organization. Management Information System (MIS) is a computer based system which deals with the use, storage and retrieval of information in an organization.

MIS is a "system of people, equipment, procedures, documents and communication that collects, validates, and operates on transformers, stores, retrieves and present data for use in various management activities such as planning, budgeting, accounting, controlling and various other processes.

Management Information Systems (MIS) are information systems typically computer-based, that are used within an organization. An information system can be defined as "a system that collects and processes data (information) and provides it to managers at all levels who use it for decision making, planning, program implementation, and control." An information system is comprised of all the components that collect, manipulate, and disseminate data or information. It usually includes hardware, software, communications systems such as telephone lines, and the data itself. The activities involved include inputting data, processing of data into information, storage of data and information, and the production of outputs such as management reports.

The functions of MIS can be shown with the help of following diagram:



(b) Important characteristics of MIS:

1. **Management oriented:** The effort for the development and usage of information system should start from an appraisal of management needs and overall business objectives. It is not only for the top management, it meets the information needs of different levels of management in an organization.
2. **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 effectiveness. It is necessary for the management to devote their sufficient time not only at the stage of designing the system but for its review as well to ensure that the implemented system meets the specification of design system.
3. **Integrated:** 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 management.
4. **Common Data Flow:** It means the use of common input, processing and output procedures and media whenever possible is desirable. Data is captured by system analysts only once and as close to its original source as possible. Then they try to utilize 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.
5. **Heavy planning element:** An MIS usually takes 3 to 5 years and sometimes even longer to get established firmly within an organization. Therefore, a heavy planning element must be present in MIS development.
6. **Sub-System concept:** Even though the information system is viewed as a single entity, it must be broken down into digestible sub-systems which can be implemented one at a time by developing a phasing plan. The breaking down of MIS into meaningful sub-systems sets the stage for this phasing plan.
7. **Common Database:** Database is the mortar that holds the functional systems together. It is defined as the "superfile" which consolidates and integrates data records formerly stored in separate data files. The organization of the database allows it to be accessed by several information sub-systems and thus eliminates the necessity of duplication in data storage, updating, deletion and protection.
8. **Computerised:** It is possible to have MIS without using a computer. But use of computer increases the effectiveness of the system. In fact, its use equips the system to handle a wide variety of applications by providing their information requirements

quickly. Other necessary attributes of the computer to MIS are accuracy and consistency in processing data and reducing clerical staff.

2. (a) **Sources of Personnel Information:** Bulk of personnel information is generated by the accounting department and within the personnel department itself. Besides, the departments and the external environment also make their contribution. This information can be generated both internally and externally. Apart from internal generation, the external information sources for the personnel function would include: employment agencies, labour unions, various governmental agencies, university placement offices etc.

The Accounting Information System: Payroll processing is the traditional channel of personnel information. The human resource accounting, though hardly prevailing in the Indian industry, can be another new channel. Finally, cost estimation for wage negotiations is another information for the personnel function.

Payroll Processing: The inputs to payroll processing are the job tickets and the clock cards. The latter indicates the total number of hours an employee spends at work each day. This document serves as the basic input to the payroll calculation and pay slip preparation function. The job ticket is used to reconcile the timing on the clock card and to compute various job statistics discussed below. For payroll of clerical, salaried and sales employees, the job time card is not used as the related expenses are not charged to production in process. However, where it is desired to charge expenses to such specific project as sales promotion, a job time card may be used. For salaried employees, the monthly gross pay is a known constant and for salesmen paid on commission basis, sales data are required for payroll processing. Besides, such adjustments as additions, deletion, amendments etc. constitute another class of input data for payroll processing.

The basic output of payroll processing is pay slips and pay cheques. Reports of statistical nature are also compiled. Take a production operation for example. The average time spent by each employee on it may be computed and the grand average derived there from. This in comparison to the standard time derived by yields the efficiency with the operation is being performed. Likewise, the efficiency of an individual employee can be established. This would be a weighted average of his efficiency in all of the various operations he has performed. Such statistics when aggregated over a department provides the departmental efficiencies. These measures can be used to evaluate the performance of the departmental foreman. If a standard cost system is in use then labour cost variances can also be computed. Other types of possible reports and analysis are listed below:

- i. Reports on absenteeism
- ii. Analysis of indirect labour by the cost of inspection, material handling, maintenance etc.
- iii. Reports on actual standard costs by department.
- iv. Analysis of overtime pay by departments, fringe benefits, salesmen commission, etc.
- v. Such statistical measures as total number of employees, total hours worked, total labour cost, average wage rate, rate of absenteeism, turnover and total fringe benefit costs. These may be statistically analysed for trends and correlation etc.

Cost Estimating for Wage Negotiations: The management has the choice of trade-offs on the following variables during negotiations with the labour unions.

- Wage raise
- Paid holiday
- Contribution to employees, insurance and pension plan
- Overtime premiums etc.

Cost accountants/payroll accountants would be in the best position to make various estimates for the cost implications of trade-off.

The Personnel Department itself generates a great deal of information in the form of personnel files and job specifications. The former would include such data about each employee as below:

- Physical characteristics
- Educational background and experience
- Payroll information
- Quantitative and qualitative evaluations of his past performance
- State of health and medical history
- Result of tests of ability and aptitude, etc.

Such information is quite useful for placement of employees for various positions, promotions etc.

The job specifications detail of the training and experience for each job. Other information generated within the personnel department may include aggregate safety and accident statistics, forecasts of manpower requirements by job category within the organisation, records and statistics of training programmes, health services, etc.

The departmental supervisors provide useful information about their employees in their merit evaluations, as also information about manpower requirements of their departments. The merit evaluations would throw light on personality, initiative, attitude, judgement, character etc. of the employees.

- (b) Five characteristics of the types of information used in executive decision-making are lack of structure, high degree of uncertainty, future orientation, informal source and low level of detail.
- (i) **Lack of structure:** Many of the decisions made by executives are relatively unstructured. These types of decisions are not as clear-cut as deciding how to debug a computer program or how to deal with an overdue account balance. Also, it is not always obvious which data are required or how to weigh available data when reaching a decision.
 - (ii) **High degree of uncertainty:** Executives work in a decision space that is often characterized by a lack of precedent. Executives also work in a decision space where results are not scientifically predictable from actions.
 - (iii) **Future orientation:** Strategic-planning decisions are made in order to shape future events. As conditions change, organization must change also. It is the executives' responsibility to make sure that the organization keeps pointed toward the future.
 - (iv) **Informal source:** Executives, more than other types of managers, rely heavily on informal source for key information. Informal sources such as television might also feature news of momentous concern to the executive – news that he or she would probably never encounter in the company's database or in scheduled computer reports.
 - (v) **Low level of detail:** Most important executive decisions are made by observing broad trends. This requires the executive to be more aware of the large overview than the tiny items. Even so may executives insist that the answers to some questions can only be found by mucking through details.

3. Systems Approach to Problem Solving

To solve problems, managers must view the organization as a dynamic whole and they should anticipate the intended and unintended impacts of the decisions. By using system approach, management will understand that they do not solve individual problems. Rather, they intervene in a system of interrelated parts and the managerial functions. The procedure usually followed to solve problems by system approach can be outlined.

