

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

QUESTIONS

1. Define the following terms:
 - (a) System
 - (b) Information
 - (c) Direct Processing
 - (d) Database
 - (e) Snapshot Techniques
 - (f) Dynamic Analyser
 - (g) Transaction File
 - (h) Data Flow Diagram
 - (i) Middleware
 - (j) Prototype
 - (k) Legal Feasibility
 - (l) Function Code
 - (m) Virus
 - (n) Scavenging
 - (o) Test Data Generator.
2.
 - (a) Define 'System' and its environment in brief.
 - (b) What are the characteristics of good or useful information?
3.
 - (a) How transactions can be grouped in business organization? Discuss in brief.
 - (b) What are the essential factors that determine the effective MIS in an organization?
 - (c) What are the various categories of information needed in management process.
4.
 - (a) Discuss various benefits which are attained by implementing a computerized model for making decision.
 - (b) Describe the components of the DSS in brief.
 - (c) Briefly describe the purpose of an Executive Information System.
5.
 - (a) What is Client-Server Technology? Enumerate any six of its benefits.
 - (b) Explain the major categories of risks involved in transition from the mainframe computers to client servers.
6.
 - (a) Discuss in brief the various approaches to System Development.
 - (b) State the reasons why the organisations fail to achieve their system development objectives?
7.
 - (a) Discuss various important factors to be kept in mind while designing an Input from an information system.
 - (b) Discuss the importance of Coding System in an information system. What are the desired characteristics of a good coding scheme?
8.
 - (a) Discuss the various factors that should be considered while selecting a computer system.
 - (b) Explain the stages through which the program has to pass during its development.
9.
 - (a) Describe in brief various activities that are involved for successful conversion of an existing manual system to a computerised Information System.
 - (b) Why is personnel training important for the successful implementation of Information System? Discuss with example.
10. For an online real time sales order Processing System, draw a system flow chart and explain the following:
 - (i) Transactions and processing
 - (ii) Files
 - (iii) Output reports and documents.

11. (a) What is an ERP System? Describe the major benefits achieved by implementing the ERP packages.
- (b) What are the general guidelines which are to be followed before starting the implementation of an ERP package.
12. (a) What are the different types of Security and Controls that are required in a computer centre environment.
- (b) What do you mean by "Disaster Recovery Plan"? Discuss its various components in detail.
13. Explain, in brief, the broad classes of input controls.
14. (a) What are the primary risks to business organisations from computer frauds?
- (b) Discuss, in details, the various controls which help to ensure the accuracy, integrity and safety of system resources and also makes it difficult to commit computer frauds.
15. What is Digital Signature? How is it used? What are the duties of certifying authorities in regard to its usage.
16. (a) Discuss the various issues that are of primary concern for an auditor involved in IS Auditor.
- (b) Briefly discuss the framework on which the auditor should work for the audit of Computer Security.
17. (a) Describe in brief the best approach to implement Information Security.
- (b) Explain the role played by an Information Security Administrator.
18. (a) What are CASE Tools? Describe in detail the categories of CASE Tools.
- (b) Describe Testing Workbenches in detail.
19. Define the following:
 - (a) Materials Requirement Planning (MRP)
 - (b) Expert Systems
 - (c) Data Dictionary
 - (d) System Testing
 - (e) Point-scoring analysis in vendor evaluation
 - (f) Bench Marking problem for vendor's proposals
 - (g) Personal Computer Controls
 - (h) Firewalls
 - (i) Transaction Logs
 - (j) Disc Imaging and Analysis Techniques.

SUGGESTED ANSWERS/HINTS

1. (a) System: It a set of interrelated elements that operate collectively to accomplish some common purpose or goal. A business is also a system where economic resources such as people, money, materials, machines, etc. are transformed by various organisational processes into goods and services.
- (b) Information: Information is data that have been put into a meaningful and useful context. It is defined as" information is data that has been processed into a form that is meaningful to the recipient and is of real or perceived value in current or progressive decision".
- (c) Direct Processing: In direct processing, individual transactions are posted directly to ledgers rather than being batched to build a transaction file. A ledger may be periodically

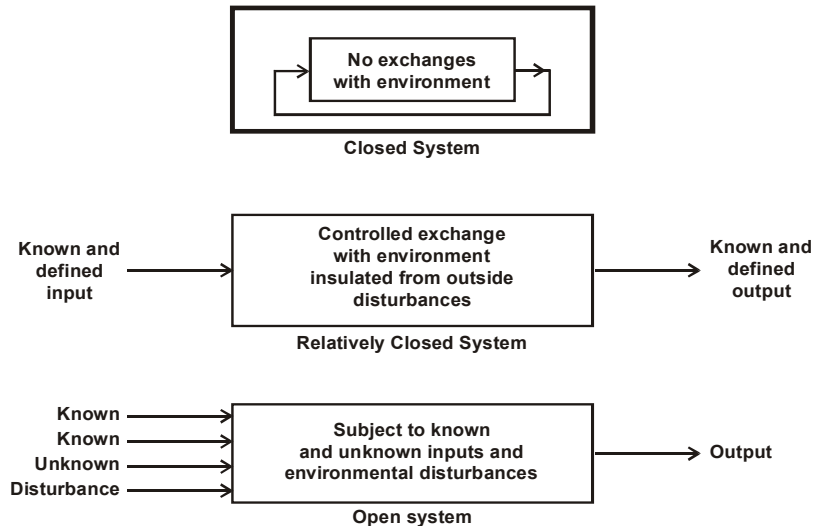
processed to generate a listing of transactions that have been posted to it over some period of time. This transaction file is created as a by-product of posting the ledger.

- (d) Database: It can be defined as a “superfile” which consolidates data records formerly stored in many data files. The data in database is organised in such a way that access to the data is improved and redundancy is reduced.
 - (e) Snapshot technique: This is a concurrent audit technique that examines the way transactions are processed by marking selected transactions with a special code. Snapshot data are recorded in a special file and reviewed by the auditor to verify that all processing steps have been properly executed.
 - (f) Dynamic analyser: It produces a source code listing annotated with the number of times each statement was executed when the program was run.
 - (g) Transaction file: It is a collection of transaction input data. Transaction files usually contain data that are of temporary nature rather than permanent interest.
 - (h) Data flow diagram: A data flow diagram (DFD) graphically describes the flow of data within an organisation. It is used to document existing systems and to plan and design new ones.
 - (i) Middleware: The network system implemented within the client/server technology is commonly called by the computer industry as middleware. Middleware is the distributed software needed to allow clients and servers to interact.
 - (j) Prototype: It is a working system with software that accepts input, performs calculations, and carries out other meaningful activities. It is designed to be evaluated by users and modified repeatedly until a system is developed that suits their requirement.
 - (k) Legal feasibility: Legal feasibility is largely concerned with any conflict between a newly proposed system and the organisation's legal obligations.
 - (l) Function code: It states the activities or work to be performed without spelling out all of the details in narrative statements. Data required for input vary depending on what function is needed. Adding a new record would require all data elements to be input, including the function code.
 - (m) Virus: A virus is a program (usually destructive) that attaches itself to a legitimate program to penetrate the operating system. The virus destroys application programs, data files, and operating systems in a number of ways.
 - (n) Scavenging: Gaining access to confidential information by searching corporate records is known as scavenging. Scavenging methods range from searching trashcans for printouts or carbon copies of confidential information to scanning the contents of computer memory.
 - (o) Test data generator: It Generates test data for the program to be tested. It may be accomplished by selecting data from a database or by using patterns to generate random data of the correct form.
2. (a) System (from Latin systēma) is a set of entities, real or abstract, comprising a whole where each component interacts with or is related to at least one other component and they all serve a common objective. The system may be defined as a set of interrelated elements that operate collectively to accomplish some common purpose or goal. A business is also a system where economic resources such as people, money, material, machines, etc are transformed by various organizational processes (such as production, marketing, finance etc.) into goods and services. A computer based information system is also a system which is a collection of people, hardware, software, data and procedures that interact to provide timely information to authorized people who need it. A general models of a physical system is input, process and output.

All systems function within some sort of environment. The environment, like the system, is a collection of elements. These elements surround the system and often interact with it. For any given problem, there are many types of systems and many types of environments. The

features that define and delineate a system form its boundary. The system is inside the boundary; the environment is outside the boundary.

