Notes on

Information Systems Control and Audit

January 15

2010

These notes are for students preparing for Paper 6 (New Course) of CA final examination conducted by the Institute of Chartered Accountants of India. To know how best a student can prepare for this subject, tips to score maximum marks, how to use these notes, etc. pls. read FAQ.pdf in the Files section at http://groups.yahoo.com/group/ISCAicai For queries/suggestions feel free to reach the author at nsshah@sjshah.in

[Past Exam Questions up to June 2009 covered]

Contents

1 - INFORMATION SYSTEMS CONCEPTS

1. System: A set of interrelated elements that operate collectively to accomplish some common purpose or goal.
Abstract system: Orderly arrangement of interdependent ideas or constructs. For example, a system of theology is an orderly arrangement of ideas about Good and the relationship of humans to God.
Physical system is a set of elements which operate together to accomplish an objective.

2. General model of a system: A general model of a physical system is input, process and output. This is, of course, very simplified because a system may have several inputs and outputs.

3. System Environment: 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.

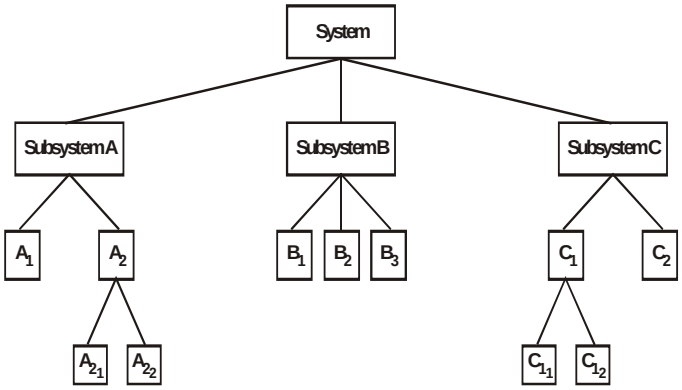
4. Boundary: The Features that define and delineate a system form its boundary. The system is inside the boundary; the environment is outside the boundary. It is fairly simple to define what is part of the system and what is not.

5. Subsystem: 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 subsystem being delineated by its boundaries.

6. Interfaces: The inter connections and interactions between the subsystem are termed interface. The number of inter connections if all sub- systems interact is in general n(n-1)/2 each inter connections is a potential interface for communication among subsystems.

7. Supra System: A supra system refers to the entity formed by a system and other equivalent systems with which it interacts (the system above it). For example, marketing may be viewed as a system that consists of elements such as market research, advertising, sales, and so on. 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.

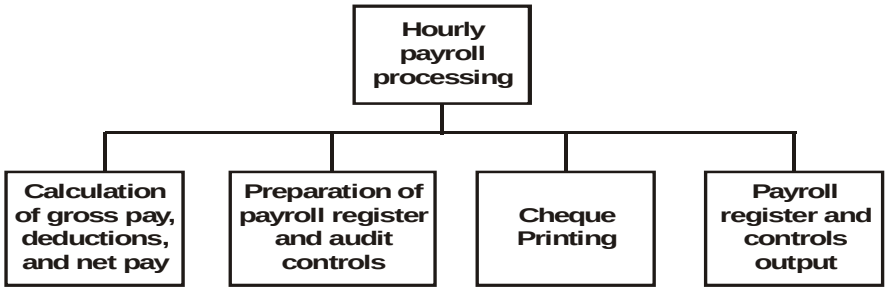
8. Decomposition: A complex system is difficult to comprehend when considered as a whole. Therefore, it is better that the system is decomposed or factored into sub systems. The boundaries and interfaces are defined, so that sum of the sub systems constitutes the entire system. This process of decomposition is continued with sub systems divided into smaller sub systems until the smallest sub systems are of manageable size. The sub systems resulting from this process generally form hierarchical structure as shown in the figure given below:



9. Hierarchical relations of subsystems:

An example of decomposition is the factoring of an information processing system into sub systems. One approach to decomposition might proceed as follows:

1. Information system divided into sub system such as:
   Sales and order entry
   Inventory
   Production
   Personnel and payroll
   Purchasing
   Accounting and control
   Planning
   Environmental intelligence
2. Each sub system is divided further into sub systems. For example, the personnel and payroll sub system might be divided into the following smaller sub systems:
   Creation and update of personnel pay roll records.
   Personnel reports
   Payroll data entry and validation
   Hourly payroll processing
   Salaried payroll processing
   Payroll reports for management
   Payroll reports for Government
3. If the task is to design and program a new system, the sub systems (major applications) defined above might be further sub divided into smaller sub systems or modules. For example, the hourly payroll processing sub system might be factored into modules as shown below:



Decomposition into sub systems is used to

A) Analyse an existing system and

B) To design and implement a new system.

In both the cases, the designer must decide how to factor i.e. where to draw the boundaries.

The general principle in decomposition, which assumes that system objectives dictate the process, is functional cohesion. Components are considered to be part of the same sub system if they perform or are related to the same function. The boundary then needs to be clearly specified, interfaces simplified and appropriate connections established among the subsystems.

10. Characteristics of a business system

Doing business is also a system with its components being marketing, manufacturing, sales, research, shipping, accounting and personnel. All these components work together with a common focus to create a profit that benefits the organization.

All systems have some common characteristics. These are as follows:

1) All systems work for predetermined objectives and the system is designed and developed accordingly.
2) In general a system has a number of interrelated and interdependent subsystems or components. No subsystem can function in isolation; it depends on other subsystems for its inputs.
3) If one subsystem or component of a system fails, in most cases the whole system does not work. However, it depends on how the subsystems are interrelated.
4) The way a subsystem works with another subsystem is called interaction. The different subsystems interact with each other to achieve the goal of the system
5) The work done by individual subsystems is integrated to achieve the central goal of the system. The goal of individual subsystem is of lower priority than the goal of the entire system.

11. NATURE AND TYPES OF SYSTEM

11.1 Computer-based business system and Manual system:

Manual system – where data collection, manipulation, maintenance and final reporting are carried out absolutely by human efforts.

Automated systems – where computers or microprocessors are used to carry out all the tasks mentioned above. However it will be wrong to say that a business system is 100% automated; rather, to some extent, it depends on manual intervention, may be in a negligible way. Computers made it possible to carry out processing which would have been either too difficult or too much time-consuming or even impossible to do manually.

11.1.1 Major areas of computer – based applications are:

1) Finance and Accounting: The main goal is to ensure financial viability of the organization, enforce financial discipline and plan and monitor the financial budget. Also it helps forecasting revenues, determining the best resources and uses of funds and managing other financial resources. Typical sub-application areas in finance and accounting are:
   - Financial accounting
   - General ledger
   - Accounts receivable/payable
   - Asset accounting
   - Investment management
   - Cash management
   - Treasury management
   - Fund management
   - Balance sheet
2) Marketing and Sales: The objective is to maximize sales and ensure customer satisfaction. It facilitates the chances of order procurement by marketing the products of the company, creating new customers and advertising the products. The sales department may use an order processing system to keep status and track of orders, generate bills for the orders executed and delivered to the customer. Servicing is an important function

of sales department. Strategies for rendering services during warranty period and beyond may be implemented by using a computer based system that uses a large database of customers. Analyzing the sales data by category such as by region, product, salesman or sales value helps the corporate managers take decisions in many crucial areas. The system may also be used to compute commissions for dealers or salesmen.

3) Production or Manufacturing: The objective of this subsystem is to optimally deploy man, machine and material to maximize production or service. The system generates production schedules and schedules of material requirements, monitors the product quality, plans for replacement or overhauling the machinery. It also helps in overhead cost control and waste control.
   A whole new discipline – Computer Aided Design and Computer Aided Manufacturing (CAD / CAM) has evolved due to application of IT and using this technology quick change in design and manufacturing process is possible to examine the possibilities of various alternatives.
4) Inventory/Stores Management: The inventory management system is designed with a view to keeping track of materials in the stores. The system is used to regulate the maximum and minimum level of stocks, raise alarm at danger level stock of any material, give timely alert for re-ordering of materials with optimal re-order quantity and facilitate various queries about inventory like total inventory value at any time, identification of important items in terms stock value (ABC analysis), identification most frequently moving items (XYZ analysis) etc.
5) Human resource management: Human resource management system aims to achieve less disputes, right utilization of manpower and quiet environment that will ensure smooth sailing in business. Skill database maintained in HRM system, with details of qualifications, training, experience, interests etc helps management for allocating manpower to right activity at the time of need or starting a new project. This system also keeps track of employees' output or efficiency. Administrative functions like keeping track of leave records or handling other related functions are also included HRM system. An HRM system may have the following modules
   − Personnel administration
   − Recruitment management
   − Travel management
   − Benefit administration
   − Salary administration
   − Promotion management
   An ideal HR development emphasizes an optimal utilization of human resource by introducing a consistent and coherent policy aiming at promoting commitment to the enterprise.