Let us consider the problem of long delays between receipts of order and delivery in some hypothetical company. To seek a solution for the problem by applying system approach, we should make use of the following six steps:

1. **Defining of the problem:** The problem involved here is of inordinate delay between receipts of order and the delivery. This problem affects the vendor in many ways, for example, bad reputation, loss of customers, reduction in profitability and even stoppage of due payments.
2. **Gathering and analyzing the data concerning the problem:** The problem of delay in meeting orders, in this case, say, arises due to following reasons:
 - a. Excessive orders in the hand of vendors.
 - b. Shortage of power (fall in production due to shortage of power).
3. **Identification of alternative solutions:** To overcome the stated problem by system approach, suppose the following two solutions exist:
 - a. Refusal of orders, in case the total size of the orders exceeds the plant capacity of one shift.
 - b. To run the plant in double shift to meet the commitment in time. Any short fall in power supply can be made by installing a generator.
4. **Evaluation of alternative solutions:** Out of the two identified solutions under the preceding step, the second solution say accounts for an overall increase for the profitability of the concern after offsetting additional cost for the generated produced power. It also helps in retaining customers and growth of the concern.
5. **Selection of the best alternative:** Under this step, management more closely examines the alternatives and puts its stamp on the best possible alternative.
6. **Implementation of the solution:** The implementation of the solution requires the necessary policy changes. Besides this, the resources required to run the plant in double shift and the installation of a generator also are to be arranged. Finally, appropriate procedures are developed to exercise smooth production and timely supply to customers; the concerned officers are accordingly instructed.

The **diagram on the next page** depicts the systems approach to problem solving for the given problem.

4. (a) **Client Server Architecture**

Client server refers to computing technologies in which the hardware and software components (i.e. Client and server) are distributed across a network. The Client /server software architecture is a versatile, message-based and modular infrastructure that is intended to improve usability, flexibility, interoperability and scalability as compared to centralized, mainframe, time sharing computing. This technology includes both the traditional database-oriented c/s technology, as well as more recent general distributed computing technologies.

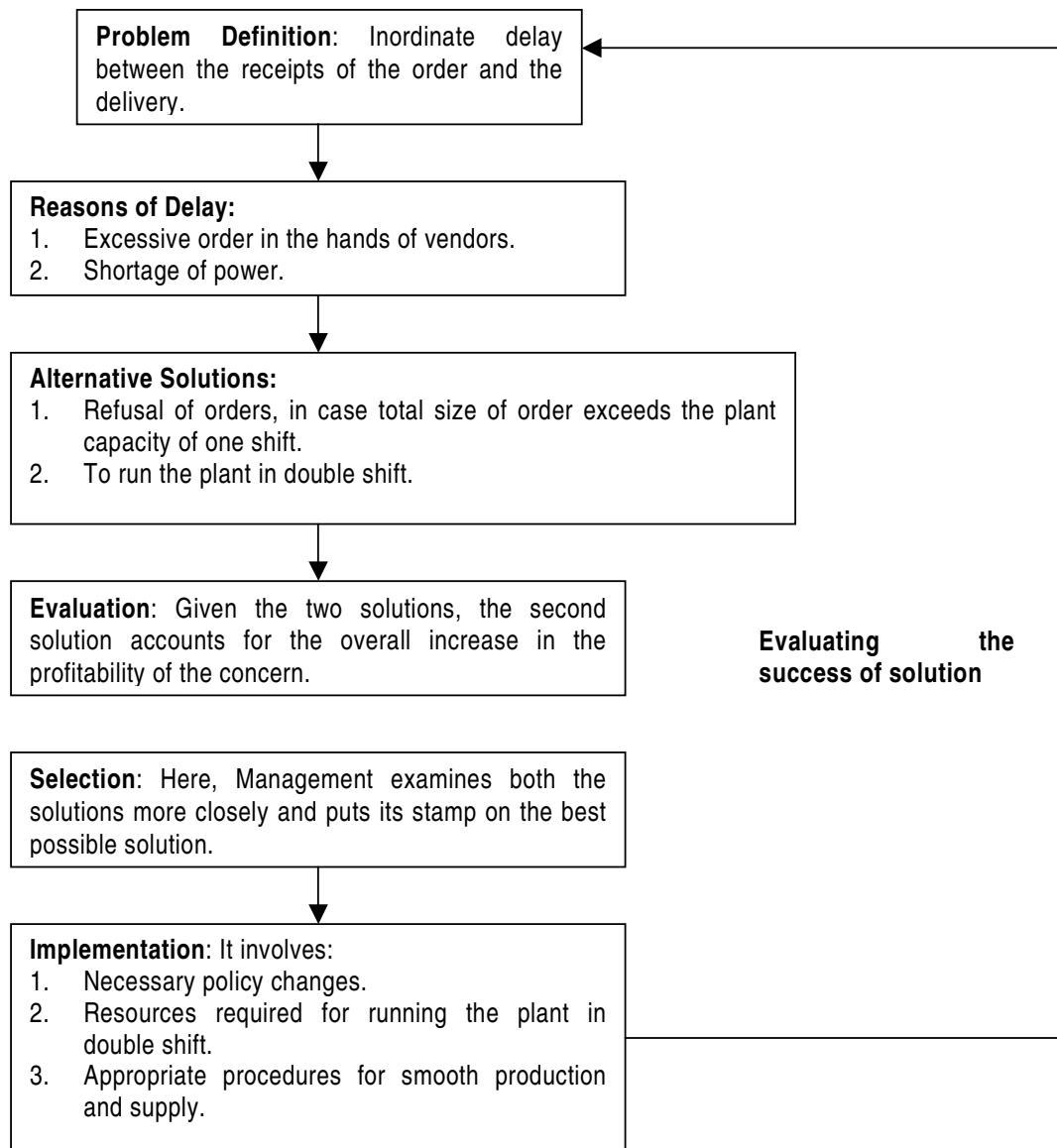
Properties of a server:

- Passive (Slave)
- Waiting for requests
- On requests serves them and send a reply

Properties of a client:

- Active (Master)
- Sending requests
- Waits until reply arrives

The use of LANs has made the client/server model even more attractive to organizations.



Characteristics of Client/Server Technology:-

There are ten characteristics that reflect the key features of client / server system. These ten characteristics are as follows:

1. Client/server architecture consists of a client process and a server process that can be distinguished from each other.
2. The client portion and the server portions can operate on separate computer platforms.
3. Either the client platform or the server platform can be upgraded without having to upgrade the other platform.
4. The server is able to service multiple clients concurrently: in some client/server systems, clients can access multiple servers.
5. The client/server system includes some sort of networking capability.
6. A significant portion of the application logic resides at the client end.

7. Action is usually initiated at the client end, not the server end.
8. A user-friendly graphical user interface (GUI) generally resides at the client end.
9. A structured query language (SQL) capability is characteristic of the majority of client/server systems.
10. The database server should provide data protection and security.

(b) Risks involved in client /server model?