A subsystem is a part of a larger system. Each system is composed of subsystems, which in turn are made up of other subsystems, each sub-system being delineated by its boundaries. The interconnections and interactions between the subsystems are termed interfaces. Interfaces occur at the boundary and take the form of inputs and outputs.



A supra-system refers to the entity formed by a system and other equivalent systems with which it interacts. Collectively, these elements in the marketing area may be viewed as making up the marketing supra-system. Similarly the various functional areas (subsystems) of an organisation are elements in the same supra-system within the organisation.

(b) The important characteristics of useful and effective information are as follows:

1. Timeliness
2. Purpose
3. Mode and format
4. Redundancy
5. Rate
6. Frequency
7. Completeness
8. Reliability
9. Cost benefit analysis
10. Validity
11. Quality.

For more details of the above points, students are advised to refer to the study material Chapter-1, Section 1.5.1.

3. (a) A transaction processing cycle organises transactions by an organisation's business processes. The nature and types of transaction processing cycles vary, depending on the information needs of a specific organisation. Nevertheless, most business organisations have common transactions that may be grouped according to four common cycles of business activity.

- (1) Revenue cycle: 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 receivable and sales reporting.
- (2) Expenditure cycle: Events related to the acquisition of goods and services from other entities and the settlement of related obligations. It includes application systems involving vendor selection and requisitioning, purchasing, accounts payments payable and payroll.
- (3) Production cycle: 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.
- (4) Finance cycle: 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.

A transaction processing cycle consists of one or more application systems. Application system processes logically related transactions. The transaction cycle model of an organisation includes a fifth cycle – the financial reporting cycle. The financial reporting cycle is not an operating cycle. It obtains accounting and operating data from the other cycles and processes these data in such a manner that financial reports may be prepared. The concept of transaction processing cycles provides a framework for analyzing an organisation's activities. Although different organizations may not include the same application systems within a given transaction processing cycle, the cycle concept provides a basis for categorizing the flow of economic events that are common to all organisations.

(b) The essential factors for an effective MIS are:

- (1) Database: It can be defined as a "superfile" which consolidates data records formerly stored in many data files. The data in database is organised in such a way that access to the data is improved and redundancy is reduced. The database is sub-divided into major information sub-sets needed to run a business. The main characteristic of a database is that each sub-system utilises same data and information kept in the same file to satisfy its information needs.
- (2) Qualified system and management staff: The second pre-requisite of an effective MIS is that it should be manned by qualified officers. These officers are expert in the field and understand clearly the views of their fellow officers. The organisational management base should comprise of two categories of officers viz. (1) Systems and Computer experts and (2) Management experts.
- (3) Support of Top Management: The management information system to be effective, should receive full support of the top management. To gain the support of top management, the officers should place before top management, all the supporting facts and state clearly the benefits, which will accrue from it to the concern. This step will certainly enlighten management, and will change their attitude towards MIS. Their wholehearted support and cooperation will help in making MIS an effective one.
- (4) Control and maintenance of MIS: Control of the MIS means the operation of the system as it was designed to operate. Some time, users develop their own procedures or short cut methods to use the system, which reduce its effectiveness. To check such habits of users, the management at each level in the organisation should devise checks for the information system control. Maintenance is closely related to control. Formal methods for changing and documenting changes must be provided.
- (5) Evaluation of MIS: An effective MIS should be capable of meeting the information requirements of its executives in future as well. This capability can be maintained by evaluating the MIS and taking appropriate timely action.

For more details of the above points, students are advised to refer to the study material Chapter-1, Section 1.5.1.

- (c) The information is necessary to managers for performing the functions of planning and controlling. The task of establishing the information requirements for the aforesaid functions is usually performed by system analysts and system designers. They establish the information requirement by interviewing and analysing the functions, which each executive in the organisation is required to perform. The planning information requirements of executives can be categorised into three broad categories viz. (a) environmental, (b) competitive and (c) internal.
 1. Environment information:
 - (i) Government policies
 - (ii) Factors of production
 - (iii) Technological environment
 - (iv) Economic trends
 2. Competitive information:
 - (i) Industry demand
 - (ii) Firm demand
 - (iii) The competitive data
 3. Internal information: It includes information concerning organisations'
 - (i) sales forecast, (ii) financial plan/budget, (iii) supply factors, and (iv) policies, which are vital for subsidiary planning at all levels in the organisation.
4. (a) A growing number of companies are making effective use of MIS in aiding the decision making process. For example, a major chemical company uses a computer model to simulate an industry segment and the company's potential for a share of market and profitability. A computerized model may incorporate accounting, production, transportation, manufacturing and marketing operations of the company. Such models allow a decision maker to consider a large number of factors in decision-making process, which was not possible in manual system. This highlights the need to reduce skepticism that managers have toward sophisticated computerized decision making aids. This type of model puts pertinent information into a analytical framework that aids the management decision making process.

Some of the benefits offered by computerized model for decision-making are:

- (1) Managers must deal immediately with many day-to-day business problems, as well as plan and control their operations. Managers require different information for the various kinds of decisions they must make. Computerised model provides reports on variances, cost-volume-profit analyses, etc to help managers in decision-making.
- (2) Computerised models provide managers with data to which ratios analysis tools may be applied. They provide management with a variety of measures of the soundness of the organization and make it possible to explore ways of improving the organization's financial condition.
- (3) Computerised models make a fairly accurate forecasts that will affect the organization's performance in the future. Forecasting the financial health of the organization through long-range budget estimates, provides managers with opportunities to consider actions that will help the organization survive bad times or take advantage of a future environment.
- (4) Computerised models permit managers in tracing variances i.e. actual revenues and expenses and compare these amounts to expected revenues and expenses.

Comparison of budget data against such standards allows managers to assess how they use their resources to achieve their goals.

- (5) The models also estimate the amount of cash that will be received and spent each month i.e. in which months there will be excess funds that might be put to use and in which month there will be insufficient funds. Thus, the information supplied helps managers to make decisions about investing, purchasing and borrowing money. The models also help in tracking cash balances on a day-to-day basis and help the managers in their investment decisions so as to maximize organization income.
 - (6) Computerized models are highly useful for carrying out analysis of historical data speedily, which may be quite difficult or even impossible manually for forecasting the future.
- (b) Decision support system has four basic components:
- (1) The users: The user of a decision support system is usually a manager with an unstructured or semi-structured problem to solve. The manager may be at any level of authority in the organisation either top management or operating management. The most important knowledge is a thorough understanding of the problem and the factors to be considered in finding a solution.
 - (2) Databases: Decision support systems include one or more databases. These databases contain both routine and non-routine data from both internal and external sources. The data from external sources include data about the operating environment surrounding an organisation. The database may also capture data from other subsystems such as marketing, production, and personnel.
 - (3) Planning languages: Two types of planning languages that are commonly used in decision support systems are: (1) general –purpose planning languages and (2) special-purpose planning languages. General-purpose planning languages allow users to perform many routine tasks – for example, retrieving various data from a database or performing statistical analyses. The languages in most electronic spreadsheets are good examples of general-purpose planning languages. The languages, such as SAS, SPSS, and Minitab, are examples of special purpose planning languages.
 - (4) Model base: The model base is the “brain” of the decision support system because it performs data manipulations and computations with the data provided to it by the user and the database. The analysis provided by the routines in the model base is the key to supporting the user's decision. The model base may dictate the type of data included in the database and the type of data provided by the user.
- (c) The purpose of EIS are:
- (1) The primary purpose of an Executive Information System 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.
 - (2) A secondary 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. Timely access also influences learning. Using traditional methods, by the time the answer is produced, the context of the question may be lost, and the learning cycle will not continue.
 - (3) A 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. The powerful focus of an EIS is due to the saying “what gets measured gets done.” Managers are particularly attentive to concrete information about their performance when it is available to their superiors. This focus is very valuable to an organization if the information reported is actually important and represents a balanced view of the organization's objectives.

5. (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 database-oriented C/S technology, as well as more recent general distributed computing technologies. The use of LANs has made the client/server model even more attractive to organizations.

Client/server systems have been hailed as bringing tremendous benefits to the new user, especially the users of mainframe systems. Consequently, many businesses are currently in the process of changing or in the near future will change from mainframe (or PC) to client / server systems. Client / Server has become the IT solution of choice among the country's largest corporations. In fact, the whole transition process, that is a change to a client/ server invokes, can benefit a company's long run strategy.