11.1.2 The reasons for using computer in business area:

- Handling huge volume of data that is not manageable by human efforts.
- Storing enormous volume of data for indefinite period without any decay.
- Quick and accurate processing of data to match the competitive environment.
- Quick retrieval of information on query.
- Quick and efficient transportation of data/information to distant places almost at no cost.
- Availability of software tools for quick decision making in a complex situation.

11.2 Closed and open systems:

Closed Systems: A closed system is self contained and does not interact or make exchange across its boundaries with its environment. Closed systems do not get the feedback they need from the external environment and tend to deteriorate eventually. For example, if a marketing system does not get feedback from the market, its efficiency will gradually continue to decrease.

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

Open Systems: Open systems actively interact with their environment. Such systems regularly get inputs and give outputs to its environment. These systems are also subject to unknown inputs and environmental disturbances. Open

systems are also able to adapt to environmental changes for their survival and growth. Business organization is an example of such system.

11.3 Deterministic and Probabilistic system:

Deterministic system: A deterministic system operates in a predictable manner. The interaction among the parts is known with certainty. If one has a description of the state of the system at a given point in time plus a description of its operation, the next state of the system may be given exactly, without error. An example is a correct computer program, which performs exactly according to a set of instructions.

Probabilistic system: The probabilistic system can be described in terms of probable behaviour, but a certain degree of error is always attached to the prediction of what the system will do. An inventory system is an example of a probabilistic system. The average demand, average time for replenishment, etc, may be defined, but the exact value at any given time is not known. Another example is a set of instructions given to a human who, for a variety of reasons, may not follow the instructions exactly as given.

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

Information is the substance on which business decision are based. Therefore, the quality of information determines the quality of action or decision. The management plays the part of converting the information into action through the familiar process of decision-making. Information has come to occupy a very important position in the survival of a business.

12.1 Characteristics of Information: The important characteristics of useful and effective information are as follows:

(i) **Timeliness:** Timeliness refers to when user needs information. Some information is required on regular, periodic basis while other information is generated on the request of the manager.

(ii) **Purpose:** Information must have purposes at the time it is transmitted to a person or machine, The basic purpose of information is to inform, evaluate, persuade and organize. It helps in creating new concepts, identifying problems, solving problems, decision making, planning and controlling.

(iii) **Mode and Format:** The mode of communicating information in business are either visual, verbal or in written form. Format of information should be so designed that it assists in decision-making, solving problems, planning, controlling and searching. Also the data should be classified into categories, which have relevance to the problem at hand.

(iv) **Redundancy:** It means the excess of information carried per unit of data. However, in business situation redundancy may sometime be necessary to safeguard against error in the communication process.

(v) **Rate:** The rate of transmission/reception of information may be represented by the time required to understand a particular situation. Quantitatively, the rate for humans may be measured by the number of numeric characters transmitted per minute. For machines, the rate may be based on the number of bits of information per character per unit of time.

(vi) **Frequency:** The frequency with which information is transmitted or received affects its value. Frequency has some relationship with the level of management and with operational needs. For example, at the level of foreman it should be on weekly basis but at the management level, it should be usually on monthly basis.

(vii) **Completeness:** The information should be as complete as possible. For example, net present value models provide a point estimate and do not give any indication of the range within which these estimates may vary. Thus, complete information helps the manager to arrive at better decisions.

(viii) **Reliability:** In statistical surveys, for example, the information that is arrived at should have an indication of the confidence level. Even otherwise also, information should be reliable.

(ix) **Cost benefit analysis:** The benefits that are derived from the information must justify the cost incurred in

procuring information. The information may be categorised into four categories:

(i) absolutely essential statements: Cannot be discontinued whatever be the cost of preparing them necessary

(ii) necessary statements: may have a high cost but may be discontinued only in very stringent circumstances

(iii) normal statements: may be discontinued or replaced if their costs are too high

(iv) extra statements: may be prepared only if the benefits arising out of them are substantially higher than the costs involved

(x) **Validity:** It measures the closeness of the information to the purpose, which it purports to serve. The measures suiting the organisation may have to be carefully selected or evolved.

(xi) **Quality:** It refers to the correctness of information, which is likely to be spoiled by personal bias. Hence, proper internal controls and procedures should be developed.

12.2 INFORMATION SYSTEM AND ITS ROLE IN MANAGEMENT

An *information system* can be considered as an arrangement of a number of elements that provides effective information for decision-making and / or control of some functionalities of an organization. Information is an entity that reduces uncertainty about an event or situation. For example, correct information about demand of products in the market will reduce the uncertainty of production schedule. Enterprises use information system to reduce costs, control wastes or generate revenue. Some of important implications of information system in business are as follows:

(1) Effective decision-making to achieve the organizational goal.

(2) Gain edge in the competitive environment.

(3) Help take right decision at the right time.

(4) Innovative ideas for solving critical problems.

(5) Knowledge gathered though information system may be utilized by managers in unusual situations.

(6) If information system is viewed as a process it can be integrated to formulate a strategy of action or operation.

12.3 Factors on which Information requirements Depend

The factors on which information requirements of executives depend are:

1. Operational function.
2. Type of decision making.
3. Level of management activity.

(1) Operational function: The grouping or clustering of several functional units on the basis of related activities into a sub-systems is termed as operational function. For example, in a business enterprise, marketing is an operational function, as it is the clustering of several functional units like market research, advertising, sales analysis and so on. Likewise production finance, personnel etc. can all be considered as operational functions. In fact, the content of information depends upon the activities performed under an operational function. For example, in the case of production, the information required may be about the production targets to be achieved, resources available and so on. Whereas in the case of marketing functions, the content of information may be about the consumer behaviour, new product impact in the market etc. The characteristics which must be possessed by a particular information too are influenced by an operational function. For example, the information required by accounts department for preparing payroll of the employees should be highly accurate.

(2) Type of decision making: Organisational decisions can be categorised as programmed and non-programmed ones.

Programmed decisions or structured decisions: Decision which are of repetitive and routine nature are known as programmed decisions. For example, preparation of payroll and disbursement of pay through bank account for taking such decisions, guidelines and rules required are provided in the form of procedure manual.

Non-programmed decisions or unstructured decisions are those which are made on situations and problems which are novel and non-repetitive and about which not much knowledge and information are available. They are non-programmed in the sense that they are made not by reference to any pre-determined guidelines, standard operating procedures, precedents and rules but by application of managerial intelligence, experience, judgement and vision to

tackling problems and situations, which arise infrequently and about which not much is known.

(3) Level of management activity : Different levels of management activities in management planning and control hierarchy are–Strategic level, tactical level and operational level.

Strategic Level or Top level : Strategic level management is concerned with developing of organisational mission, objectives and strategies. Decisions made at this level of organization to handle problems critical to the survival and success of the organisation are called strategic decisions.

Tactical Level or middle level: Tactical level lies in middle of managerial hierarchy. At this level, managers plan, organise, lead and control the activities of other managers. Decisions made at this level called the tactical decisions (which are also called operational decisions) are made to implement strategic decisions. A single strategic decision calls for a series of tactical decisions, which are of a relatively structured nature. Tactical decisions are relatively short, step-like spot solutions to breakdown strategic decisions into implementable packages.

Supervisory or operational Level: This is the lowest level in managerial hierarchy. The managers at this level coordinate the work of others who are not themselves managers. They ensure that specific tasks are carried out effectively and efficiently.

12.4 Types of Information

Information, broadly, can be divided into two different types – internal information and external information in the context of business organizations.

Examples of internal and external - required at every one of the levels of management are stated below:

Information requirement at TOP LEVEL for making decision

External	Internal
Competitive Activities	Historical-sales, costs
Customer preferences, style, changes	Profit, cash flow, divisional, income, sales, expenses.
Economic trends	Financial ratios, interests; credit outstanding, long-term debt, delinquent accounts.
Technological changes, legal rulings	Projects' progress reports and cost updates.

Information requirement at MIDDLE LEVEL for making decision

External	Internal
Price changes; shortages	Descriptive information (happenings)
Demand or supply, credit conditions.	Current performance indicators.
	Over-under budgets.

Information requirement at LOWER LEVEL for making decision

External	Internal

Sensitive changes affecting material supplies and sales.	Unit sales and expenses Current performances. Shortages and bottle-necks Operating efficiencies and inefficiencies. Input-output ratios. Maintenance reports.

13. Information Systems at Different Levels of Management:

13.1 Transaction Processing System (TPS)

TPS at the lowest level of management is an information system that manipulates data from business transactions. Any business activity such as sales, purchase, production, delivery, payments or receipts involves transaction and these transactions are to be organized and manipulated to generate various information products for external use. For example, selling of a product to a customer will give rise to the need of further information like customer billing, inventory status and increase in account receivable balance. Transaction processing system will thus record and manipulate transaction data into usable information. Typically, a TPS involves the following activities:

(i) Capturing data to organize in files or databases.