The benefits of client/server are truly praiseworthy but there are also risks involved in the transition from mainframes to client/server model. They can be classified into the following four categories:

1. **Technological Risks:** The risks here are very simple. The questions that arise in one's mind are -- will the new system work? In the short term, will it really work? Will the system grow obsolete in the long run, if it will, how long will it run before it does. To resolve this issue, the IT consultant should understand the system standards and the market trends and use them in his decision making process while deciding what system to incorporate in the organization.
2. **Operational Risks:** These risks parallel the technological risks in both short and long term. Broadly, the two main issues here are: Will the performance be achieved from the new technology that is implemented and will the software be able to adapt to the growing needs of the business? Sound planning and keeping an eye on the future are the only remedies to avoid these risks.
3. **Economic Risks:** In the short run, organizations are susceptible to hidden costs associated with the initial implementation of the new client/server system along with maintaining the old mainframe system. Costs rise in the short term because of the development of the new system in parallel to the old existing system. In the long run, the costs incurred are mainly for the support of the new system.
4. **Political Risks:** Finally, political risks involved 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. The long run question concerns the costs.

If the mainframe is not completely replaced within the large organization then the total cost of transaction processing for the corporation goes up as one division of the organization might create its own independent system and move off the mainframe. They might have reduced their local cost of transaction processing but they would increase the cost of processing for divisions remaining on the mainframe and this creates political problems.

- a. There are many layers of complexity and compatibility issues between the client and the server.
 - b. Compatibilities of the software such as security and management tools are not as mature as their mainframe counterparts.
 - c. It takes time to become proficient with these tools.
 - d. Information system departments may balk at giving up control of a centralized computing environment.
5. To increase the security, an IS auditor should ensure that the following control techniques are in place:
- (i) Access to data and application is secured by disabling the floppy disk drive.
 - (ii) Diskless workstation prevents unauthorized access.
 - (iii) Unauthorised users may be prevented from overriding login scripts and access by securing automatic boot or startup batch files.

- (iv) Network monitoring can be done to know about the client so that it will be helpful for later investigation, if it is monitored properly.
 - (v) Data encryption techniques are used to protect data from unauthorized access.
 - (vi) Authentication systems can be provided to a client, so that they can enter into system only by entering login name and password.
 - (vii) Smart cards can be used. It uses intelligent hand held device and encryption techniques to decipher random codes provided by client-server based operating systems.
 - (viii) Application controls may be used and users will be limited to access only those functions in the system that are required to perform their duties.
6. (a) There are many reasons why organizations fail to achieve their systems development objectives:
- (i) **Lack of senior management support for and involvement in information systems development:** 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 challenges 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 organisation 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 as familiar with the technology.
 - (v) **Lack of standard project management and systems development methodologies:** Some organizations do not formalise their project management and systems development methodologies, thereby making it very difficult to consistently complete projects on time or within budget.
 - (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 organizations, 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 systems 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 system.
- (b) The selection of an appropriate computer system in terms of both hardware and application software package demands a high level of expertise and many organizations use a consultant either to provide guidance to their personnel or to manage this activity.

The steps involved in selection of a computer system are:

1. Prepare the design specifications.
2. Prepare and distribute an RFP (Request for proposal) to selected computer vendors.
3. On the basis of an analysis of proposals, eliminate vendors whose proposals are inferior.
4. Have vendors present their proposals.
5. Conduct further analysis of the proposals.
6. Contact present users of the proposed systems.
7. Conduct equipment benchmark tests.
8. Select the equipment.

During feasibility study, the EDP manager will list down various requirements of the organisation based on which design specifications of the computer will be laid down. These mandatory specifications would then constitute an over-riding criterion of selection. If a vendor fails to meet them, the manager would simply screen out that vendor without any further reconsideration. These specifications would establish a desired configuration that might include for example, the required minimum main memory size, the required characteristics of secondary memory, and general types and capacities of input and output equipments need etc. Usually, design specifications should be developed without reference to any specific models of equipment or to a particular vendors' product line.

After that, a RFP (request for proposal) is prepared by the organization and given to vendors, asking the vendor to prepare a bid and submit it to the organization. The RFP contains all details that are necessary for the vendor to prepare a fully detailed proposal. Typically, the RFP also contains a deadline for bidding, the length of which depends on the complexity of the project – for example, just a few weeks for hardware, and long periods of time for systems requiring custom development tasks. After responses to RFP have been received, they are evaluated by the organization. Meetings are scheduled with each vendor, whose bid is competitive in terms of price and meeting the requirements of the RFP. The participants at each meeting include representatives from the vendor, representatives from the steering committee, and representatives from the design team. The vendor's role is to present its proposal and to answer questions from the other participants. The evaluation committee's role is to listen to the vendor proposals, provide input to the steering committee about the pros and cons of each one, and perhaps make a recommendation for a preferred vendor.

Frequently, vendors who survive this presentation are nevertheless asked to revise their proposal in significant respects. The after presentation equipment analysis is carried out in even greater details, and it involves the proposals of only those vendors who remain in competition which may be only one or two. At this point, the organization should be satisfied that the systems still being considered can solve its problems in a cost effective manner. If this is not the case, the drastic steps of rewriting the design specifications and of submitting RFPs to other vendors must be considered.

7. (a) Systems Acquisition and Software development

Acquiring systems components from vendors: Acquiring the appropriate hardware and software is critical for the success of the whole project .After the management gives its consent to go ahead with the project , the acquisition process starts.

A. Procuring Computer Hardware:

The following points may be considered while selecting a computer system:

1. All computer system offered in the market today have good hardware, competent software and roughly similar facilities. Latest possible technology should be acquired.
2. Commercial data processing consists mainly of reading-in-data, printing out data and storing and retrieving information from magnetic media.
3. The selection of computer should be made on software consideration. Packages for commercial applications as inventory control and production planning are offered by all, some manufacturers also offer packages specially designed for a particular industry.
4. Modern computers are marketed as series of compatible machines with increasingly powerful central processors and interchangeable peripherals.
5. The selection of computers continues to the selection of a configuration and a plan for its gradual expansion.

B. Software Acquisition: Make or Buy

The nature of the application software requirement must be assessed by the systems analyst. This decision is often called the make-or-buy decision.

Advantages of Application Packages: The four advantages are as follows

1. Rapid implementation: Application packages are readily available.
2. Low risk: Application packages are available in finished form.
3. Quality: Specialist in their products niche area.
4. Cost: Application vendors can leverage the cost of developing a product by selling the product to several other firms .

C. Sources of Packaged Software: Thousands of programs are available in the market today for purchase. Computer manufacturers, large and small software houses and computer retail stores are some of the sources from where these packages can be purchased.

Buying packaged software is risky. Some are difficult to install .

Validation of the Vendors' Proposals:

The process consists of evaluating and ranking the proposals submitted by vendors and is quite difficult, expensive and time consuming , but in any case it has to be gone through.

The following factors have to be considered towards rigorous evaluation:

1. The Performance Capability of each proposed System in Relation to its Costs
2. The Costs and Benefits of Each Proposed System
3. The Maintainability of Each Proposed System
4. The Compatibility of Each Proposed system with Existing System
5. Vendor Support

Methods of validating the proposal: Mandatory requirements would constitute overriding criteria in that, if a vendor fails to meet them , he would be screened out without any further consideration .

The methods are

1. **Checklist:** It is the most simple and rather a subjective method for validation and evaluation.
2. **Point Scoring Analysis:** Another approach for evaluating those accounting packages .
3. **Public Evaluation Report:** Comparison of Hardware and Software performance for various manufactures.