The main benefits offered by client / server technology are stated below:

- (1) The expenses of hardware and network in the client/server environment are less than those in the mainframe environment.
 - (2) 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.
 - (3) Client/server applications make organisations more effective by allowing them to port applications simply and efficiently.
 - (4) Reduces 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.
 - (5) Reduces 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.
 - (6) 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.
- (b) The four categories of risks involved in the transition from mainframe to client server are :
- (1) Technological risks: It is quite simple. How long will the system work without becoming obsolete? It will become obsolete is inevitable thus the question becomes – how soon will it become obsolete?. To resolve this issue, the firm and the IT consultant/division should understand system standards and market trends and use them in their decision-making processes while deciding what system to incorporate into their organisation.
 - (2) Operational risks: These risks parallel the technological risks in both the short and long run. The questions that arise are - Will you achieve the performance you need from the new technology and will the software that you chose be able to grow or adapt to the changing needs of the business? Only sound planning and keeping an eye to the future are the remedies for these risks.
 - (3) Economic risks: In the short run, firms are susceptible to hidden costs associated with the initial implementation of the new client/server system. Cost will rise in the short term since one needs to maintain the old system (main frame) and the new client server architecture development. In the long run, the concern centres around the support cost of the new system.
 - (4) Political risks: Political risks involved in this transition are based on short-term and long- term concerns. The short- term concern is-will end users and management be

satisfied? The answer is negative if the system is difficult to use or is plagued with problems.

6. (a) Approaches to Systems Development:

- (1) Traditional approach: In the traditional approach of the systems development, activities are performed in sequence. When the traditional approach is applied, an activity is undertaken only when the prior step is fully completed. Under traditional approach the managers and users should thoroughly review the work before granting their permission to start the next activity.

The traditional approach is applied to the development of larger computer based information systems such as the transaction processing systems. Because the processing requirements of these systems are well understood, the risk of users and systems analysts misperceiving the system are less than for other types of systems.

- (2) Prototyping approaches: The traditional approach sometimes may take years to analyse, design and implement a system. In order to avoid such delays, prototyping techniques is used to develop smaller systems such as decision support systems, management information systems and expert systems. The goal of prototyping approach is to develop a small or pilot version called a prototype of part or all of a system. A prototype is a usable system or system component that is built quickly and at a lesser cost, and with the intention of being modifying or replacing it by a full-scale and fully operational system. Prototyping can be viewed as a series of four steps:

Step 1: Identify Information System Requirements

Step 2: Develop the Initial Prototype

Step 3: Test and Revise

Step 4: Obtain User Signoff of the Approved Prototype.

- (3) End user development approach: In end-user development, it is the end user and not the computer professional who is responsible for systems development activities. Many different kinds of organisations allow end-users to develop systems. For example, whenever a manager or a department acquires its own, relatively inexpensive micro computers or office information systems, end-user development often takes place.
- (4) Top down approach: The top down approach assumes a high degree of top management involvement in the planning process and focuses on organisational goals, objectives and strategies. Using the top down approach, we begin by analysing organisational objectives and goals and end by specifying application programs and modules that need to be developed to support those goals.
- (5) Bottom up approach: The development of information system under this approach starts from the identification of life stream systems. Life stream systems are those systems, which are essential for the day-to-day business activities. The examples of life stream systems include payroll, sales order, inventory control and purchasing etc. The development of information system, for each life stream system starts after identifying their basic transactions, information file requirements and information processing programs.

The next step is towards the integration of data kept in different data files of each information system. The next step under bottom up approach may be the addition of decision models and various planning models for supporting the planning activities involved in management control.

- (6) Systematic approach for development in small organisations: In smaller organisations, fewer MIS professionals are employed and they may have such a variety of responsibilities that they have little time to develop new systems for users. This systematic approach generally consists of the following steps:

- (a) Identify requirements.
- (b) Locate, evaluate and secure suitable software.
- (c) Locate, evaluate and select suitable hardware on which the above software can be run.
- (d) Implement the system.

For more details of the above points, students are advised to refer to the study material Chapter-7, Section 7.2.2.

(b) Achieving systems development objectives:

- (1) Lack of senior management support 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.
- (2) Shifting user needs: User requirements for information technology are constantly changing. As these changes accelerate, there will be more requests for systems development and more development projects. When these changes occur during a development process, the development team may be faced with the challenge of developing systems whose very purposes have changed since the development process began.
- (3) 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.
- (4) 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.
- (5) Lack of standard project management and systems development methodologies: Some organisations do not formalise their project management and systems development methodologies, thereby making it very difficult to consistently complete projects on time or within budget.
- (6) Overworked or under-trained development staff: Estimates of the backlog of systems development work facing development staffs range up to 4 years!. 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, training plan and training budget do not exist.
- (7) 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" (or "rightsizing").
- (8) 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 reduce user resistance to change.

- (9) Inadequate testing and user training: New systems must be tested before installation to determine that they will operate correctly. Users must be trained to effectively utilise the new system.
- 7. (a) Input design consists of developing specifications and procedures for data preparation, developing steps which are necessary to put transactions data into a usable form for processing, and data-entry, i.e., the activity of putting the data into the computer for processing.

Many of the issues involved in input designs are:

- (1) Content: The analyst is required to consider the types of data that are needed to be gathered to generate the desired user outputs. This can be quite complicated because new systems often mean new information and new information often requires new sources of data. Sometimes, the data needed for a new system are not available within the organisation. Hence, the system designer has to prepare new documents for collecting such information.
- (2) Timeliness: In data processing, it is very important that data is inputted to computer in time because outputs cannot be produced until certain inputs are available. Hence, a plan must be established regarding when different types of inputs will enter the system. In transaction data processing, the people needing output are not the same who input most of the data. Hence, timeliness of input becomes more relevant for such systems.
- (3) Media: Another important input consideration includes the choice of input media and subsequently the devices on which to enter the data. Various user input alternatives available in the market include display workstations, magnetic tapes, magnetic disks, key-boards, optical character recognition, pen-based computers and voice input etc. A suitable medium may be selected depending on the application to be computerised.
- (4) Format: After the data contents and media requirements are determined, input formats are considered. While specifying the record formats, for instance, the type and length of each data field as well as any other special characteristics (number decimal places etc.) must be defined. However, designing input formats in mainframe and mini-computer database environments often require the assistance of a professional programmer or database administrator.
- (5) Input volume: Input volume refers to the amount of data that has to be entered in the computer system at any one time. In some decision-support systems and many real-time transaction processing systems, input volume is light. In batch-oriented transaction processing systems, input volume could be heavy which involves thousands of records that are handled by a centralised data entry department using key-to-tape or key-to-disk systems.
- (b) Information systems projects are designed with space, time and cost saving in mind. Hence, coding methods in which conditions, words or relationships are expressed by a code are developed to reduce input, control errors and to speed up the entire process. A code is a brief number, title or symbol used instead of lengthy or ambiguous description. Descriptions are particularly unsuited for computerised applications. They are usually far too long and would require much higher computer time for processing than the codes. Therefore, when an event occurs, the details of the event are summarised by the code. With code, fewer details are necessary in input but it results in no loss of information. The system analyst is responsible for devising an appropriate coding scheme. Some of the desired characteristics of a good coding scheme are enumerated below:
 - 1. Individuality
 - 2. Space
 - 3. Convenience

4. Expandability
5. Suggestiveness
6. Permanence.

For more details of the above points, students are advised to refer to the study material Chapter-8, Section 8.3.3.