(ii) Processing of files / databases using application software.

(iii) Generating information in the form of reports.

(iv) Processing of queries from various quarters of the organization.

A transaction processing system may follow periodic data preparation and batch processing (as in payroll application) or on-line processing (as in inventory control application). Both approaches have their merits and demerits. However in industries and business houses now-a-days on-line approach is preferred in many applications as it provides information with up-to date status. It is to be noted that the people who participate in Transaction processing system usually are not in a position to take any management decision.

13.2 Management Information System (MIS): Many experts have defined MIS in different languages. But the central theme of all these definitions is same. A Management Information System has been defined by Davis and Olson as ' *an integrated user-machine system designed for providing information to support operational control, management control and decision making functions in an organization'.*

MIS comprises of three elements viz., management, information and system. The concept of MIS is better understood if each element of the term MIS is defined separately.

Management: A manager may be required to perform following activities in an organisation:

(i) Determination of organisational objectives and developing plans to achieve them.

(ii) Securing and organising human beings and physical resources so as to achieve the laid down objectives.

(iii) Exercising adequate controls over the functions performed at the lower level.

(iv) Monitoring the results to ensure that accomplishments are proceeding according to plans.

Thus, management comprises of the processes or activities that describe what managers do while working in their organisation. They in fact plan, organise, initiate, and control operations. In other words, management refers to a set of functions and processes designed to initiate and co-ordinate group efforts in an organised setting directed towards promotion of certain interests, preserving certain values and pursuing certain goals. It involves mobilisation, combination, allocation and utilisation of physical, human and other needed resources in a judicious manner by employing appropriate skills, approaches and techniques.

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

determines the quality of action or decision. The management plays the part of converting the information into action through the familiar process of decision-making. Information has come to occupy a very important position in the survival of a business.

System: System may be defined as a composite entity consisting of a number of elements which are interdependent and interacting, operating together for the accomplishment of an objective. One can find many examples of a system. Human body is a system, consisting of various parts such as head, heart, hands, legs and so on. The various body parts are related by means of connecting networks of blood vessels and nerves. This system has a main goal which we may call "living". Thus, a system can be described by specifying its parts, the way in which they are related, and the goals which they are expected to achieve. A business is also a system where economic resources such as people, money, material, machines, etc. are transformed by various organisation processes (such as production, marketing, finance, etc.) into goods and services.

Thus, MIS can be defined as a network of information that supports management decision making. The role of MIS is to recognise information as a resource and then use it for effective and timely achievement of organisational objectives.

13.2.1 Characteristics of an effective MIS : Important characteristic for an effective MIS are eight in number and are briefly discussed below :

1. Management oriented: It means that effort for the development of the information system should start from an appraisal of management needs and overall business objectives.

2. Management directed: Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts. Mere one time involvement is not enough. For system's effectiveness, it is necessary for management to devote their sufficient time not only at the stage of designing the system but for its review as well, to ensure that the implemented system meets the specifications of the designed system.

3. Integrated: Development of information should be an integrated one. It means that all the functional and operational information sub-system should be tied together into one entity. An integrated information system has the capability of generating more meaningful information to management. The word integration here means taking a comprehensive view or a complete look at the interlocking sub-systems that operate within a company.

4. Common data flows: It means the use of common input, processing and output procedures and media whenever possible is desirable. Data is captured by system analysts only once and as close to its original source as possible. They, then, try to utilise a minimum of data processing procedures and sub-systems to process the data and strive to minimise the number of output documents and reports produced by the system. However, some duplication is necessary in order to insure effective information system.

5. Heavy planning element: An MIS usually takes 3 to 5 years and sometimes even longer period to get established firmly within a company. Therefore, a heavy planning element must be present in MIS development. The designer must avoid the possibility of system obsolescence before the system gets into operation.

6. Sub system concept: Even though the information system is viewed as a single entity, it must be broken down into digestible sub-systems which can be implemented one at a time by developing a phasing plan. The breaking down of MIS into meaningful subsystems sets the stage for this phasing plan.

7. Common database: Database is the mortar that holds the functional systems together. It is defined as a "superfile" which consolidates and integrates data records formerly stored in many separate data files. The organisation of a database allows it to be accessed by several information sub-systems and thus, eliminates the necessity of duplication in data storage, updating, deletion and protection. Although it is possible to achieve the basic objectives of MIS without a common database, thus paying the price of duplicate storage and duplicate file updating, database is a definite characteristic of MIS.

8. Computerised: It is possible to have MIS without using a computer. But use of computers increases the effectiveness of the system. In fact, its use equips the system to handle a wide variety of applications by providing their information requirements quickly. Other necessary attributes of the computer to MIS are accuracy and consistency in processing data and reduction in clerical staff. These attributes make computer a prime requirement in management information system.

13.2.2 Misconceptions or Myths about MIS:

1. The study of management information system is about the use of computers. This statement is not true. MIS may or may not be computer based, computer is just a tool, just take any other machine. Installing a MIS depends largely on several factors such as, how critical is the response time required for getting an information; how big is the organisation, and how complex are the needs of the information processing.

2. More data in reports means more information for managers : This is a misapprehension. It is not the quantity of data, but its relevance, which is important to managers in process of decision-making. Data provided in reports should meet information requirements of managers. It is the form of data and its manner of presentation that is of importance to business managers. Unorganised mass of data creates confusion.

3. Accuracy in reporting is of vital importance : The popular belief is that accuracy in reporting should be of high order. At the operating level, it is true. Other examples, where accuracy is really important, can be the dispensing of medicine; the control of aircraft; the design of a bridge etc. Accuracy, however, is a relevant but not an absolute ideal. Higher levels of accuracy involve higher cost. At higher decision levels, great accuracy may not be required. The degree of accuracy is closely related to the decision problem. Higher management is concerned with broad decisions on principles and objectives. A fairly correct presentation of relevant data often is adequate for top management decisions. For a decision on a new project proposal, top management is not interested in knowing the project cost in precise rupee terms. A project cost estimated at a fairly correct figure is all what it wants.

13.2.3 Pre-requisites of an MIS – The following are pre-requisites of an effective MIS:

(i) **Database –** It is 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. Normally, the database is subdivided into major information sub-sets needed to run. The database should be user-oriented, capable of being used as a common data source, available to authorized persons only and should be controlled by a separate authority such as DBMS.

(ii) **Qualified System and Management Staff -** MIS should be manned by qualified officers. These officers who are experts in the field should understand clearly the views of their fellow officers. The organizational management base should comprise of two categories of officers (i) System and Computer experts and (ii) Management experts. Management experts should clearly understand the concepts and operations of a computer. Their whole hearted support and cooperation will help in making MIS an effective one.

(iii) **Support of Top Management -** An MIS becomes effective only if it receives the full support of top management. To gain the support of top management, the officer should place before them all the supporting facts and state clearly the benefits which will accrue from it to the concern. This step will certainly enlighten the management and will change their attitude towards MIS.

(iv) **Control and Maintenance of MIS –** Control of the MIS means the operation of the system as it was designed to operate. Sometimes users develop their own procedures or shortcut methods to use the system, which reduces its effectiveness. To check such habits of users, the management at each level in the organisation should device checks for the information system control.

Maintenance is closely related to control. There are times when the need for improvements to the system will be discovered. Formal methods for changing and documenting changes must be provided.

(v) **Evaluation of MIS** – An effective MIS should be capable of meeting the information requirements of its executives in future as well. The capability can be maintained by evaluating the MIS and taking appropriate timely action. The evaluation of MIS should take into account the following points:

- Examining the flexibility to cope with future requirements ;
- Ascertaining the view of the users and designers about the capabilities and deficiencies of the system ;
- Guiding the appropriate authority about the steps to be taken to maintain effectiveness of MIS.

13.2.4 Constrains in Operating a MIS:

1. **Non availability of qualified staff:** The most important requirement for operating an effective MIS is that of qualified system and management staff. These officers should understand the views of their fellow officers. Moreover, experts should be capable of understanding the objectives of the organization and provide a desired direction for installing and operating system. This problem may be overcome by grooming internal staff. The grooming of staff should be preceded by proper selection and training.
2. **Selection of Sub system of MIS:** Experts usually face the problem of selecting the sub system of MIS to be installed and operated upon. This constraint could be overcome by identifying the need and importance of the function for which MIS can be installed first.
3. **Non Cooperation from staff:** This is a very crucial problem. It should be handled carefully and tactfully. This problem may be solved by educating the staff about the utility of MIS. The task should be carried out by organizing lectures, showing films and explaining the utility of the system. Besides this, some persons from staff should also be involved in the development and implementation of the system.
4. **High turnover of MIS experts:** High turnover is on account of several factors such as pay packet, promotion chances, future prospects, behaviour of top managers etc. This problem can be handled by creating the better working conditions and paying at least at par with similar *organizations*.
5. **Non-standardised approach:** Due to varied objectives of the business organizations, the approach adopted by experts for designing and implementing MIS is a non standardized one. Though in this regard, nothing can be done at the initial stage, but by and by standardization may be arrived at, for the organizations in the same industry.
6. **Difficulty in quantifying the benefits of MIS:** Due to the difficulties in quantifying the benefits of MIS, the justification of the cost involved is difficult. Therefore, this raises the questions by departmental managers about the utility of MIS. They forget that MIS is a tool which is essential to fight out competition and the state of uncertainty that surrounds business today. This constraint can be resolved by educating the top managers and telling them about the advantages of MIS. Moreover, the example from similar industries could be brought to the notice of top executives which are having better profits.