Software Development: An In-House development of the software application is not an easy process. The system developer must instruct the computer to do step precisely without errors and in the correct sequence.

An In-House development involves following six stages :

- (a) **Program Analysis:** -Programmer ascertains all the requirements of an application, whether those are the output or input requirements. Then he ascertains whether the application should be programmed at all.
- (b) **Program Design:** In this stage he develops general organization of the program with the help of tools viz., flowcharts, input, output and file layouts.
- (c) **Program Coding:** The program outlined is converted into instructions at this stage. Specific rules according to the program are outlined. The programmers pursue three objectives i.e., simplicity, efficient storage and least processing time. After writing the source program, it is translated into machine language and compiled to find the program syntax errors.
- (d) **Debug:** Debugging follows after the program is compiled which is a tedious task. Compiler finds errors, the programmers then correct the lines of code and resubmit it to the compiler. The time for debugging can be shortened by the use of interactive compiler and use of CRT or printer to print errors .A structured walkthrough is followed in which the programmer mentally executes the program by making use of list of errors as each logical path is followed . Programmer should test each program by making test plans for each step as well as testing every exceptions. Interactive Testing programs are available which help to reduce time considerably. Establishment of standards are very much required because it is necessary to check the code against the parameters set so that deviation can be checked and necessary actions can be taken.
- (e) **Program Documentation:** Documentation is required because in case of any drop outs of the programmer or addition of any new member in the team, then the time is not wasted to make them understand the entire process and the progress achieved. Documentation should be simple and it should be made sure that it is understandable.
- (f) **Program Maintenance:** For program maintenance a separate category of people are required who are known as maintenance programmers. It is not an easy task to review the program since the developers of the program are different from the ones who are reviewing it.

(b) **Design Tools:** There are several Design Tools available which help to efficiently design the program:

1. **Flow charts:** They depict the logical steps required through which the program must proceed in order to solve the problem. The major disadvantage is that these do not provide the broad view of the program organization.They are useful for abstract types of user problems.
2. **Pseudo code:** Instead of using graphical methods, flow lines etc., pseudo code presents the program logic in English. It is preferred because it examines the program more closely .It is useful in designing transaction processing and information retrieval

programs.

3. **Structure Chart:** In a structured chart, the program is divided into modules and they are formed in the hierarchy model. The higher modules represent control portions and lower level modules do the actual task of the programs.
4. **4GL Tools:** Fourth generation language makes use of automated tools which provide consistency and efficiency since manual tasks are more prone to errors
5. **Object oriented programming and design tools:-** They make use of objects ,classes and their relationship with one another. This design is often taken from data flow design (DFD).

(c) Importance of Training personnel

A system can succeed or fail depending on the way it is operated and used. Therefore, the quality of training received by the personnel involved with the system in various capacities helps or hinders the successful implementation of information system. Thus, training is becoming a major component of systems implementation. When a new system is acquired which often involves new hardware and software, both users and computer professionals generally need some type of training. Often this is imparted through classes, which are organized by the vendor, and through hands-on learning techniques.

Training Systems Operators: Many systems depend on the computer-centre personnel who are responsible for keeping the equipment running as well as for providing the necessary support services. Their training must ensure that they are able to handle all possible operations, both routine and extra-ordinary. Operator training must also involve the data entry personnel. If the system calls for the installation of new equipment, such as a new computer systems, special terminals or data-entry equipments, the operators training should include such fundamentals as how to turn the equipment on and use it, and knowledge of what constitute normal operation and use. The operators should also be instructed in what common malfunctioning may occur, how to recognize them, and what steps to take when they arise. As part of their training, operators should be given both a trouble shooting list that identifies possible problems and remedies for them, as well as the names and telephone numbers of individuals to contact when unexpected or unusual problem arise. Training also involves familiarization with run procedures, which involve working through the sequence of activities needed to use a new system on an on-going basis.

User Training: User training may involve equipment use, particularly in the case where a micro-computer is in use and the individual involved is both operator and user. In these cases, users must be instructed how to operate the equipment. User training must also instruct the individuals involved in trouble shooting of the system, determining whether the problem is caused by the equipment or software or by something they have done in using the system. Most user training deals with the operation of the system itself. Training in data coding emphasises the methods to be followed in capturing data from transactions or preparing data for decision support activities. Users should be trained on data handling activities such as editing data, formulating inquiries (finding specific records or getting responses to questions) and deleting records of data. From time to time, users will have to prepare disks, load paper into printers, or change ribbons on printers. Some training time should be devoted to such system maintenance activities. If a micro computer or data entry system uses disks, users should be instructed in formatting and testing disks.

Training is often seen as a necessary evil by managers. While recognizing its importance, many managers have to release employees from their regular job activities so that they can be trained. When managers are actively involved in determining training needs, they are usually more supportive of training efforts. It is generally wise to have managers directly involved in evaluating the effectiveness of training activities because training deficiencies can translate into reduced user productivity level.

8. (a) **General controls:** These controls apply to a wide range of exposures that systematically threaten the integrity of all applications processed within the computer Based Information System (CB IS) environment. General controls can be further subdivided under following headings:

- (i) Operating system controls
- (ii) Data management controls
- (iii) Organisational structure controls
- (iv) Systems development controls
- (v) Systems maintenance controls
- (vi) Computer centre security and controls
- (vii) Internet and Intranet controls
- (viii) Personal computer controls.

Personal Computer Controls

The capabilities, adaptability and user friendliness of Personal Computers (PCs) are posing a serious challenge to auditors as stated below:

- PCs are likely to be shifted from one location to another or even taken outside the organization.
- Decentralized purchasing of PCs can result in hardware/software incompatibility in the long run.
- Floppies can be very conveniently transported from one place to another, as a result of which data corruption may occur. Mishandling, improper storage etc. can also cause damage.
- The inherent data security provided is rather poor.
- There is a chance that applications software are not thoroughly tested.
- Segregation of duties is not possible, owing to limited number of staff.
- The operating staff may not be adequately trained.
- Computer viruses can slow down the system, corrupt data and so on.

The security measures that could be exercised are as follows:

- Physically locking the keyboard or the PC itself must be enforced.
- Proper logging of equipment shifting must be done.
- The PC purchases must be centrally coordinated and company-wide standards established for spread sheets, word-processors, applications software etc.
- Floppies must be stored in secured places and their issues duly authroised. They must be adequately packed before any shipment.
- Data and programs on hard-disks must be secured using hardware/software mechanisms. Backups must be taken regularly.
- Minimum standard must be set for developing, testing and documenting applications.
- Properly organized training programs must be periodically conducted. More than one user should be trained on each application.
- Virus prevention and detection software obtained from reliable sources must be used. Write protect tables should be used on diskettes that do not require any alteration. Pirated software should be strictly avoided.
- The PCs and their peripherals must be maintained regularly.

While the proliferation of powerful PCs in recent years has its own plus points, the

associated risks must not be ignored. Thus, implementing effective controls is of prime importance.