8. (a) The following points may be considered while selecting a computer system :
 - (1) When selecting the new computer, the latest possible technology should be acquired. As long as this general principle is adhered to, the choice of a particular computer will not significantly affect the success of the computer effort.
 - (2) Computer performance for commercial work is mainly determined by the speed and capabilities of input/output and storage peripherals. Scientific, engineering and operations problems require good computational facilities. Thus, the efficiency of a computer in handling such problems will depend on the main storage available and the instruction execution speed, and repertoire. A comparison along these lines can be made quickly and quite effectively.
 - (3) The software supplied by the manufacturer may make a significant difference if it contains a package of special applicability to the jobs envisaged. In general, most manufacturers' packages are good. There are, of course, individual differences but these are usually not too important. The superiority of software may not be strong enough to influence a computer acquisition decision.
 - (4) Modern computers are marketed as series of compatible machines with increasingly powerful central processors and interchangeable peripherals. The choice of a computer really becomes a choice of a model within a series, based on a long-range plan of expansion. This however, means that one is dependent on the manufacturer and subject to his whims and fancies. But dependence is preferable to reprogramming which can be prohibitively expensive.
 - (5) The selection of a computer does not end within the choice of a manufacturer and a model. It continues to the selection of a configuration and a plan for its gradual expansion. This can be as important as the choice of manufacturer and a properly considered model can save a great deal of money. Outside assistance in computer selection can be had from computer manufacturers, Once, however, the vendor is selected, he can be counted upon to provide useful guidance for machine selection also.
- (b) A programs commonly involves the following six stages:
 - (1) Program Analysis: In this stage, for a particular application, the programmer ascertains the inputs available, the output required and to achieve that, what kind of processing is needed. Depending upon the complexity, the programmer then determines whether the proposed application can be or should be programmed at all. It is not unlikely that the proposal is shelved for modification on technical grounds.
 - (2) Program Design: Depending upon the main function to be performed, the programmer develops the general organisation of the program. The input, output, file layouts, flowcharts, and program specification etc. are provided to the programmer by the analyst.
 - (3) Program Coding: The logic of the program expressed in the flowchart is converted into program instructions. While coding, the syntax of the language used is to be kept in mind. The coded instructions are then entered into the magnetic media through available sources such as key to diskette. The program is then compiled through compiler of the language. Several syntax errors may crop up at this stage. These errors are required to be removed after getting the printed listing etc.

- (4) Debug the program: The meaning of debugging is to remove the errors so that the program may compile without errors. Many a times, structured walk through is to be adopted to remove the errors.

After debugging, the program is executed against test data. Several tests are performed and later the codes are reviewed to see whether these adhere to standards or not.

- (5) Program Documentation: The writing of narrative procedures and instructions for people who will use software is carried out throughout the program life cycle. Managers and users should carefully review documentation to ensure that the software and system behave as the documentation indicates. If they do not, documentation should be revised. Following technical design specifications are generally included:

- (i) A brief narrative description of what the program should do.
- (ii) A description of the output, inputs and processing to be performed by the program.
- (iii) A deadline for finishing the program.
- (iv) The identity of the programming languages to use along with coding standards to follow.
- (v) A description of the system environment into which the program should fit.
- (vi) A description of the testing required to certify the program for use.
- (vii) A description of documentation that must be generated for users, maintenance programmers and operational personnel.

The programmer writes the coding in the light of above documentation.

- (6) Program Maintenance: The requirements of business applications keep on changing and thus call for modification of various programs. The maintenance of the programs is generally done by people called maintenance programmers. The task of understanding the program written by some one and modifying the same is difficult. Therefore, the maintenance people should be involved from the beginning itself.

9. (a) Conversion includes all those activities which must be completed to successfully convert from the existing manual system to the computerized information system. Fundamentally these activities can be classified as follows:

- (1) Procedure conversion: Operating procedures should be completely documented for the new system. This applies to both computer operations and functional area operations. Before any parallel or conversion activities can start, operating procedures must be clearly spelled out for personnel in the functional areas undergoing changes. Information on input, data files, methods, procedures, outputs, and internal controls must be presented in clear, concise and understandable terms for the average reader. Written operating procedures must be supplemented by oral communication during the training sessions on the system change. Brief meetings must be held when changes are taking place in order to inform all operating employees of any changes initiated. Revisions to operating procedures should be issued as quickly as possible. These efforts enhance the chances of successful conversion.

Once the new system is completely operational, the system implementation group should spend several days checking with all supervisory personnel about their respective areas.

- (2) File conversion: Because large files of information must be converted from one medium to another, this phase should be started long before programming and testing are completed. The cost and related problems of file conversion are significant whether they involve on-line files (common data base) or off-line files. Present manual files are

likely to be inaccurate and incomplete where deviations from the accepted formats are common. Computer generated files tend to be more accurate and consistent.

In order for the conversion to be as accurate as possible, file conversion programs must be thoroughly tested. Adequate controls, such as record counts and control totals, should be the required output of the conversion program. The existing computer files should be kept for a period of time until sufficient files are accumulated for back-up. This is necessary in case the files must be reconstructed from scratch after a "bug" is discovered later in the conversion routine.

- (3) **System conversion:** After on-line and off-line files have been converted and the reliability of the new system has been confirmed for a functional area, daily processing can be shifted from the existing information system to the new one. A cut-off point is established so that data base and other data requirements can be updated to the cut-off point. All transactions initiated after this time are processed on the new system. System development team members should be present to assist and to answer any questions that might develop. Consideration should be given to operating the old system for some more time to permit checking and balancing the total results of both systems. All differences must be reconciled. If necessary, appropriate changes are made to the new system and its computer programs. The old system can be dropped as soon as the data processing group is satisfied with the new system's performance.
- (4) **Scheduling personnel and equipment:** Scheduling data processing operations of a new information system for the first time is a difficult task for the system manager. As users become more familiar with the new system, however, the job becomes more routine. Before the new design project is complete, it is often necessary to schedule the new equipment. Some programs will be operational while others will be in various stages of compiling and testing. Since production runs tend to push aside new program testing, the system manager must assign ample time for all individuals involved. Schedules should be set up by the system manager in conjunction with departmental managers of operational units serviced by the equipment.

Just as the equipment must be scheduled for its maximum utilisation, so must be personnel who operate the equipment. It is also imperative that personnel who enter input data and handle output data be included in the data processing schedule. Otherwise, data will not be available when the equipment needs it for processing.

- (5) **Alternative plans in case of equipment failure:** Alternative-processing plans must be implemented in case of equipment failure. Who or what caused the failure is not as important in case of equipment failure as the fact that the system is down. Priorities must be given to those jobs critical to an organization, such as billing, payroll, and inventory. Critical jobs can be performed manually until the equipment is set right.

Documentation of alternative plans is the responsibility of the computer section and should be fully covered by the organization's systems and procedures manual. It should state explicitly what the critical jobs are, how they are to be handled in case of equipment failure, where compatible equipment is located, who will be responsible for each area during downtime and what dead-lines must be met during the emergency. A written manual of procedures concerning what steps must be undertaken will help expedite the unfavorable situation. Otherwise, panic will result in the least efficient methods when time is of the essence.

- (b) 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 organised by vendor, and through hands-on learning techniques.

Training Systems Operators: Many systems depend on the computer centre personnel, who are fully 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 called for the installation of new equipment, such as new computer system, special terminals or data entry equipments, the operator's training should include such fundamentals as how to turn the equipment on and use it, knowledge of what constitutes 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 problems arise. Training also involves familiarization with run procedures, which involve working through the sequence of activities needed to use a new system on an ongoing basis.

User Training: User training may involve equipment use, particularly in the case where a microcomputer is in use and the individual involved is both operator and user. In these cases, users must be instructed first how to operate the equipment. User training must also instruct 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. Users should be trained on data handling activities such as editing data, formulating inquiries and deleting records of the data. From time to time, users will have to prepare disks, load papers into printers or change ribbons on printers. Some training time should be devoted to such system maintenance activities. If a microcomputer or data entry system uses disks, users should be instructed in formatting and testing disks.

10. An online, real time (OLRT) sales order processing system processes transactions as soon as they arrive, thus no delay occurs during computer processing.

This system may have point of sales order (POS) transaction recording and entry system where transactions are entered directly into the computer and recorded in a machine readable form in order to make it fully automated system. The flow diagram of the system is given on next page

Transactions & processing: The transactions such as customer order by telephone or through fax is being received. The salesperson who receives customer's orders immediately keys the transactions at a terminal as shown in the figure. Some of the events that take place in processing are listed below:

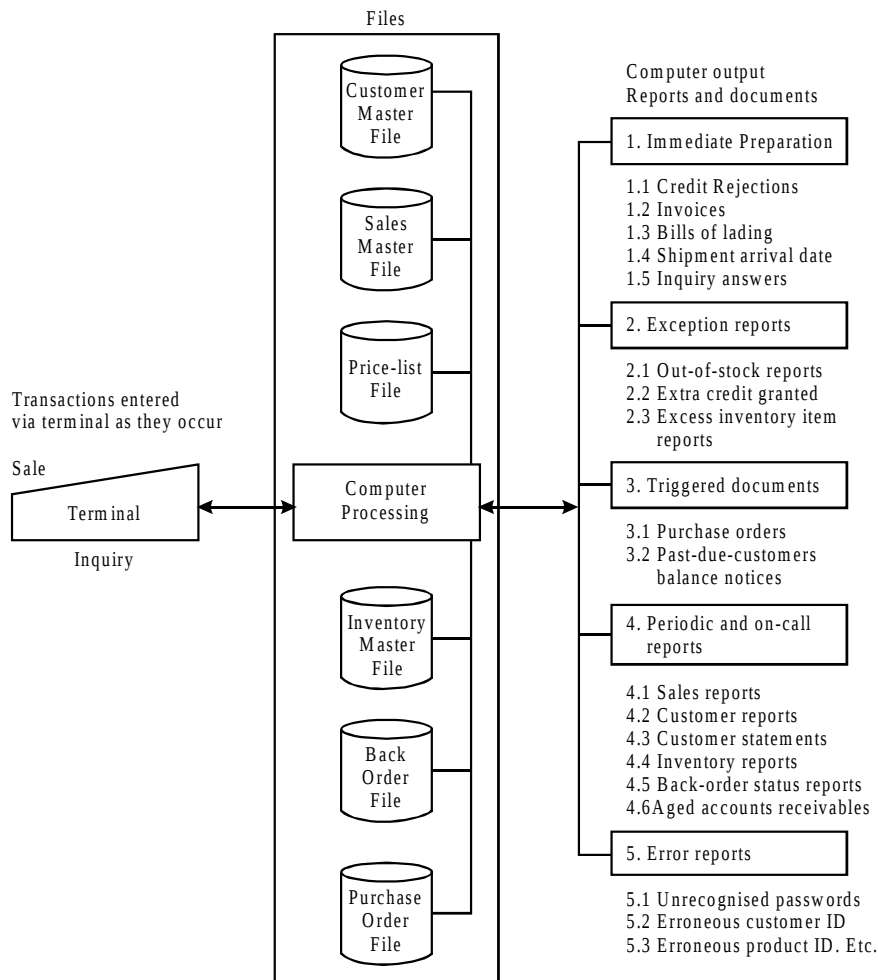
- (1) Type of transaction is identified by the transaction code entered by the sales person. Depending upon the code, the sales order processing computer program gets activated. The customers number, the item number and quantity are then entered.
- (2) The computer program checks the customer's account in the customer file & validates the customer number and determines his credit limit etc. Depending upon the company rules, the transaction is either accepted or cancelled.
- (3) The details of the product are checked from the inventory file and also the stock is checked. Depending upon the quantity available, either the supply is made or if there is insufficient quantity of a product, either the order is cancelled, or the salesman changes the order to the quantity available and backorders the addition items desired, according to the customer's wishes.

The communication is sent to the customer.

- (4) The computer program then seeks product pricing and quantity discount information from the price list and special "preferred customer" discount information, if any, from the customer file. According to the price etc, the bill is prepared.

- (5) All necessary reports etc. are then printed.

The transaction processing described above may occur within a minute or two after the transaction is originally entered, while the customer is still on the phone. In an OLRT system, the records can be kept current on a minute by minute basis.



Files: As shown in the figure, there are six random access files for OLRT application. These files have all necessary data for handling the sales to the customer online. These files are:

1. Customer master file — Contains records of the customers such as customer ID, name, address, credit limit etc.
2. Sales Master file — Sales information, such as to whom and what was sold, when etc.
3. Price list — Product number, unit price, quantity discount information
4. Inventory master file — Product no, quantity in store, reorder quantity, supplier code etc.
5. Backorder file — Customer id, product id, no of units ordered but not supplied
6. Purchase order file — Details about the purchase of items, due date of shipment

Report: Each of the reports shown in the figure can be produced at any location desired. Typically the credit rejection report, the inquiry answers, and the error reports are displayed or printed at the terminal from where the transaction is entered. Triggered reports occur when an

internal condition automates a programmed algorithm. For example, when the quantity of an item on hand drops below a reorder level, a purchase order may be printed.

11. (a) An Enterprise resource planning system is a fully integrated business management system covering functional areas of an enterprise like Logistics, Production, Finance, Accounting and Human Resources. It organizes and integrates operation processes and information flows to make optimum use of resources such as men, material, money and machine. ERP is a global, tightly integrated closed loop business solution package and is multifaceted.

In simple words, Enterprise resource planning promises one database, one application, and one user interface for the entire enterprise, where once disparate systems ruled manufacturing, distribution, finance and sales. Taking information from every function, it is a tool that assists employees and managers to plan, monitor and control the entire business. A modern ERP system enhances a manufacturer's ability to accurately schedule production, fully utilize capacity, reduce inventory, and meet promised shipping dates.

The following are some of the benefits that are achieved by implementing the ERP package:

- (1) 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.
 - (2) Reduces paper documents by providing on-line formats for quickly entering and retrieving information.
 - (3) Improves timeliness of information by permitting posting daily instead of monthly.
 - (4) Greater accuracy of information with detailed content, better presentation satisfactory for the auditors.
 - (5) Improved cost control.
 - (6) Faster response and follow-up on customers.
 - (7) More efficient cash collection, say, significant reduction in delay in payments by customers.
 - (8) Better monitoring and quicker resolution of queries.
 - (9) Enables quick response to change in business operations and market conditions.
 - (10) Helps to achieve competitive advantage by improving its business process.
 - (11) Improves supply-demand linkage with remote locations and branches in different countries.
 - (12) Provides a unified customer database usable by all applications.
 - (13) Improves International operations by supporting a variety of tax structures, invoicing schemes, multiple currencies, multiple period accounting and languages.
 - (14) Improves information access and management throughout the enterprise.
 - (15) Provides solution for problems like Y2K and Single Monetary Unit (SMU) or Euro Currency.
- (b) 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 organisation 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 organisation.

- (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 customisation.
 - (8) Training end users.
 - (9) Adapting the new system and making the required changes in the working environment to make effective use of the system in future.
12. (a) 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 equipments, security from water damage, safeguards from energy variation, pollution and unauthorized intrusion.

- (1) 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.
- (2) 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 that 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.
- (3) **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.
 - (4) **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.
 - (5) **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.
- (b) **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. The primary objective of a disaster recovery plan is to assure the management that normalcy would be restored in a set time after any disaster occurs, thereby minimizing 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:

- (1) **Emergency Plan:** This part of the Disaster Recovery Plan (DRP) outlines the actions to be undertaken immediately after a disaster occurs. It identifies the personnel to be notified immediately, for example, fire service, police, management, insurance company etc. It provides guidelines on shutting down the equipment, termination of power supply, removal of storage files and disks, if any. It sets out evacuation procedures like sounding the alarm bell, activating fire extinguishers, evacuation of personnel. It also provides return procedures as soon as the primary facility is ready for operation like backing up data files at off-site, deleting data from disk drives at third party's site, relocation of proper versions of backup files, etc.
- (2) **Recovery Plan:** This part of the DRP sets out how the full capabilities will be restored. A recovery committee is constituted. Preparing specifications of recovery like setting out priorities for recovery of application systems, hardware replacement etc. will be the responsibility of the Recovery Committee.

The following steps may be carried out under this plan:

- (i) An inventory of the hardware, application systems, system software, documentation etc., must be taken.
- (ii) Criticality of application systems to the organisation and the importance of their loss must be evaluated. An indication must be given of the efforts and cost involved in restoring the various application systems.

- (iii) The application systems hierarchy must be spelt out.
 - (iv) Selection of a disaster recovery site must be made. A reciprocal agreement with another organisation having compatible hardware and software could be made.
 - (v) A formal back agreement with another company must be made. This should cover the periodical exchange of information between the two sites regarding changes to hardware/software, the time and duration of systems availability, modalities of testing the plan etc.
- (3) **Back-up 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, standby must be kept with regard to the needs of particular computer environments. So far as the software is concerned, it is necessary to make copies of important programs, data files, operating systems and test programs etc. The backup copies must be kept in a place, which is not susceptible to the same hazards as the originals.
- (4) **Test plan:** This plan looks after the testing of DRP and analysis of the results. It identifies deficiencies in the emergency, backup or recovery plan. It contains procedures for conducting DRP testing like
- (i) **Paper walk-throughs:** It involves critical personnel in the plan's execution, reasoning out what might happen in the event of different disasters.
 - (ii) **Localised tests:** It simulates system crash. This test is performed on different aspects of DRP.
 - (iii) **Full operational test:** It is nearer to disaster conditions. Paper walkthrough and localised tests should have been conducted before completely shutting down the operations to simulate disasters.
13. The data collection component of the information system is responsible for bringing data into the system for processing. Input controls at this stage attempt to ensure that these transactions are valid, accurate, and complete. Input controls are divided into six broad classes. These control classes are not mutually exclusive divisions. Some control techniques could fit logically into more than one class.
- (1) **Source Document Controls:** In systems that use physical source documents to initiate transactions, careful control must be exercised over these instruments. Source document frauds can be used to remove assets from the organisation. To control against this type of exposure, the organisation must implement control procedures over source documents to account for each document, as described below:
 - (i) Use Pre-numbered Source Documents
 - (ii) Use Source Documents in Sequence
 - (ii) Periodically Audit Source Documents.
 - (2) **Data Coding Controls:** Coding controls are checks on the integrity of data codes used in processing. A customer's account number, an inventory item number, and a chart of accounts number are all examples of data codes. Three types of errors can corrupt a data code and cause processing errors: transcription, single transposition and multiple transposition. Check digit can be used to ensure integrity of the code in subsequent processing.
 - (3) **Batch Controls and hash totals:** They are an effective method of managing high volumes of transaction data through a system. The objective of batch controls is to reconcile output produced by the system with the input originally entered into the system. Batch controls ensure that all records in the batch are processed, no records are processed more than once, an audit trail of transactions is created from input through processing to the output

stage of the system. Hash total is a simple control technique that uses non-financial data to keep track of the records in a batch.