13.2.5 Effects of using computer in MIS:-

(i) ***Speed of processing and retrieval of data increases*:** Computer with its unbelievably fast computational capability and systematic storage of information with random access facility has emerged as an answer to the problems of providing relevant information with minimal loss of time. The speed of computer processing is in new range i.e. an operation takes only billionths of a second. This characteristic of computer has accounted for as a major factor in inducing MIS development.

(ii) ***Scope of use of information system has expanded:*** System experts in business organizations developed areas and functions, where computerized MIS could be used to improve the working of the concern. These types of applications are not feasible under the manual system. For example, online systems can provide information to various users sitting at a remote distance from a centrally located computer system.

(iii) ***Scope of analysis widened:*** The use of computer can provide multiple type of information accurately and in no time to decision makers. Such information equips an executive to carry out a thorough analysis of the problems and to arrive at the final decision. Computer is capable of providing various types of sales reports, which are useful in analyzing the sales department working and to ascertain their weakness so that adequate measures may be taken in time.

(iv) ***Complexity of system design and operation increased:*** The need for highly processed and sophisticated information based on multitudes of variables has made the designing of the system quite complex.

(v) ***Integrates the working of different information subsystem:*** There are number of subsystems like production, material, marketing, finance, engineering and personnel which constitute MIS. Each of these sub systems are required to provide information to support operational control, management control and strategic planning. Such information may be available from a common data base which meets the information requirements of different information sub system by utilizing the services of computers for storage, processing, analyzing and providing such

information as and when required.

(vi) ***Increases the effectiveness of Information Systems:*** Before the existence of computer technology, it was difficult to provide the relevant information to business executives in time even after incurring huge expenses. The use of computer technology has overcome this problem, by providing timely, accurate and desired information for the purpose of decision-making.

(vii) ***More comprehensive information:*** The use of computer for MIS enabled system expert to provide more comprehensive information to executives on business matters.

13.2.6 Limitations of the Management Information System:

(i) MIS is not a substitute for effective management. It cannot replace managerial judgement in making decisions in different functional areas.

(ii) MIS may not have requisite flexibility to quickly update itself with changing needs of time.

(iii) MIS cannot provide tailor-made information packages suitable for the purpose of every type of decision made by executives.

(iv) MIS takes into account mainly quantitative factors, thus it ignores the non-quantitative factors like morale and attitude of members of the organization.

(v) MIS is less useful for making non-programmed decisions.

(vi) The effectiveness of MIS decreases due to frequent changes in top managements, organisational structure and operational team.

(vii) MIS effectiveness is reduced where culture of hoarding information and not sharing with others exists.

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

13.3 Decision Support Systems (DSS):

A decision support system (DSS) can be defined as a system that provides tools to managers to assist them in solving semistructured and unstructured problems in their own, somewhat personalized, way. Often, some type of modeling environment perhaps a very simple environment such as the one accompanying a spreadsheet package is involved. A DSS is not intended to make decisions for managers, but rather to provide managers with a set of capabilities that enables them to generate the information required by them in making decisions. In other words, *a DSS supports the human decision-making process, rather than providing a means to replace it.*

13.3.1 DSS GOALS AND APPLICATIONS

The decision support systems are characterised by at least three properties:

(1) They support semistructured or unstructured decision-making.

(2) They are flexible enough to respond to the changing needs of decision makers, and

(3) They are easy to use.

We will now briefly discuss each of the above mentioned characteristics.

(i) Semi-structured / Unstructured decisions – Structured decisions are those that are easily made from a given set of inputs. Unstructured decisions and semi-structured decisions are decisions for which information obtained from a computer system is only a portion of the total knowledge needed to make the decision. The DSS is particularly well adapted to help with semi-structured / unstructured decisions. In DSS, the problem is first defined and formulated. It is then modelled with DSS software. The model is run on the computer to provide results. The modeller, in reviewing these results, might decide to completely reformulate the problem, refine the model, or use the model to obtain other results.

(ii) Ability to adapt to changing need – Semi-structured / unstructured decisions often do not conform to a predefined set of decisions-making rules. Because of this, their decision support system must provide for enough flexibility to enable users to model their own information needs. The DSS designer understands that managers usually do not know in advance what information they need and, even if they do, those information

needs keep changing constantly. Thus, rather than locking the system into rigid information producing requirements, capabilities and tools are provided by DSS to enable users to meet their own output needs.

(iii) Ease of Learning and Use - Since decision support systems are often built and operated by users rather than by computer professionals, the tools that company possesses should be relatively easy to learn and use. Such software tools employ user-oriented interfaces such as grid, graphics, non-procedural 4GL and easily read documentation. These interfaces make it easier for user to conceptualise and perform the decision making process.

13.3.2 COMPONENTS OF A DSS:

A decision support system has four basic components: (1) the user, (2) one or more databases, (3) a planning language, and (4) the model base

(i) **The User:** The user of a decision support system is usually a manager with an unstructured or semi-structured problem to solve. Users do not need a computer background to use a decision support system for problem solving. The most important knowledge is a thorough understanding of the problem and the factors to be considered in finding a solution. A user does not need extensive education in computer programming in part because a special planning language performs the communication function within the decision support system.

(ii) **One or more databases:** Decision support systems include one or more databases which contain both routine and non-routine data from both internal and external sources. The data from external sources include data about the operating environment surrounding an organization. Decision support system users may construct additional database themselves. Some of the data may come from internal source.

(iii) **A planning language:** Two types of planning languages that are commonly used in decision support system are (1) general purpose planning languages and (2) special purpose planning languages. General purpose planning languages allow users to perform many routine tasks like-retrieving various data from a database or performing statistical analysis. The languages in most electronic spreadsheets are good example of general purpose planning languages. These languages enable the user to tackle a broad range of budgeting, forecasting and other worksheet oriented problems. Special purpose planning languages are more limited. Some statistical languages, such as SAS, SPSS and Minitab are examples of special purpose planning languages.

(iv) **Model Base:** The model base is the "brain" of the decision support system because it performs data manipulation and computations with the data provided to it by the user and the database. There are many types of model bases but most of them are custom-developed models that do some type of mathematical functions. The analysis provided by the routine in the model base is the key to supporting the user's decision.

13.3.3 The tools of decision support systems

The tools of decision support include a variety of software supporting database query, modeling, data analysis, and display. These tools falling into these four categories

1) **Database Languages :** Tools supporting database query and report generation use mainframe, minicomputer, and microcomputer-based databases. FOCUS, RAMIS, and NOMAD II, for example, are mainframe-based languages supporting database query, report generation, and simple analysis. FOCUS and RAMIS are also available in PC versions.

2) **Model-Based Decision Support Software:** Model-based analysis tools such as spreadsheet software enable managers to design models that incorporate business rules and assumptions. Microcomputer-based spreadsheet programs such as Lotussuits and Excel all support model building and "what if?" types of analysis. Mainframe-based spreadsheets such as Megacalc and Omnicalc fulfill the same purpose. Modeling tools like IFPS and Model are designed to support financial modeling and analysis.

3) **Statistics and Data Manipulation:** Statistical analysis software such as SAS and SPSS supports market researchers, operations research analysts, and other professionals using statistical analysis functions. Because of the need for increased "number crunching" capabilities, this type of software usually runs on mainframe computers. Microcomputer-based statistical packages are available as well.

4) **Display-Based Decision Support Software:** The final category of decision support software is display-based software.

Graphic displays of output generated from MS-Excel spreadsheets, for example, are very effective in management presentations. Graphics tools running in a mainframe environment include DISSPLA, TELLAGRAF, and SASGRAPH. Micro computer based tools such as Harvard Graphics and Power Point display graphics output in the form of pie charts, bar charts, and graphs.