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

Weak Access Control: Security software that provides log-on procedures is available for PCs. Most of these programs, however, become active only when the computer is booted from the hard drive. A computer criminal attempting to circumvent the log-on procedure may do so forcing the computer to boot from the A: drive, where by an uncontrolled operating system can be loaded into the computer's memory. Having bypassed the computer's stored operating system and security package, the criminal has unrestricted access to data and programs on the hard disk.

Disk locks are devices that prevent unauthorized individuals from accessing the floppy disk drive of a computer. One form of disk lock is a memory-resident program that prevents the computer from being booted from the A: drive. The lock will also prevent the A: drive from being used to run programs, upload data and programs to the hard disk. This form of disk lock is password controlled so it can be disabled as needed by an authorized user.

Multilevel Password Control: It is used to restrict employees who are sharing the same computer to specific directories, programs, and data files. The technique uses stored authorization tables to further limit an individuals' access to read-only, data input, data modification, and data deletion capability. Multilevel password control can greatly enhance the small organisation's control environment.

Inadequate Backup Procedures: To preserve the integrity of mission-critical data and programs, organizations need formal backup procedures. Computer failure, usually disk failure, is the primary cause of significant data loss in the PC environment. If the hard drive of the microcomputer fails, it may be impossible to recover the data stored on the disk. Formal procedures for making backup copies of critical data (and program) files can reduce this threat considerably. There are a number of options available for dealing with this problem.

Floppy Disk Backup: Files can be backed up to floppy disks at routine periods during processing and stored away from the computer. In the event of a microcomputer failure, the data file can be reconstructed from the backup disks.

Dual Internal Hard Drives: Microcomputers can be configured with two physical internal hard disks. One disk can be used to store production data while the other stores the backup files.

External Hard Drives: A popular backup option is the external hard drive with removable disk cartridge, which can store more than a gigabyte of data per cartridge. When a cartridge is filled, the user can remove it and insert a new one. External hard drives can be used as an effective and simple backup technique.

- (b) The term 'disaster Recovery' describes the contingency measures that organizations have adopted at key computing sites to recover from, or to prevent any monumentally bad event or disaster. A disaster may result from natural causes such as fire, flood or earthquake etc. or from other sources such as a violent takeover, willful or accidental destruction of equipment or any other act of such catastrophic proportions that the organization could be ruined. The primary objective of disaster recovery plan is to assure the management that normalcy would be restored in a set time after any disaster occurs, thereby minimising losses to the organization. The disaster recovery plan must take into account the physical location of the computer centre, since it can increase or decrease the chance of a disaster. Protection against flood, fire, earthquake or water logging etc. must be considered.

Although each organization would like to have a specifically tailored disaster recovery plan, the general components of the plan would be as follows:

- (i) **Emergency Plan:** This part of the Disaster Recovery Plan (DRP) outlines the actions

to be undertaken immediately after a disaster occurs. It identifies the personnel to be notified immediately, for example, fire service, police, management, insurance company etc. It provides guidelines on shutting down equipment, termination of power supply, removal of storage files and removable disks, if any. It sets out evacuation procedures like sounding the alarm bell, activating fire extinguishers, evacuation of personnel. It also provides return procedures as soon as the primary facility for operation like backing up data files at off-site, deleting data from disk drives at third party's site, relocation of proper versions of backup files, etc.

(ii) **Recovery Plan:** This part of the DRP sets out how the full capabilities will be restored. A recovery committee is constituted. Preparing specifications of recovery like setting out priorities of recovery of application systems, hardware replacement etc. will be the responsibility of Recovery Committee.

- An inventory of the hardware, application systems, system software, documentation etc. must be taken.
- Criticality of application systems to the organization and the importance of their loss must be evaluated. An indication must be given of the efforts and cost involved in restoring the various application systems.
- An application systems hierarchy must be spelt out. This would be used when the management decides to accept a degraded mode of operation.
- Selection of a disaster recovery site must be made. A reciprocal agreement with another organization having compatible hardware and could be made. However, systems availability and data security problems must be considered at this point. Hiring a service bureau is another option. If the situation warrants, a fully operational backup site could also be considered.
- A formal backup agreement with another company must be made. This should cover the periodical exchange of information between the two sites regarding changes to hardware/software, the time and duration of systems availability, modalities of testing the plan etc.

(iii) **Backup Plan:** Organisations no matter how physically secure, their systems are always vulnerable to the disaster. Therefore, an effective safeguard is to have a backup of anything that could be destroyed, be it hardware or software. As regards hardware, stand by, as discussed above, must be kept with regard to the needs of a particular computer environment. So far as the software is concerned, it is necessary to make copies of important programs, data files, operating systems and test programs etc. in order to get back into operation before the company can suffer an intolerable loss. Often, the originals are stored at site that is physically distant from the actual site, and where duplicate copies are used for processing. The backup copies must be kept in a place which is not susceptible to the same hazards as the originals.

(iv) **Test Plan:** This plan looks after the testing of DRP and analysis of the result. It identifies deficiencies in the emergency, backup or recovery plan. It contains procedures for conducting DRP testing like:

- Paper walk-through: It involves crucial personnel in the plan's execution, reasoning out what might happen in the event of different disasters.
- Localised tests: It simulates system crash. This test is performed on different aspects of DRP.
- Full operational test: It is nearer to disaster conditions. Paper walkthrough and localized tests should have been conducted before completely shutting down the operations to simulate disasters.

9. (a) Control objectives of an operating system are as follows:

(i) The operating system must protect itself from users. User applications must not be

able to gain control of, or damage in any way, the operating system, thus causing it to cease running or destroy data.

- (ii) The operating system must protect users from each other. One user must not be able to access, destroy or corrupt the data or programs of another user.
- (iii) The operating system must protect users from themselves. A user's application may consist of several modules stored in separate memory locations, each with its own data. One module must not be allowed to destroy or corrupt another module.
- (iv) The operating system must be protected from itself. The operating system is also made up of individual modules. No module should be allowed to destroy or corrupt another module.
- (v) The operating system must be protected from its environment. In the event of a power failure or other disaster, the operating system should be able to achieve a controlled termination of activities from which it can later recover.

- (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 system to crash. Operating system failures are also caused by errors in user application programs that the operating system 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.

Intentional 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 organisation, 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