- (4) **Validation Controls:** Input validation controls are intended to detect errors in transaction data before the data are processed. Validation procedures are most effective when they are performed as close to the source of the transaction as possible. However, depending on the type of Computer Based Information Systems (CBISs) in use, input validation may occur at various points in the system. There are three levels of input validation controls:
 - (a) Field interrogation
 - (b) Record interrogation
 - (c) File interrogation
- (5) **Input error correction:** When errors are detected in a batch, they must be corrected and the records should be resubmitted for reprocessing. This must be a controlled process to ensure that errors are dealt with completely and correctly. There are three common error-handling techniques: (1) immediate correction, (2) create an error file, and (3) reject the entire batch.

For more details of the above points, students are advised to refer to the study material Chapter-14, Section 14.1.

14. (a) **Primary risk to the business organisations from computer frauds are:**
 - (1) **Internal threats:** There is an evidence that internal fraud is a greater risk to business than external fraud. One way to categorise computer frauds is to use the data processing model: input processor, computer instructions, stored data and output.
 - ◆ **Input:** The simplest and most common way to commit a fraud is to alter computer input, it requires little, if any, computer skills. It includes collusive frauds, disbursement frauds, payroll frauds, cash receipts frauds.
 - ◆ **Processor:** Computer frauds can be committed through unauthorised system use, including the theft of computer time and services.
 - ◆ **Computer Instructions:** Computer frauds can be accomplished by tampering with the software that processes company data. This may involve modifying the software, making illegal copies, or using it in an unauthorised manner. It might also involve developing a software program or module to carry out an unauthorized activity.
 - ◆ **Data:** Computer frauds can be perpetrated by altering or damaging a company's data files or by copying, using, or searching them without authorisation. There have been numerous instances of data files being scrambled, altered, or destroyed by disgruntled employees. Company data can also be stolen. Data can also be destroyed, changed, or defaced – particularly if stored on a company web site. One noted hacker stated that all companies that use the web, especially those with important trade secrets or valuable information technology assets, are under constant attack.
 - ◆ **Output:** Computer frauds can be carried out by stealing or misusing system output. System output is usually displayed on monitors or printed on paper. Unless properly safeguarded, monitor and printer output is subject to pry eyes and unauthorised copying.
 - ◆ **Malicious alterations of email:** This can happen when a employee has a grudge against another member of staff or management. The effects can be troublesome, if not damaging.

- (2) External threats: The dangers of hacking are well known. The main threats from hacking are:
 - (i) Removal of information;
 - (ii) Destruction of system integrity;
 - (iii) Interference with web pages;
 - (iv) Transmission of viruses by email;
 - (v) Interception of email;
 - (vi) Interception of electronic payments.
- (b) One way to deter fraud is to design a system with sufficient controls to make fraud difficult to perpetrate. These controls help to ensure the accuracy, integrity, and safety of system resources.
 - (1) Develop a Strong System of Internal Controls: The overall responsibility for a secure and adequately controlled system lies with top management. Managers typically delegate the design of adequate control systems to systems analysts, designers, and end users. The corporate information security officer and the operations staff are typically responsible for ensuring that control procedures are followed.
 - (2) Segregate Duties: There must be an adequate segregation of duties to prevent individuals from stealing assets and covering up their tracks.
 - (3) Require Vacations and Rotate Duties: Many fraud schemes, such as lapping and kiting, require the ongoing attention of the perpetrator. If mandatory vacations were coupled with a temporary rotation of duties, such ongoing fraud schemes would fall apart.
 - (4) Restrict Access to Computer Equipment and Data Files: Computer fraud can be reduced significantly if access to computer equipment and data files is restricted.. Physical access to computer equipment should be restricted, and legitimate users should be authenticated before they are allowed to use the system.
 - (5) Encrypt Data and Programs: Another way to protect data is to translate it into a secret code, thereby making it meaningless to anyone without the means to decipher it.
 - (6) Protect Telephone Lines: Computer hackers (called phreakers when they attack phone systems) use telephone lines to transmit viruses and to access, steal, and destroy data. One effective method to protect telephone lines is to attach an electronic lock and key to them. When a new phone system is installed, never use the default passwords as they are all published on the Internet. On established systems, change the passwords frequently.
 - (7) Protect the System from Viruses: A system can be protected from viruses. Fortunately, some very good virus protection programs are available. Virus protection programs are designed to remain in computer memory and search for viruses trying to infiltrate the system. When an infection attempt is detected, the software freezes the system and flashes a message to the user. Virus identification programs scan all executable programs to find and remove all known viruses from the system.
 - (8) Control Sensitive Data: To protect its sensitive data, a company should classify all of its data as to importance and confidentiality and then apply and enforce appropriate access restrictions. It should shred discarded paper documents. Controls can be placed over data files to prevent or discourage copying Sensitive and confidential information, backup tapes, and system documentation should be locked up at night and should not be left out on desks. Servers and PCs should also be locked when not in use. Companies should never store all of their data in one place or give an employee access to all of it. Local area networks can use dedicated servers that allow data to be

downloaded but never uploaded to avoid infection by a network computer. Closed-circuit televisions can be used to monitor areas where sensitive data or easily stolen assets are handled.

(9) Control Laptop Computers: Special care should be given to laptops because thieves are increasingly breaking into cars and hotel rooms to steal laptops for the confidential information they contain. To control laptops, companies should take following measures:

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

15. 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 tampering 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 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. It will also enable a person who has a public key to identify the originator of the message.

Section 5 of 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.
16. (a) Auditors involved in reviewing an information system should focus their concerns on the system's control aspects. They must look at the total systems environment not just the computerized segment. This requires their involvement from the time that a transaction is initiated until 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 (i.e. transactions) entered into the system and controls to ensure the integrity of those 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 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.
 - ◆ Developing detailed evaluation criteria so that it is possible to determine whether the implemented system has met predetermined specifications.
 - ◆ 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 (i.e. operational platforms) is compatible and controlled.
 - ◆ Databases are adequately designed and controlled to ensure that common definitions of data are used throughout the organization, that redundancy is eliminated or controlled and that data existing in multiple databases is updated concurrently.

This list affirms that the auditor is primarily concerned with adequate controls to safeguard the organization's assets.

- (b) It contains a framework for auditing computer security. It shows the following:
- (1) Types of security errors and frauds faced by companies: These include accidental or intentional damage to system assets; unauthorized access, disclosure, or modification of data and programs; theft; and interruption of crucial business activities.
 - (2) Control procedures to minimize security errors and fraud: These include developing an information security/protection plan, restricting physical and logical access, encrypting data, protecting against viruses, implementing firewalls, instituting data transmission controls, and preventing and recovering from system failures or disasters.
 - (3) Systems review audit procedures: These include inspecting computer sites; interviewing personnel; reviewing policies and procedures; and examining access logs, insurance policies, and the disaster recovery plan.