13.3.4 Examples of Decision support systems in accounting

Decision Support Systems are widely used as part of an organisation's AIS. The complexity and nature of decision support systems vary from organization to organization. Many are developed in-house using either a general type of decision support program or a spreadsheet program to solve specific problems. Below are the examples of DSS in Accounting includes:

- **Cost Accounting System:** The health care industry is well-known for its cost complexity. Managing cost in this industry requires controlling costs of supplies, expensive machinery, technology, and a variety of personnel. Cost Accounting applications help health care organisations calculate product costs for individual procedures or services. Decision support systems can accumulate these product costs to calculate total costs per patient. Combining cost accounting DSS and Productivity system applications allows managers to measure the effectiveness of specific operating processes to improve its management decision-making.
- **Capital Budgeting System:** Companies require new tools to evaluate high-technology investment decisions. Decision makers need to supplement analytical techniques with decision support tools that consider some benefits of new technology. One decision support system designed to support decisions about investments in automated manufacturing technology that is AutoMan, which allows decision makers to consider financial, non-financial, quantitative, and qualitative factors in their decision-making processes. Using this decision support system, accountants, managers, and engineers identify and prioritize these factors. They can then evaluate up to seven investment alternatives at once.
- **Budget Variance Analysis System:** Financial institutions rely heavily on their budgeting systems for controlling costs and evaluating managerial performance. DSS allows comptrollers to graph, view, analyse, and annotate budget variances, as well as create additional one-and five year budget projections using the forecasting tools provided in the system. The decision support system thus helps the comptrollers create and control budgets for the cost-center managers reporting to them.
- **General Decision Support System: T**hese types of decision support systems are a decision-maker's tools that are used to input the data and answer questions about a specific problem domain to make use of this type of decision support system. An example is a program called Expert Choice. This program supports a variety of problems requiring decisions. The user works interactively with the computer to develop a hierarchical model of the decision problem. The decision support system them asks the users to compare decision variables with each other. Expert Choice analyses investment judgments and presents the decision maker with the best alternative.

13.4 Executive Information Systems (EIS)

It is a tool that is designed to meet the special needs of top-level managers. It provides direct on-line access to relevant information in a useful and navigable format. Relevant information is timely, accurate, and actionable about aspects of a business that are of particular interest to the senior manager. The useful and navigable format of the system means that it is specifically designed to be used by individuals with limited time, limited keyboarding skills, and little direct experience with computers. An EIS is easy to navigate so that managers can identify broad strategic issues, and then explore the information to find the root causes of those issues.

Executive information systems differ from traditional information systems in the following ways.

1. They are specifically tailored to executive's information needs.
2. They are able to access data about specific issues and problems as well as aggregate reports.
3. They provide extensive on-line analysis tools including trend analysis and exception reporting etc.
4. They can access a broad range of internal and external data.
5. They are particularly easy-to-use (typically mouse or touch- screen driven).

6. They are used directly by executives without assistance.
7. All EISs are delivered through terminals using easy-to-use software.
8. Information tends to be presented by pictorial or graphical means, whereas in most traditional information systems, information is usually presented in numerical or textual form, usually in printed report format.
9. Information is presented in summary format e.g. sales for the whole company. There is the facility to drill down to the other levels of information to see how the sales figures were arrived at – by geographical location, by product group etc.
10. The ability to manipulate data, to project `what if' outcomes and to work with modeling tools within the system are also evident in EIS. This is particularly so with external information that can be super imposed on to the company's information e.g. sales forecasts with information from the meteorological office about the weather.

13.4.1 EIS serves the following purpose:

(i) 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.
(ii) A secondary purpose is to allow timely access to information so that based on the answers to questions, strategic decisions could be taken by a manger in time.
(iii) It directs the attention of the management to specific areas of the organization or specific business problems. It makes managers and subordinates to work together to determine the root causes of issues highlighted by EIS
(iv) Sometimes misaligned reporting systems can result in inordinate management attention to things that are not so important. An EIS system can provide information that is actually important and represents a balanced view of the organisation's objectives.

13.4.2 Executive Roles and Decision Making: Most executive decisions fall into one of three classes: strategic planning, tactical planning, and "fire-fighting" activities. Also, executives need a certain degree of control to ensure that these activities are carried out properly.
1) Strategic Planning: Strategic planning involves determining the general, long-range direction of the organisation. Typically, the CEO is ultimately responsible for the development of strategic plans.
2) Tactical Planning: Whereas strategic planning addresses the general concerns of the firm, tactical planning refers to the how, when, where, and what issues involved with carrying out the strategic plan. Although executives will not normally be concerned with tactical details, they do need to worry about general tactics.
3) Fire Fighting: Major problems arise sometimes that must be resolved by someone at an executive level. For example, if a company is involved in a big lawsuit that threatens its financial solvency, an executive must get involved.
4) Control: In addition to planning and fire-fighting, executive management also needs to exert some general control over the organisation.

13.4.3 The Executive Decision-Making Environment: The three main sources for executive information are as follows:
1. Environmental information
2. Competitive information
3. Internal information

The type of decisions that executives must make is broad. Often, executives make these decisions based on a vision they have regarding what it will take to make their companies successful. *To a large extent, executives rely much more on their own intuition than on the sophisticated analytical skills.* The intuitive character of executive decision-making is reflected strongly in the types of information found most useful to executives.

Five characteristics of the types of information used in executive decision-making are discussed below:

(i) Lack of structure: Many of the decisions made by executives are relatively unstructured. For Instance, what general direction should the company take? Or what type of advertising campaign will best promote the new product line? These types of decisions are not so clear-cut as deciding how to debug a computer program or how

to deal with an overdue account balance. Also, it is not always obvious which data are required or how to weigh available data when reaching at a decision.

(ii) High degree of uncertainty: Executives work in a decision space that is often characterized by lack of precedent. For example, when the Arab oil embargo hit in the mid-1970s, no such previous event could be referenced for advice. Executives also work in a decision space where results are not scientifically predictable from actions. If prices are lowered, for instance, product demand will not automatically increase.

(iii) Future orientation: Strategic-planning decisions are made in order to shape future events. As conditions change, organisations must also change. It is the executive's responsibility to make sure that the organisation keeps pointed toward the future. Some key questions about the future include: "How will future technologies affect what the company is currently doing? Where will the economy move next, and how might that affect consumer buying patterns? As one can see, the answers to all of these questions about the future external environment are vital.

(iv) Informal source: Executives rely heavily on informal source for key information. For example, lunch with a colleague in another firm might reveal some important competitor strategies. Some other important information sources of information are meetings, tours around the company's facilities to chat with employees, brainstorming with a trusted colleague or two, and social events. Informal sources such as television might also feature news of momentous concerns to the executives.

(v) **Low level of detail:** Most important executive decisions are made by observing broad trends. This requires the executive to be more aware of the large overviews than the tiny items. Even so, many executives insist that the answers to some questions can only be found by mucking through details.

13.4.3 Principles to be followed while designing an EIS

Various principles to be followed while designing EIS are:

(i) EIS measures must be easy to understand and collect. An EIS should not add substantially to the workload of managers or staff.

(ii) EIS measures must be based on a balanced view of the organisation's objectives.

(iii) Performance indicators in an EIS must reflect everyone's contribution in a fair and consistent way. Indicators should be as independent as possible from variables outside the control of managers.

(iv) EIS measures must encourage management and staff to share ownership of the organisation's objectives. Performance indicators must promote both team-work and friendly competition. Measures will be meaningful for all staff; people must feel that they as individuals, can contribute to improving the performance of the organization.

(v) EIS information must be available to everyone in the organization. The objective is to provide everyone with useful information about the organisation's performance. Confidential information should not be part of the EIS.

(vi) EIS measures must evolve to meet the changing needs of the organization.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
				10	What do you mean by Information? Describe the important characteristics of information which makes it useful to the organization.
				5	Differentiate between open and closed system.
				10	System analysts develop various categories of information systems to meet a variety of business needs. Discuss any three such systems briefly.
				5	Write short note: Closed and open systems.
				8	Differentiate among Strategic, Tactical and Operational categories of Information required for different levels of Managerial decision-making.
				10	Discuss the effect of applying computer technology to

					Management Information System.
				6	Mention at least two pieces of information-one internal and one external-required at every one of the levels of Management.
				3	Describe briefly three levels of Management
				10	Explain three board categories of the planning information requirements of executives.
				5	Write short note : Strategic and Tactical decisions
				5	Describe the main pre-requisites of a Management Information System which makes it an effective tool.
				5	Discuss the limitations of the management Information System.
				10	State the factors to be considered for designing the effective Management Information System.
				5	Write short note: Programmed decisions.
				12	In what ways does an Executive Information System differ from the Traditional Information System?
				5	Write short note : Decision Support Systems
				4	Write Short Note : Executive Information Systems
				5	Successful executives take decisions relying more on intuition than on any quantitative analytical decision technique. Mention five characteristics of the types of information that are responsible for this phenomenon in executive decision-making.
				5	"A decision support system supports the human decision-making process rather than providing a means to replace it". Justify the above statement by stating the characteristics of decision support system.
				10	What is an Executive Information System? Discuss its various purposes.
				5	Describe various software tools used in Decision support system.
				10	"Decision support systems are widely used as part of an Organisation's Accounting Information system". Give examples to support this statement.
				5	Briefly explain the principles to guide the design of measures and indicators to be included in EIS.
				5	Briefly discuss four basic components of Decision Support System.
Nov-08	[2(b)]	1		5	What is Decision Support System?. Briefly explain three characteristics of Decision Support System.
Nov-08	[2(c)]	1		5	Explain Executive Information System(EIS). What purpose does it serve?