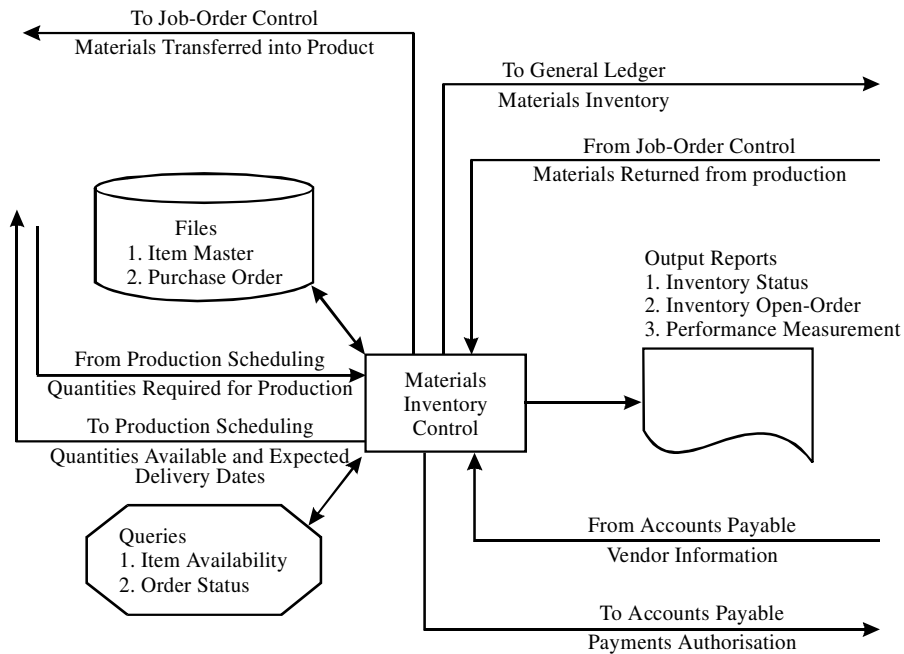
10. The material inventory control system is the point at which materials enter the manufacturing accounting system. This system controls inventory and minimises the costs of purchasing and holding of inventory. The materials inventory control system interfaces directly with the accounts payable, general ledger, production planning, production scheduling and work-in-process control systems as shown in the system flow chart given on the next page.

The objectives of materials inventory control system are to provide accounts payable system with information about vendors and the receipt of goods. Vendor information is first required when sourcing decisions are made. When an order is received, the material inventory control system reports to accounts payable, which in turn, reports to authorise payment.

Materials inventory control provides the general ledger with certain accounting information such as the value of the purchases received, materials transferred into production and the inventory on hand. It generates aggregate journal entries under the following heads: materials inventory accounts payable, work in process and factory overhead control – indirect materials, which are sent to general ledger for the accounting transactions.

Information regarding direct and indirect materials requisitioned from the materials inventory control system is transferred to work-in-process system. Similarly, information about materials

returned from the production department is recorded in materials inventory control. It also provides information concerning quantities available and expected delivery dates to the production scheduling system. This information is then used for scheduling production.



Inputs

There are two basic input files for the materials inventory control system. The items master file contains one record for each item of the inventory. Some of the data items contained in each record are: inventory item number, item description and specification, current quantity on hand, current quantity on order, current period receipts, year-to-date receipts, current period issues, year-to-date issues, standard cost and vendor identification.

The item master is updated when a purchase order is created or items are placed in the inventory.

The purchase order file contains information about new purchase orders. These results from reduced quantities in the inventory or anticipated production requirements. The following data items are found in each record of the purchase order file; inventory item number, item description and specification, vendor identification, quantity ordered, date of order, delivery date, shipping instructions, order status, purchase cost, purchase order number and item quantity actually received.

Reports

The materials inventory control system generally produces following reports on periodic basis:

- (i) An inventory status report contains the quantity of each item available on a particular date. The report provides the unit cost of an item and any costing technique such as FIFO, LIFO and average cost etc. can be used. The report also includes the beginning balance, transfers, receipts, adjustments and ending balance of each item.
- (ii) An open purchase order report contains information concerning the status of open purchase orders. It includes the item number, vendor identification, date of order, unit cost, quantity ordered, promised shipping date, and other status information.
- (iii) Performance measurement reports contain information concerning turnover, stock-outs, shrinkage, investment and other appropriate measurements related to management

performance in inventory control.

The material inventory control system provides the facility of frequently answering the queries about item's availability. These queries result due to potential rush orders from customers or problems encountered during production. The item master file supplies the information regarding these queries. Queries are also received about the status of purchase orders. Delays by vendors frequently cause production delays and scheduling problems. The open purchase order report can be used to identify such problems. For example, if a vendor misses a shipping date, cost estimation and production scheduling departments can be notified so that production schedules can be adjusted. The system is designed to respond instantaneously to these queries so that constant monitoring and control can be exercised on material inventory.

- 11 The different types of securities required for computer system can be categorized as security from accidental breach and incidental breach. Accidental breach of security due to such natural calamities as fire, flood and earthquake etc. may cause total destruction of important data and information. Incidental or fraudulent modification or tampering of financial records maintained by the organization can cause considerable amount of money to be disbursed to fraudulent personnel. Similarly, unauthorized access to secret records of the organization can cause leakage of vital information to competitors. Hence, there is a great need for security of the computer system.

Physical security includes arrangements for fire detection and fire avoiding equipment, security from water damage, and safeguards from energy variation, pollution and unauthorized intrusion.

- (i) **Fire damage:** It is a major threat to the physical security of a computer installation. Some of the major features of a well-designed fire protection system are given below:

- Both automatic and manual fire alarms are placed at strategic locations.
- Companies have a choice of either installing highly sophisticated fire detection equipments or low-tech fire extinguishers.
- A control panel may be installed which shows where in the installation an automatic or manual alarm has been triggered.
- Besides the control panel, master switches may be installed for power and automatic extinguisher system.
- Manual fire extinguishers can be placed at strategic locations.
- Fire extinguishers and fire exits should be clearly marked.
- When a fire alarm is activated, a signal may be sent automatically to permanently manned station.
- All staff members should know how to use the system. The procedures to be followed during an emergency should be properly documented.

- (ii) **Water damage :** Water damage to a computer installation can be the outcome of a fire; the specific system sprays water that enters hardware or water pipes may burst. Water damage may also result from other resources such as cyclones, tornadoes etc. Some of the major ways of protecting the installation against water damage are as follows:

- Wherever possible have waterproof ceilings, walls and floors.
- Ensure an adequate drainage system exists.
- Install alarms at strategic points within the installation.
- In flood areas have the installation above the high water level.
- Have a master switch for all water mains.
- Use a dry pipe automatic sprinkler system that is charged by an alarm and activated by the fire.
- Cover hardware with a protective fabric when it is not in use.

- (iii) **Energy Variation:** Voltage regulators and circuit breakers protect the hardware from temporary increase or decrease of power. Battery back-up can be provided in case a temporary loss of power occurs. A generation plant is needed for sustained losses in power.
- (iv) **Pollution damage:** The major pollutant in a computer installation is dust. Dust caught between the surfaces of magnetic tape / disk and the reading and writing heads may cause either permanent damage to data or read/ write errors. Due consideration should be given for dust free environment in the computer room. Regular cleaning of walls, floors and equipment etc. is essential. Only such materials and finishing may be used inside the room which enables it to remain dust free.
- (v) **Unauthorized intrusion:** Unauthorised intrusion takes two forms. First, the intruder by physically entering the room may steal assets or carry out sabotage. Alternatively, the intruder may eavesdrop on the installation by wire tapping installing an electronic bug or using a receiver that picks up electro-magnetic signals. Physical entry may be prevented by restricting the entry to the computer room by various means. A badge system may be used to identify the status of personnel in the computer room. Eavesdropping breaches the privacy of data. It may be used by an intruder to obtain a password or sensitive information of the organization. Various devices are available to detect the presence of bugs by the intruder.