- (4) Tests of controls audit procedures: Auditors test security controls by observing procedures, verifying that controls are in place and work as intended, investigating errors or problems to ensure they were handled correctly, and examining any tests previously performed. The security breakdown was possible because of poor administrative controls and inadequate security software.
 - (5) Compensating controls: If security controls are seriously deficient, the organization faces substantial risks. Sound personnel policies and effective segregation of incompatible duties can partially compensate for poor computer security. Good user controls will also help, if user personnel can recognize unusual system output. However, it is unlikely that these controls can compensate indefinitely for poor computer security. Hence, auditors should strongly recommend that security weaknesses be corrected.
17. (a) To meet the security objectives, and develop and maintain adequate controls in compliance with generally accepted core principles, an ongoing and integrated approach is necessary. Executive management and especially chief executive officer support is essential for the successful development, design, implementation, and monitoring of security controls.
- (1) Security Policies: A good security policy should suggest procedures and policies that can prevent losses and also help in saving money and increasing productivity. A security policy defines ways in which resources in a computer system may be accessed and used. Security policies might differ depending upon the system under consideration.
 - (2) Policy Development: The security policy should support and complement existing organizational policies. The thrust of the policy statement must be to recognize the underlying value of, and dependence on, the information within an organization.
 - (3) Roles and Responsibilities: For security to be effective, it is imperative that individual roles, responsibilities, and authority are clearly communicated and understood by all. Since every organization will have its own unique needs, it is not possible to provide a generic approach. Organizations must assign security-related functions in the appropriate manner to nominated employees. Responsibilities to consider include: Executive Management, Information Systems Security Professionals, Data Owners, Process Owners, Technology providers, Users, Information Systems Auditors.
 - (4) Design: Once a policy has been approved by the governing body of the organization and related roles and responsibilities assigned, it is necessary to develop a security and control framework. This consists of standards, measures, practices, and procedures within which individual systems are then introduced and maintained. The process concludes with the design of an integrated security system that is compatible with the needs of the organization, given technical and cost constraints.
 - (5) Implementation: Once the design of the security standards, measures, practices and procedures has been approved, the solution should be implemented on a timely basis, and then maintained.
 - (6) Monitoring: Information systems are subject to a wide range of disruptive incidents of varying degrees of intensity. Preventive measures may not always be feasible or cost-effective to minimize loss, disclosure, damage, or disruption. Hence, monitoring measures need to be established to detect and ensure correction of security breaches, such that all actual and suspected breaches are promptly identified, investigated, and acted upon. This will also ensure ongoing compliance with policy, standards, and minimum acceptable security practices. The immediate benefit of instituting monitoring measures and procedures over systems, processes and their environment, is to promptly identify, contain damage, and expedite recovery.
 - (7) Awareness, Training, and Education: Awareness of the need to protect information, training in the skills needed to operate them securely, and education in security

measures and practices are of critical importance for the success of an organization's security program. The overriding benefits of awareness, training, and education, are in improving employee behavior and attitudes towards information security and in increasing the ability to hold employees accountable for their actions.

For more details of the above points, students are advised to refer to the study material Chapter-18, Section 18.5.

- (b) A security administrator is a person who is solely responsible for controlling and coordinating the activities pertaining all security aspects of the organisation. The security administrator performs the following functions.

- ◆ A security administrator attempts to ensure that the facilities in which systems are developed, implemented, maintained and operated are safe from threats that affect the continuity of installation and or result in loss of security.
- ◆ The security administrator sets policy, subject to board approval.
- ◆ He also investigates, monitors, advises employees, counsels management on matters pertaining to security.
- ◆ 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 are also stressed. He assigns responsibilities to job classifications and formulates what to be done in case of exceptions.
- ◆ The security administrator guides other information security administrators and users on the selection and application of security measures. He trains them on how to mark and handle processes, train security coordinators, select software security packages and solve problems

The security administrator also does the following:

- ◆ Investigates all security violations.
- ◆ Advises senior management on matters of information resource control.
- ◆ Consults on matters of information security.
- ◆ A security administrator also has the responsibility of conducting a security program, which is a series of ongoing, regular, periodic evaluations of the facilities available.
- ◆ A security administrator has to consider an extensive list of possible threats to the organisation, prepare an inventory of assets, evaluate the existing controls, implement new controls etc.

18. (a) CASE TOOLS are automated software tools. CASE stands for 'Computer Aided Software Engineering'. Software Engineering is concerned with creation of software systems. Software Systems are produced by teams of people using sound engineering principles. They use computing techniques and the aim is to produce automated tools to solve specific problems of users in the domain of their function such as Finance, Production, Sales, etc and also to develop and produce software for such applications.

There are three categories of CASE tools:

- (i) Tools that support individual process tasks such as checking the consistency of a design, compiling a program, comparing test results and so on.
- (ii) Work benches to support process phases such as specification, design etc. They consist of sets of tools with variable degree of integration.

- (iii) Environments support for all or part of software process. Includes several different work benches which are integrated in some way.

Figure below lists this classification:

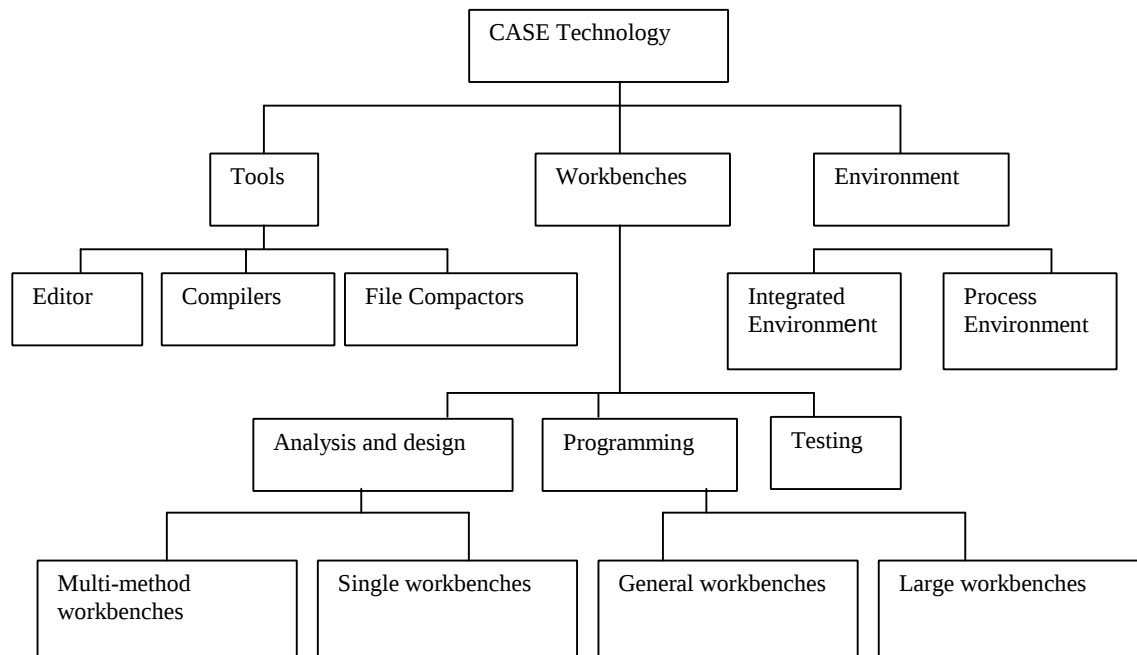
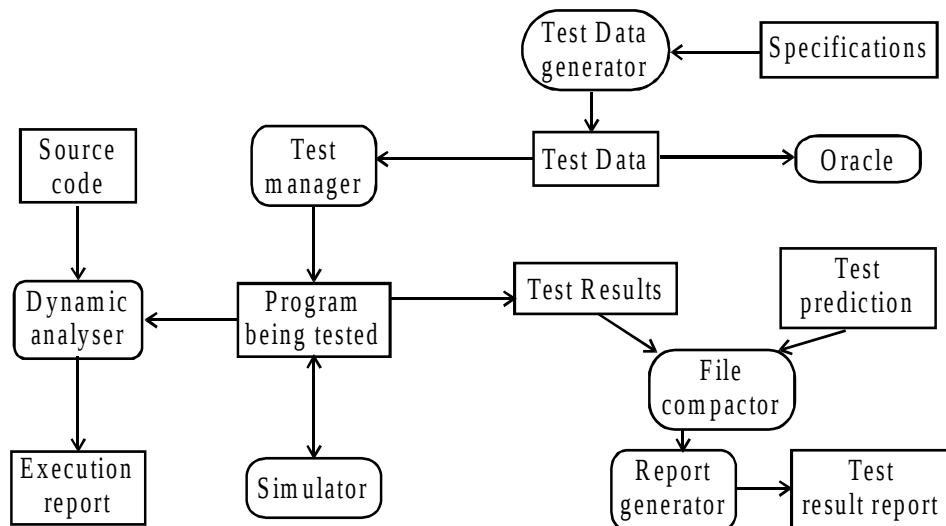


Table given below lists a number of different types of CASE tools and gives specific examples of each tool.