2 - SYSTEMS DEVELOPMENT LIFE CYCLE METHODOLOGY

1. WHAT IS SYSTEMS DEVELOPMENT PROCESS?

Systems development refers to the process of examining a business situation with the intent of improving it through better procedures and methods. Systems development can generally be thought of as having two major components: systems analysis and systems design. Systems design is the process of planning a new business system or one to replace or complement an existing system. But before this planning can be done, one must thoroughly understand the old system and determine how computers can be used (if at all) to make its operation more effective.

2. SYSTEM DEVELOPMENT LIFE CYCLE

The process of system development starts when management or sometimes system development personnel realise that a particular business system needs improvement. The system development life cycle method can be thought of as a set of activities that analysts, designers and users carry out to develop and implement an information system.

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

(i) ***Preliminary investigation*****:** It is undertaken when users come across a problem or opportunity and submit a formal request for a new system to the MIS department. This activity consists of three parts; request clarification, feasibility study and request approval.

(ii) ***Requirements analysis or systems analysis*****:** In this stage, the analysts work closely with employees and managers of the organization for determining the information requirements of the users. Several fact-finding techniques and tools such as questionnaires, interviews, observing decision-maker behaviour and office environment, etc. are used for understanding the requirements of the users. As details are gathered, the analysts study the present system to identify its problems and shortcomings and identify the features which the new system should include to satisfy the new or changed user application environment.

(iii) ***Design of the system*****:** It produces the details that state how a system will meet the requirements identified in the previous step. The analyst designs various reports/outputs, data entry procedures, inputs, files and database. He also selects file structures and data storage devices. These detailed design specifications are then passed on to the programming staff for software development.

(iv) ***Acquisition and development of software*****:** In this stage, resource requirements such as specific type of hardware, software and services are determined. Subsequently, choices are made regarding which products to buy or lease from which vendors. Software developers may modify and then install purchased software or they may write new custom designed programs.

(v) ***System testing*****:** Before the information system can be used, it must be tested. Special test data are input for processing, and results are examined. If it is found satisfactory, it is eventually tested with actual data from the current system.

(vi) Implementation and maintenance**:** After system is found to be fit, it is implemented with actual data. After implementation, the system is maintained; it is modified to adapt to changing users and business needs.

3. Achieving systems development objectives (Reasons for failure):

♦*Lack of senior management support for and involvement in information systems development.* Developers and users of information systems will watch senior management to determine which systems development projects are important and will act accordingly by shifting their efforts away from any project not receiving management attention.

♦*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.

♦*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.

♦*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.

♦*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.

♦*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 currently; in these organisations, a training plan and training budget do not exist.

♦*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 are really attempts at "downsizing" (or "rightsizing")

♦*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.

♦*Inadequate testing and user training.* New systems must be tested before installation to determine that they will operate correctly. Users must be training to effectively utilise the new system.

To overcome these and other problems, organisations must execute the systems development process efficiently and effectively.

4. Approaches to Systems Development:

4.1 Traditional approach: In traditional approach of the systems development, activities are performed in sequence. It involves basically six phases, viz; preliminary investigation, requirement analysis, system design, system acquisition, system testing and system implementation & maintenance. When traditional approach is used, managers and users interact with system analysts, system designers and application programmers during various phases. An activity is undertaken only when the prior step is fully completed. Managers and users assess and review the work performed by MIS professionals during each stage of process before proceeding to the next stage. If the work is satisfactory, they formally sign or accept the work and allow the system development team to proceed to the next phase. This approach is applied to the development of large computer based information systems such as the transaction processing systems.

4.1.1 SYSTEMS DEVELOPMENT METHODOLOGY

A systems development methodology [also known as systems development life cycle (SDLC) methodology] is a formalized, standardized, documented set of activities used to manage a systems development project. It should be used when information systems are developed, acquired, or maintained. The methodology is characterised by the following:

♦The project is divided into a number of identifiable processes, and each process has a starting point and an ending point. Each process comprises several activities, one or more deliverables, and several management control points. The division of the project into these small, manageable steps facilitates both project planning and project control.

♦Specific reports and other documentation, called deliverables, must be produced periodically during systems development to make development personnel accountable for faithful execution of system development tasks. An organisation monitors the development process by reviewing the deliverables that are prepared at the end of each key step. Many organisations rely on this documentation for training new employees; it also provides users with a reference

while they are operating the system.

♦Users, managers, and auditors are required to participate in the project. These people generally provide approvals, often called signoffs, at pre-established management control points. Signoffs signify approval of the development process and the system being developed.

♦The system must be tested thoroughly prior to implementation to ensure that it meets users' needs.

♦A training plan is developed for those who will operate and use the new system.

♦Formal program change controls are established to preclude unauthorized changes to computer programs.

♦A post-implementation review of all developed systems must be performed to assess the effectiveness and efficiency of the new system and of the development process.

4.1.2 System Development Team:

a) Steering Committee: This committee usually consists of a group of key IS services users that acts as a review body for IS plans and applications development. The steering committee ensures that ongoing systems development activities are consistently aimed at satisfying the information requirements of managers and users within the organisation.
b) IS Department: It becomes the responsibility of the IS department to develop the systems.
c) Project Management: In order to coordinate development activities of the system, a project management team generally consisting of both computer professionals and key users is appointed.
d) Systems Analysts: System analysts are subsequently assigned to determine user requirements, design the system and assist in development and implementation activities.

Accountants' involvement in development work: Most accountants are uniquely qualified to participate in systems development because they may be among the few people in an organization who can combine knowledge of IT, business, accounting, and internal control, as well as behaviour and communications, to ensure that new systems meet the needs of the user and possess adequate internal controls. They have specialized skills - such as accounting and auditing - that can be applied to the development project. For example, an accountant might perform the analysis of a proposed system's costs and benefits. As internal, information technology (IT), and independent auditors, accountants provide a unique- and independent -perspective with which to evaluate the systems development process and the systems being developed.

4.1.3 STAGE I - THE PRELIMINARY INVESTIGATION

The analyst working on the preliminary investigation should accomplish the following objectives:

1. Clarify and understand the project request: What is presently being done? What is required and why? Is there an underlying reason different from the one the user has identified?
2. Determine the size of the project: Does a request for a project call for new development or for modification of the existing system? The investigation to answer this question will also gather the details useful in estimating the amount of time and number of people required to develop the project.
3. Determine the technical and operational feasibility of alternative approaches.
4. Assess costs and benefits of alternative approaches: What are the estimated costs for developing a particular system? Will the proposed system reduce operating costs? Will the proposed system provide better services to customers, etc?
5. Report findings to the management with recommendation outlining the acceptance or rejection of the proposal.

A) Conducting the Investigation: During preliminary investigation, the analyst collects the data through two primary methods:

1 Reviewing internal documents : The analysts conducting the investigation first try to learn about the organisation involved in, or affected by, the project. For example, to review an inventory system proposal, the analyst will try to know how the inventory department operates and who are the managers and supervisors. Analysts can usually learn these details by examining organisation charts and studying written operating procedures.

2. Conducting Interviews : Written documents tell the analyst how the systems should operate, but they may not include enough details to allow a decision to be made about the merits of a systems proposal, nor do they present

users' views about current operations. To learn these details, analysts use interviews. Interviews allow analysts to know more about the nature of the project request and the reasons for submitting it. Usually, preliminary investigation interviews involve only management and supervisory personnel.

B) Feasibility study

Feasibility study refers to a process of evaluating alternative systems through cost/benefit analysis so that the most feasible and desirable system can be selected for development. The feasibility study of a system is undertaken from three angles : technical, economic and operational feasibility. The proposed system is evaluated from a technical view point first and if technically feasible, its impact on the organisation and staff is assessed. If a compatible technical and social system can be devised, it is then tested for economic feasibility.

i) Technical feasibility: It is concerned with hardware and software. Essentially, the analyst ascertains whether the proposed system is feasible with existing or expected computer hardware and software technology. The technical issues usually raised during the feasibility stage of investigation include the following:

1. Does the necessary technology exist to do what is suggested (and can it be acquired)?
2. Does the proposed equipment have the technical capacity to hold the data required to use the new system?
3. Will the proposed system provide adequate responses to inquires, regardless of the number or location of users?
4. Can the system be expanded if developed?
5. Are there technical guarantees of accuracy, reliability, ease of access, and data security?

ii) Economic feasibility : It includes an evaluation of all the incremental costs and benefits expected if the proposed system is implemented. This is the most difficult aspect of the study. The financial and economic questions raised by analysts during the preliminary investigation are for the purpose of estimating the following:

(i) The cost of conducting a full systems investigation.
(ii) The cost of hardware and software for the class of applications being considered.
(iii) The benefits in the form of reduced costs or fewer costly errors.
(iv) The cost if nothing changes (i.e., the proposed system is not developed)

The procedure employed is the traditional cost-benefit study.

iii) Operational feasibility: It is concerned with ascertaining the views of workers, employees, customers and suppliers about the use of computer facility. The support or lack of support that the firm's employees are likely to give to the system is a critical aspect of feasibility. A system can be highly feasible in all respects except the operational and fails miserably because of human problems.

iv) Schedule Feasibility: Schedule feasibility involves the design team's estimating how long it will take a new or revised system to become operational and communicating this information to the steering committee.

v) Legal Feasibility : Legal feasibility is largely concerned with whether there will be any conflict between a newly proposed system and the organisation's legal obligations.

vi) Estimating costs and benefits : After possible solution options are identified, the analyst should make a primary estimate of each solution's costs and benefits.