12. (a) Until recently most large and mid-sized organizations designed and programmed custom information systems in-house. This resulted in an array of stand-alone systems that were designed to the unique needs of specific users. While these systems dealt with their designated tasks efficiently, they did not provide strategic decision support at the enterprise level because they lacked the integration needed for information transfer across organisation boundaries. Today the trend in information systems is toward implementing highly integrated enterprise-oriented systems. These are not custom packages designed for a specific organization. Instead, they are generalized systems that incorporate the best practices in use. Organisations mix and match these prefabricated software components to assemble an enterprise resource planning (ERP) system that best meets their business requirements. This means that an organization may need to change the way that it conducts business to take full advantage of the ERP.

Therefore, implementing an ERP has more to do with changing the way an organisation does business than it does with technology. As a result, most ERP implementation failures are due to cultural problems within the firm that stand in opposition to the objective of process reengineering.

The process of re engineering or changing the way an organization does business, is difficult to accomplish because it challenges traditional work methods, job designs, and departmental functions. However, for drastic changes to occur, executive leadership needs to challenge traditional assumptions. Technology can only supplement the process by providing communications networks, access to shared databases, and access to on-line video conferencing facilities, etc.

Therefore, the given statement regarding implementation of ERP system has more to do with changing the way an organisation does business than it does with technology is true in the current scenario as well.

- (b) Several steps are involved in the implementation of a typical ERP package. These are:
- (i) Identifying the needs for implementing an ERP package.
 - (ii) Evaluating the 'As is' situation of the business i.e., to understand the strengths and weakness prevailing under the existing system.
 - (iii) Deciding the 'would be' situation for the business i.e. the changes expected after the implementation.
 - (iv) Reengineering the business process to achieve the desired results in the existing processes.

- (v) Evaluating the various available ERP packages to assess suitability.
 - (vi) Finalizing the most suitable ERP package for implementation.
 - (vii) Installing the required hardware and networks for the selected ERP package.
 - (viii) Finalising the implementation consultants who will assist in implementation.
 - (ix) Implementing the ERP package.
- 13.** 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 system. This requires their involvement from the time that a transaction is initiated while it is posted to the organization'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 system 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.
 - Authorization producers 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.
 - Data bases are adequately designed and controls 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.
- 14.** Sensitive information may be briefly classified as information relating to strategic plans, operational processes and procedures and finances.
- The factors that should be considered while deciding about the level of protection needed for information are:
- (i) Acts as a documentation aid.
 - (ii) Is useful for file security.
 - (iii) Helps in establishing an audit trail.
 - (iv) Is useful for planning the flow of transaction data through the system.
 - (v) Serves as an important aid in investigating or documenting internal control procedures.
- For details, refer to Chapter 18, Section 18.2.1 – 18.2.2 of the study material.
- 15. (a)** In a global information society, where information travels through cyberspace on a routine basis, the significance of information is widely accepted. In addition, information and the information systems and communications that deliver the information are truly pervasive throughout organization – from the users platform to local and wide area networks to servers

to mainframe computers. Organisations depend on timely, complete, valid, consistent, relevant and reliable information. Accordingly, executive management has a responsibility to ensure that the organization provides all users with a secure information systems environment.

There are not only many direct and indirect benefits from the use of information systems, there are also many direct and indirect risks relating to the information systems. These risks have led to a gap between the need to protect systems and the degree of protection applied. Security failures may result in both financial losses and / or intangible losses such as unauthorized disclosure of competitive or sensitive information. Threats to information system may arise from intentional or unintentional acts and may come from internal or external sources.

Adequate measures for information security help to ensure the smooth functioning of information systems and protect the organisation from loss or embarrassment caused by security failures.

(b) Role of Information Security Administrator:

- (i) 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.
- (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 needs to protect these securities are also stressed. He assigns responsibilities to job classification and formulates what 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 process, train security coordinators, select software security packages and solve problems.
- (vi) He investigates all security violations.
- (vii) He advises senior management on matters of information resource control.
- (viii) He consults on matters of information security.
- (ix) 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.
- (x) 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.

16. (a) Commonly used concurrent audit techniques for information systems are discussed below:

- (i) **An Integrated Test Facility Technique (ITF)** places a small set of fictitious records in the master files. Processing test transactions to update these dummy records will not affect the actual records. Since fictitious and actual records are processed together, company employees usually remain unaware that this testing is taking place. The system must distinguish ITF records from actual records, collect information on the effects of the test transactions and report the results. The auditor compares processing and expected results in order to verify that the system and its controls are operating correctly.

ITF technique can be used effectively for both batch processing system as well as online processing system.

- (ii) **The Snapshot Technique** examines the way transactions are processed. Selected transactions are marked with a special code that triggers the snapshot process. Audit modules in the program record these transactions and their master file records before and after processing. Snapshot data are recorded in a special file and reviewed by the auditor to verify that all processing steps have been properly executed.
- (iii) **System Control Audit Review File (SCARF)** uses embedded audit modules to continuously monitor transaction activity and collect data on transactions with special audit significance. The data are recorded in a SCARF file. Transactions that are generally recorded in a SCARF file include those exceeding a specified limit, inactive accounts, deviating from company policy, or containing write-downs of asset values etc. Periodically the auditor examines the SCARF file to identify questionable transactions and performs the necessary follow-up investigations.
- (iv) **Audit hooks** are audit routines that flag suspicious transactions. For example, internal auditors at an Insurance Company determined that their policyholder system was vulnerable to fraud every time a policyholder changed his or her name or address and then subsequently withdrew funds from the policy. They devised a system of audit hooks to tag records with a name or address change. The internal audit department will investigate these tagged records for fraud. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach of real-time notification displays a message on the auditor's terminal.
- (v) **Continuous and Intermittent Simulation (CIS)** module that is embedded in a data base management system, examines all transactions that update the DBMS using criteria similar to SCARF. If a transaction has special audit significance, the module independently processes the data, records the results and compares them with those obtained by DBMS. If any discrepancies exist, the details are written on to an audit log for subsequent investigation. In case of serious discrepancies, CIS may prevent the DBMS from executing the update process.

Relevance of Concurrent Audit Techniques for Information System

Millions of rupees worth of transactions can be processed in an on-line system without leaving a satisfactory audit trail. Evidence gathered after data processing is insufficient for audit purposes. Since many on-line systems process transactions continuously, it is difficult or impossible to stop the system in order to perform audit tests. When it is needed to continually monitor the system and collect audit evidence while live data are processed during regular operating hours, concurrent audit techniques are used. These techniques perform audit functions, they also report test results to the auditor and store the evidence collected for the auditor's review.

- (b) 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, fibre 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) **Fire wall:** Organizations 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 organisation's Intranet must pass through the firewall.
- Only authorised traffic between the organisation and the outside is allowed to pass through the firewall.
- The firewall must be immune to penetration from both outside and inside the organisation.

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, ACK packets and ACD packets. Computer hacker transmits hundreds of SYN packets to the receiver but never responds with an ACD 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 organisation 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 measure 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 authorised terminals or telephone numbers and prevents an intruder masquerading as a legitimate user.

- 17. E-Governance:** It refers to the legal recognition of electronic records. The law provides that information or any other matter should be in writing or in the type written or printed form, then not withstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is:

- (a) rendered or made available in an electronic form; and
- (b) accessible so as to be usable for a subsequent reference

Chapter III is associated with E-Governance. It specifies the procedures to be followed for sending and receiving of electronic records and the time and the place of the dispatch and receipt. This chapter contains sections 4 to 10.