Tool type	Examples
Management tools	PERT tools, estimation tools
Editing tools	Text editors, diagram editors, word processors
Configuration management tools	Version management system, change management system
Prototyping tools	High level language tools, user interface generators
Method support tools	Design editors, data dictionaries, code generators
Language processing tools	Compilers, interpreters
Program analysis tools	Cross reference generators, static analyzers, dynamic analyzers
Testing tools	Test data generators, file compactors
Debugging tools	Interactive debugging system
Documentation tools	Page layout program, image editors
Reengineering tools	Cross reference systems, program restructuring systems

- (b) Testing workbenches are open systems which evolve to suit the needs of the system being tested. The tools which might be included in a testing workbenches are:
- (i) Test manager: Manages the running and reporting of program tests. This involves keeping track of test data, expected results, program facilities tested and so on.
 - (ii) Test data generator: Generates test data for the program to be tested. This may be accomplished by selecting data from a database or by using patterns to generate random data of the correct form.
 - (iii) Oracle: Generates predictions of expected results.
 - (iv) File Compactor: Compares the results of program tests with previous test results and reports differences between them.
 - (v) Report generator: Provides report definition and generation facilities for test results.
 - (vi) Dynamic Analyser: Adds code to a program to count the number of times each statement has been executed.
 - (vii) Simulators: Different kinds of simulators such as Target simulators, User Interface simulators, I/O simulators are available for simulation.



19. (a) Materials Requirement Planning: One approach to improve production efficiency is materials requirements planning (MRP.) MRP integrates several production related information systems so that the 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.

- (b) Expert Systems are designed to replace the need for a human expert. They are particularly important where expertise is scarce and therefore expensive. It is a software that expresses knowledge in terms of facts and rules. This knowledge will be in a specific area, and therefore expert systems are not general, as are most decision support systems which can be applied to the most of the scenarios.

Expert systems have arisen largely from academic research into artificial intelligence. The expert system should be able to learn, i.e. change or add new rules. They are developed using very different programming languages such as PROLOG which are referred to as fifth

generation languages, or expert systems shells which can make the process quicker and easier. It has been suggested that expert systems would be of greater use in the tactical and strategic level. This has been the case in banking, where expert systems scrutinise applications for loans, and lower level staff accepts the system's decision. This has replaced the somewhat subjective decision-making of more senior managers.

- (c) **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 that describe about the 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 types and range.
 - (ii) Identity of the source documents used to create the data.
 - (iii) Names of the computer files storing the data item.
 - (iv) Identity of individuals/programs permitted to access the data item for the purpose of file maintenance, upkeep or inquiry.
 - (v) Identity of programs/individuals not permitted to access the data item.
 - (vi) Names of the computer programs that modify the data item.

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.

- (d) **System Testing:** System testing must be conducted prior to installation of an information system. It involves: (a) preparation of realistic test data in accordance with the system test plan, (b) processing the test data using the new equipment, (c) thorough checking of the results of all system tests, and (d) reviewing the results with future users, operators and support personnel.

System level testing is a very good time for training employees in the operation of the Information Systems as well as maintaining it. One of the most effective ways to perform system-level testing is to perform parallel operations with the existing system. Parallel operations consist of feeding both systems the same input data and comparing data files and output results. The process of running dual operations for both new and old systems is more difficult for on-line processing systems than it is for a batch processing system, because the new system has no true counterpart in the old system.

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

During parallel operations, the mistakes detected are often not those of the new system, but of the old. It is the responsibility of the system developers and analysts to satisfy themselves that adequate time for dual operations has been undertaken for each functional area changed.

- (e) **Point-Scoring Analysis in Vendor Evaluation:** It is an approach for evaluating those accounting packages that meet most of a company's major requirements. To illustrate, assume that in the process of selecting an accounts payable system, an organisation finds three independent vendors whose packages appear to satisfy current needs. Table 1 shows the results of the analysis (Because the cost to purchase or lease each vendor's accounts

payable software package is about the same, “cost” is not an issue in this selection process).

Table-1

Software Evaluation Criteria	Possible points	Vendor A	Vendor B	Vendor C
Does the software meet all mandatory specifications?	10	7	9	6
Will program modifications, if any, be minimal to meet company needs?	10	8	9	7
Does the software contain adequate controls?	10	9	9	8
Is the performance (speed, accuracy, reliability, etc.) adequate?	10	7	9	6
Are other users satisfied with the software?	8	6	7	5
Is the software user-friendly?	10	7	8	6
Can the software be demonstrated and test-driven?	9	8	8	7
Does the software have an adequate warranty?	8	6	7	6
Is the software flexible and easily maintained?	8	5	7	5
Is online inquiry of files and records possible?	10	8	9	7
Will the vendor keep the software up to date?	<u>10</u>	<u>8</u>	<u>8</u>	<u>7</u>
Totals	103	79	90	70

When performing a point-scoring analysis, the evaluation committee first assigns potential points to each of the evaluation criteria based on its relative importance. After developing these selection criteria, the evaluation committee proceeds to rate each vendor or package, awarding points, as it deems fit. The highest point total determines the winner.

Although point-scoring analyses provide an objective means of selecting a final system, there are no absolute rules in the selection process, only guidelines for matching user needs with software capabilities. Thus, even for a small business, the evaluators must consider such issues as the company’s data processing needs, its in-house computer skills, vendor reputations, software costs, and so forth.

- (f) Bench marking problem for vendors’ proposals: Benchmarking problems for vendors’ proposals are sample programs that represent at least a part of the buyer’s primary computer work load. They include software considerations and can be current applications programs or new programs that have been designed to represent planned processing needs i.e. benchmarking problems are oriented towards testing whether a computer offered by the vendor meets the requirements of the job on hand of the buyer. They are required to be representative of the job mix of the buyer. Obviously, benchmarking problems can be applied only if job mix has been clearly specified. The benchmarking problems would then comprise long jobs, short jobs, printing jobs, disk jobs, mathematical problems, input and output loads etc., in proportion typical of the job mix. If the job is truly represented by the selected benchmarking problems, then this approach can provide a realistic and tangible basis for comparing all vendors’ proposals. Tests should enable buyer to effectively evaluate cross performance of various systems in terms of hardware performance (CPU and input/output units), compiler language and operating system capabilities, diagnostic messages, ability to deal with certain types of data structures and effectiveness of software utilities.

Benchmarking problems, however, suffer from a couple of disadvantages. It takes considerable time and effort to select problems representative of the job mix which itself must be precisely defined. It also requires the existence of operational hardware, software and services of systems. Nevertheless, this approach is very popular because it can test the functioning of vendors' proposal. The manager can extrapolate in the light of the results of benchmarking problems, the performance of the vendors' proposals on the entire job mix.

- (g) Personal Computer Controls: The capabilities, the 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: The security software provides log-on procedures which is available for PCs. Most of these programmes, however, become active only when the computer is booted from the hard drive. Disc 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, organizations need formal back up procedures.
 - (iii) Floppy disc backup: Dual internal hard drives, external hard drives and tape back up devices are also used.
 - (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.
- (h) Firewalls: Organizations connected to the Internet or other public networks often implement an electronic "firewall" to insulate their Intranet from outside intruders. A firewall is a system that enforces access control between two networks.

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's 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 provide 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 provide 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.

- (i) **Transaction Logs:** Every transaction successfully processed by the system should be recorded on a transaction log, which serves as a journal. Figure given on next page shows this arrangement. There are two reasons for creating a transaction log. First, the transaction log is a permanent record of transactions. The validated transaction file produced at the data input phase is usually a temporary file. Once processed, the records on this file are erased (scratched) to make room for the next batch of transactions. Second, not all of the records in the validated transaction file may be successfully processed. Some of these records may fail tests in the subsequent processing stages. A transaction log should contain only successful transactions – those that have changed account balances. Unsuccessful transactions should be placed in an error file. The transaction log and error files combined should account for all the transactions in the batch. The validated transaction file may then be scratched with no loss of data.
- (j) **Disc Imaging and Analysis Technique:** To reduce the risk to business from computer fraud computer forensic tools can be used. Disk imaging and analysis 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.