Cost : System costs can be sub divided into development, operational and intangible costs. *Development costs* for a computer based information system include costs of the system development process such as

(i) salaries of the system analysts and computer programmers who design and program the system,
(ii) cost of converting and preparing data files and preparing systems manual and other supportive documents,
(iii) cost of preparing new or expanded computer facilities,
(iv) cost of testing and documenting the system, training employees, and other start up costs.

Operating costs of a computer based information system include

(i) hardware/software rental or depreciation charges,
(ii) salaries of computer operators and other data processing personnel who will operate the new system,
(iii) salaries of system analysts and computer programmers who perform the system maintenance function,
(iv) cost of input data preparation and control,
(v) cost of data processing supplies,

(vi) cost of maintaining proper physical facilities including power, light, heat, air conditioning, building rental or other facility charges and equipment and building maintenance charges, overhead charges of the business firm.

Intangible costs are costs that cannot be easily measure. For example, the development of a new system may disrupt the activities of an organisation and cause a loss of employee productivity or morale. Customer sales and goodwill may be lost by errors made during the installation of a new system. Such costs are difficult to measure in rupees but are directly related to the introduction and operation of information system.

Benefits: The benefits which result from developing new or improved information systems that utilise EDP can be subdivided into tangible and intangible benefits. Tangible benefits are those that can be accurately measured and are directly related to the introduction of a new system, such as decrease in data processing cost. Intangible benefits such as improved business image are harder to measure and define. Benefits that can result from the development of a computerised system are summarised below:

1. Increase in sales or profits (improvement in product or service quality).
2. Decrease in data processing costs (elimination of unnecessary procedures and documents).
3. Decrease in operating costs (reduction in inventory carrying costs).
4. Decrease in required investment (decrease in inventory investment required).
5. Increased operational ability and efficiency (improvement in production ability and efficiency; for example, less spoilage, waste, and idle time).
6. New or improved information availability (more timely and accurate information, and new types and forms of information)
7. Improved abilities in computation and analysis (mathematical simulation).
8. Improved customer service (more timely service).
9. Improved employee morale (elimination of burdensome and boring job tasks).
10. Improved management decision making (better information and decision analysis)
11. Improved competitive position (faster and better response to actions of competitors)
12. Improved business and community image ("progressive" image as perceived by customers, investors, other businesses, government and the public).

4.1.4 STAGE II - REQUIREMENTS ANALYSIS OR SYSTEMS ANALYSIS

This is the second stage of system development life cycle (SDLC). This analysis involves determining users' needs, studying the present system of the organisation in depth, and determining the features, which the new system should possess. Various fact-finding techniques and system development tools are used for requirement analysis.

During the requirement analysis phase of the traditional approach, the focus is one determining user needs, studying the application area in depth, assessing the strengths and weaknesses of the present system and reporting results to management.

The significance of studying in the present system is to know why the organization is not satisfied by this system. What are its strong and weak points? How the present system uses hardware, software and human resources to convert the data of the organization into information for end users. In addition, the system analysts should analyze how these resources are used to accomplish the activities of input, processing, output, storage and control.

A. The fact finding techniques used by the Analyst for requirement analysis are as follows:

1. **Documents:** Manuals, input forms, output forms, diagrams of how the current system works, organization charts showing hierarchy of users and managers responsibilities, job description for the people who work with current system, procedure manuals, program codes for applications associated with current system etc. should be looked into as thoroughly as possible, since they are the rich source of information.
2. **Questionnaires:** Users and managers are asked to complete questionnaire about the information system when the traditional system development approach is chosen. Using questionnaires, a large amount of data can be collected through a variety of users quickly.
3. **Interviews:** Users and managers may also be interviewed to extract information from them. The information so obtained provides complete picture of the present system. The interview also gives analyst the opportunity to know

about the first hand user reactions and to probe for further information.

4. **Observation:** In prototype approach, observation plays a central role in requirement analysis. The analyst visits the user place to watch how the work is taking place. While the user is experimenting with the prototype, the systems analyst observes the user and puts these observations into perspective in order to determine how the prototype should be further designed. This gives him first hand information rather than relying on other methods such as analysing documents, questionnaires etc.

B. Analysis of the present system:

Detailed investigation of the present system involves collecting, organising and evaluating facts about the system and the environment in which it operates. Enough information should be assembled so that a qualified person can understand the present system without visiting any of the operating departments. Review of existing methods, procedures, data flow, outputs, files, inputs and internal controls should be intensive in order to fully understand the present system and its related problems.

The following areas may be studied in depth:

1. **Review historical aspects**: A brief history of the organisation should identify the major turning points and milestones that have influenced its growth. A review of annual reports can provide an excellent historical perspective. The system analyst should identify what system changes have occurred in the past. These should include operations that have been successful or unsuccessful with computer equipment and techniques.
2. **Analyse inputs**: A detailed analysis of present inputs is important since they are basic to the manipulation of data. Source documents are used to capture the originating data for any type of system. The system analyst should be aware of the various sources from where the data can be initially captured, keeping in view the fact that outputs for one area may serve as an input for another area. The system analyst must understand the nature of each form, what is contained in it, who prepared it, from where the form is initiated, where it is completed, the distribution of the form and other similar considerations.
3. **Review data files maintained**: The analysts should investigate the data files maintained by each department, noting their number and size, where they are located, who uses them and the number of times per given time interval these are used. The system analyst should also review all online and off line files which are maintained in the organization as these will reveal information about data that are not contained in any output. The related cost of retrieving and processing the data is another important factor that should be considered by the systems analyst.
4. **Review methods, procedures and data communications**: Methods and procedures transform input data into useful output. A method is defined as a way of doing something; a procedure is a series of logical steps by which a job is accomplished. A procedure's review is an intensive survey of the methods by which each job is accomplished, the equipment utilized and the actual location of the operations. Its basic objective is to eliminate unnecessary tasks or to perceive improvement in opportunities in the present information system. He must review the types of data communication equipment including data interface, data links, modems, dialup and leased lines and multiplexers. The system analyst must understand how the data communications network is used in the present system so as to identify the need to revamp the network when the new system is installed.
5. **Analyze outputs**: The outputs or reports should be scrutinized carefully by the system analysts in order to determine how well they will meet the organization's needs. The analysts must understand what information is needed and why, who needs it and when and where it is needed. Additional questions concerning the sequence of the data, how often the form reporting it is used, how long it is kept on file, etc. must be investigated. Often many reports are a carryover from earlier days and have little relevance to current operations. Attempt should be made to eliminate all such reports in the new system.
6. **Review internal controls**: A detailed investigation of the present information system is not complete until internal controls are reviewed. Locating the control points helps the analyst to visualize the essential parts and framework of a system. An examination of the present system of internal control may indicate weaknesses that should be removed in the new system. The adoption of advanced methods, procedures and equipment might allow much greater control over the data.
7. **Model the existing physical system and logical system**: As the logic of inputs, methods, procedures, data files,

data communications, reports, internal control and other important items are reviewed and analyzed in a top down manner, the process must be properly documented. The logical flow of the present information system may be depicted with the help of system flow charts. The physical flow of the existing system may be shown by employing data flow diagrams. During the process of developing the data flow diagram, work on data dictionary for the new information system should be begun. The data elements needed in the new system will be found in the present system only. Hence, it is wise to start the development of the data dictionary as early as possible.

8. **Undertake overall analysis of present system**: Based upon the aforesaid investigation of the present information system, the final phase of the detailed investigation includes the analysis of :

a. the present work volume
b. the current personnel requirements
c. the present benefits and costs

Each of these must be investigated thoroughly.