Section 4: This section provides for “legal recognition of electronic records”.

Section 5: It provides for legal recognition of digital signatures.

Section 6: It lays down the foundation of electronic governance.

Section 7: This section provides that the documents, records or information which has to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form provided the following conditions are satisfied:

- (i) the information therein remains accessible so as to be usable subsequently.
- (ii) the electronic record is retained in its original format or in a format which accurately represents the information contained.
- (iii) the details which will facilitate the identification of the origin, destination, dates and time of dispatch or receipt of such electronic record are available therein.

Section 8 : It provides for the publication of rules, regulations and notifications in the electronic gazette.

Section 9: It provides that the conditions stipulated in sections 6, 7 and 8 shall not confer any right to insist that the document should be accepted in an electronic form by any Ministry or department of the Central and State Government.

Section 10: It provides power to Central Government to make rules in respect of Digital Signature.

For details, students are advised to refer to study paper, chapter 16, section 16.3 (Chapter III).

18. (a) Strategic Decision Making

Strategic level management is concerned with developing of organizational mission, objectives and strategies. Decisions made at this level of organization to handle problems critical to the survival and success of the organization are called strategic decisions. They have a vital impact on the direction and functioning of the organisation-as for example decisions on plant location, introduction of new products, making major new fund-raising and investment operations, adoption of new technology, acquisition of outside enterprises and so on. Much analysis and judgement go into making strategic decisions.

In a way, strategic decisions are comparable to non-programmed decisions and they share some of their characteristics. Strategic decisions are made under conditions of partial knowledge or ignorance.

(b) Software tools for Decision Support Systems

The tools of decision support include a variety of software supporting database query, modeling, data analysis, and display. A comprehensive tools kit for DSS would include software supporting these application areas. Examples of software tools falling into these four categories are given in Table.

Data based Software	Model Based Software	Statistical Software	Display-Based Software
Dbase IV	Foresight	SAS	Chart Master
FOCUS	IFPS	SPSS	SASGRAPH
NOMAD II	Lotus 1-2-3	TSAM	TELLAGRAF
RAMIS	Model		
R: base 5000	Multiplan		
SQL	Omnicalc		

Database Languages: Tools supporting database query and report generation use mainframe, minicomputer, and microcomputer-based databases. FOCUS, RAMIS, and NOMAD II, for example, are mainframe-based languages supporting database query, report generation, and simple analysis. FOCUS and RAMIS are also available in PC versions. Ingress, Oracle, and Informix are database languages on mainframes, minicomputers, and microcomputers. Managers frequently use microcomputer-based database tools such as MS-Access and R: base 5000.

Model based analysis tools such as spread-sheet software enable managers to design models that incorporate business rules and assumptions. Modeling tools are designed to support financial modeling and analysis.

Statistical analysis tools such as SAS and SPSS support market researchers, O.R. analysts and other professionals using statistical analysis functions.

Display-based decision support software which generate graphical outputs are very effective in management presentation.

(c) System Design Phase

After the completion of requirements analysis for a system, systems design activity takes place for the alternative which is selected by the management. The system design phase usually consists of following three activities:

- (i) Reviewing the system's informational and functional requirements;
- (ii) Developing a model of the new system, including logical, and physical specifications of outputs, inputs, processing, storage, procedures and personnel;
- (iii) Reporting results to management.

The system's design must conform to the purpose, scale and general concepts of the system that management approved during the requirements analysis phase. Therefore, users and systems analysts must review each of these matters again before starting the design because they establish both the direction and the constraints that system developers must follow during rest of the activities.

As mentioned above, system design involves first logical design and then physical construction of a system. When analysts formulate a logical design, they write the detailed specifications for the new system, they describe its features; the outputs, input files, databases and procedures, all in a manner that meets systems requirements. The statement of these features is termed as the design specifications of the system.

(d) Implementation Guidelines for ERP

There are certain general guidelines, which are to be followed before starting the implementation of an ERP package.

1. Understanding the corporate needs and culture of the organization and then adopt the implementation technique to match these factors.
2. Doing a business process redesign exercise prior to starting the implementation.
3. Establishing a good communication network across the organization.
4. Providing a strong and effective leadership so that people down the line are well motivated.
5. Finding an efficient and capable project manager.
6. Creating a balanced team of implementation consultants who can work together as a team.
7. Selecting a good implementation methodology with minimum customization.
8. Training end uses.
9. Adapting the new system and making the required changes in the working environment to make effective use of the system in future.

19. (a) Middleware: The network system 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. General middleware allows for communication, directory services, querying, distributed file sharing and printing. The middleware is typically composed of four layers, which are Service, Back-end Processing, Network operating system and Transport Stocks. The service layer carries coded instructions and data from software application to the Back-end Processing layer for encapsulating network-routing instructions. Next, the Network Operating Systems adds additional instructions to ensure that the Transport layer transfers data packets to its designated receiver efficiently and correctly. During the early stage of middleware development, the transfer method was both slow and unreliable.

(b) Trojan Horse: A Trojan Horse is a program whose purpose is to capture Ids and passwords from unsuspecting users. The program is designed to mimic the normal log-on procedures of the operating system. When the user enters his/her ID and password, the Trojan horse stores a copy of them in a secret file. At some later date, the author of the Trojan Horse uses these Ids and passwords to access the system and masquerade as an authorized user.

Threats from destructive programs can be substantially reduced through a combination of technology controls and administrative procedures. The following examples are relevant to most operating systems:

- Purchase software only from reputable vendors and accept only those products that are in their original, factory-sealed packages.
- Examine all upgrades to vendor software for viruses before they are implemented.
- Establish an educational program to raise user awareness regarding threats from viruses and malicious programs.
- Install all new applications on a stand-alone computer and thoroughly test them with antiviral software prior to implementing them on the mainframe or LAN server.
- Routinely make back copies of key files stored on mainframes, servers, and workstations.
- Use antiviral software (also called vacancies) to examine application and operating system programs for the presence of a virus and remove it from the affected program.

(c) 4GL workbenches: 4GL work benches are geared towards producing interactive application which rely on extracting information from an organizational database, presenting it to end users on their terminal or work stations and then updating the database with changes made by users. The user interface usually consists of a set of standard forms or a spread-sheet. The tools which may be included in a work bench are:

- (i) **A database query language** such as SQL which may either be input directly or generated automatically from forms filled in by end users.
 - (ii) **A form design tool** which is used to create forms for data input and display.
 - (iii) **A spread-sheet** which is used for the analysis and manipulation of numeric information.
 - (iv) **A report generator** which is used to define and create reports from information in the database.
- (d) **Program maintenance:** The requirement of business data processing applications are subject to continual changes. This calls for modification of the various programs. There are, usually separate categories of programmers called maintenance programmers who are entrusted with this task. There is a difficult task of understanding and then revising the program they did not write. This should bring out the necessity of writing programs in the first place that are simple to understand.

Maintenance can be categorized in the following two ways:

- (i) Scheduled maintenance is anticipated and can be planned for. For example, the implementation of a new inventory coding scheme can be planned in advance.
- (ii) Rescue maintenance refers to previously undetected malfunctions that are not anticipated but require immediate solution. A system that is properly developed and tested should have few occasions of rescue maintenance.