C. Systems Analysis of Proposed Systems: After each functional area of the present information system has been carefully analysed, the proposed system specifications must be clearly defined. The required systems specifications which should be in conformity with the project's objectives are as follows:

a. Outputs produced with great emphasis on timely managerial reports that utilise the 'management by exception' principle.

b. Database maintained with great accent on online processing capabilities.

c. Input data prepared directly from original source documents for processing by the computer system.

d. Methods and procedures that show the relationship of inputs and outputs to the database, utilizing data communications where deemed appropriate.

e. Work volumes and timings carefully considered for present and future periods including peak periods.

D. SYSTEM DEVELOPMENT TOOLS

Many tools and techniques have been developed to improve current information systems and to develop new ones. Such tools help end users and systems analysts to:

♦conceptualise, clarify, document and communicate the activities and resources involved in the organisation and its information systems.

♦analyse present business operations, management decision making and information processing activities of the organisation.

♦Propose and design new or improved information systems to solve business problems or pursue business opportunities that have been identified.

Many systems development tools take the form of diagrams and other graphic representations. The major tools used for system development can be grouped into four categories based on the systems features each document has:

1. System components and flows : These tools help the system analysts to document the data flow among the major resources and activities of an information system. System flow charts are typically used to show the flow of data media as they are processed by the hardware devices and manual activities. A data flow diagram uses a few simple symbols to

illustrate the flow of data among external entities (such as people or organisations, etc.), processing activities and data storage elements. A system component matrix provides a matrix framework to document the resources used, the activities performed and the information produced by an information system.

2. User interface: Designing the interface between end users and the computer system is a major consideration of a system analyst while designing the new system. Layout forms and screens are used to construct the formats and contents of input/output media and methods. Dialogue flow diagrams analyse the flow of dialogue between computers and people. They document the flows among different display screens generated by alternative end user responses to menus and prompts.

3. Data attributes and relationships : The data resources in information system are defined catalogued and

designed by this category of tools. A data dictionary catalogs the description of the attributes (characteristics) of all data elements and their relationships to each other as well as to external systems. Entity-relationship diagrams are used to document
the number and type of relationship among the entities in a system. File layout forms document the type, size and names of the data elements in a system. Grid charts help in identifying the use of each type of data element in input/output or storage media of a system.

4. Detailed system process : These tools are used to help the programmer develop detailed procedures and processes required in the design of a computer program. Decision trees and decision tables use a network or tabular form to document the complex conditional logic involved in choosing among the information processing alternatives in a system.

Structure charts document the purpose, structure and hierarchial relationships of the modules in a program.

We will now describe some of these tools in detail.

(a) Systems flow chart : It is a graphic diagramming tool that documents and communicates the flow of data media and information processing procedures taking place in an information system. This is accomplished by using a variety of labeled symbols connected by arrows to show the sequence of information processing activities. System flow charts typically emphasise the media and hardware used and the processes that take place within an information system. Thus, they represent a graphic model of the physical information system that exists or is proposed. Systems flow charts are widely used to communicate the overall structure and flows of a system to end-users.

(b) Data flow diagrams : 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. There is no ideal way to develop a DFD; different problems call for different methods. A DFD is composed of four basic elements: data sources and destinations, data flows, transformation processes, and data stores.

Data source and destinations: Represents an organization or individual that sends or receives the data.

Data Flows: Represents the flow of data between processes, data stores, and data sources and destinations.

Processes: Processes represent the transformation of data.

Data Stores: A temporary or permanent repository of data.

(c) Layout forms and screens: These consist of electronic displays or preprinted forms on which the size and placement of titles, heading, data and information can be designed. Layout forms and screens are used to design source documents, input/output and storage records, files and output displays and reports.

(d) System components matrix : The system components matrix can be used as an information system framework for both systems analysis and system design. It views the information system as a matrix of components that highlights how the basic activities of input, processing, output, storage and controls are accomplished in an information system, and how the use of hardware, software and people resources can convert data resources into information products.

(e) CASE Tools : The data flow diagram and system flow charts that users review are commonly generated by systems developers using the on-screen drawing modules found in CASE (Computer-Aided-Software Engineering) software packages. CASE refers to the automation of any thing that humans do to develop systems. In 1980s, these tools enabled
system analysts and programmers to create flow charts and data flow diagrams on a mini computer or a micro computer workstation. Today, CASE products can support virtually all phases of traditional system development process. For example, these packages can be used to create complete and internally consistent requirements specifications with graphic generators and specifications languages.

(f) Data Dictionary: It is a computer file that contains descriptive information about the data items in the files of a business information system. In other words, it is a computer file about data. The information included in each record of a Data Dictionary may include the following about an item:

(i) Codes describing the data item's length, data type and range.

(ii) Identity of the source documents used to create the data.

(iii) Names of the computer files storing the data item.
(iv) 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.

4.1.5 STAGE III: SYSTEMS DESIGN

The system design phase usually consists of following three activities:
(i) Reviewing the system's informational and functional requirements;
(ii) Developing a model of the new system, including logical and physical specifications of outputs, inputs, processing, storage, procedures and personnel;
(iii) Reporting results to management.

Developing a model for a new system: When designing a system, the systems analysts and systems development team determine how both manual and software/hardware components will be realised at logical and physical levels in each of the following areas: (i) Output, (ii) Input, (iii) Processing, (iv) Storage, (v) Procedures and (vi) Personnel.

(I) **(I) Designing system outputs:** In designing computer output, analysts identify the specific output that is needed to meet the information requirements, select methods for presenting information, create documents, reports or other formats that contain information produced by the system.

Output objectives: The output from an information system should accomplish the following objectives:
1. Convey information about past activities, current status or projections of the future.
2. Signal important events, opportunities, problems or warnings.
3. Trigger an action.
4. Confirmation of an action.

Important Factors in Output Design

There are six important factors which should be considered by the system analyst while designing user outputs. These are briefly discussed below:

(i) **Content:** Content refers to the actual pieces of data included among the outputs provided to users. Too much content can cause managers to waste time in isolating the information that they need; it also diminishes the impact of truly important information. Hence, only the required information should be included in various outputs.

(ii) **Form:** Form refers to the way that content is presented to users. Content can be presented in various forms; quantitative, non-quantitative, text, graphics, video and audio. Sometimes, converting absolute values to relative values such as percentages often help managers to comprehend the data easily and make better decisions. Hence, the form of the output should be decided keeping in view the requirements for the concerned user.

(iii) **Output volume:** The amount of data output required at any one time is known as output volume. It is better to use high-speed printer or a rapid-retrieval display unit, which are fast and frequently used output devices in case the volume is heavy. Unusually heavy output volume normally causes concern about paper cost. In such a case, alternative methods of output display such as COM (Computer Output Microfiche) may be considered.

(iv) **Timeliness:** Timeliness refer to when users need outputs. Some outputs are required on a regular, periodic basis - perhaps daily, weekly, monthly, at the end of a quarter or annually. Other types of outputs are generated on request. A sales manager, for example, may be requiring a weekly sales report. Other users, such as airline agents, require both real- time information and rapid response times in order to render better client service. Hence, the system designer might require that display information be provided to the airline agents

within a few seconds at least 95% of the time. Communication-oriented and real-time systems are often the solution for such situations.

(v) Media: Input-output medium refers to the physical device used for input, storage or output. A variety of output media are available in the market these days which include paper, video display, microfilm, magnetic tape/disk and voice output. Many of these media are available in different forms. The system designer can select a medium, which is best suited to the user requirements.

(vi) Format: The manner in which data are physically arranged is referred to as format. This arrangement is called output format when referring to data output on a printed report or on a display screen. Traditionally, when formatting the printed report for managers or users, a design tool called a printer spacing chart is used. On the chart, titles, headings, columns of data and other types of report elements are set up in the manner desired by the user.

Designing printed output:

There are few guidelines to design the output, which should be followed while preparing the layout form are:

1. Reports and documents should be so designed that it is to be read from left to right and top to bottom.
2. It should be easiest to find the most important items/highlights of the report.
3. Each page of the report should include the title and heading of the report along with the page no., date of report generation and column headings. The title should be descriptive but yet concise. Each page should be numbered. Date of generation helps the users in determining the utility of the report at the time of reference and makes the complete review process a very effective one. Column headings serve to orient the user to the report contents.
4. Each data item should have a heading, a very short and descriptive. Similar items should be grouped together on the report with the description printed only once at the change or in case it spills over to the next page.
5. Control breaks should be used in the report for better readability. They should be clearly separated from rest of data with additional lines. In order to draw the attention of the user, either the boxes or bold letters or both should be used at control breaks. One can use special characters also to highlight the control breaks. This makes it easier to find critical information.
6. There should be sufficient margin at left and right as well as at top and bottom for better concentration of the user. It also helps in getting the report bound for permanent records storage without any information being hidden in binding.
7. The detail line for variable data should be defined by indicating whether each space is to be used for an alphabetic, special or numeric character.
8. Finally the mock reports should be thoroughly reviewed by the users and programmers for feasibility, readability, usefulness, understandability as well as aesthetic appeal. This not only helps in generating the quality reports but also saves significant development efforts, which go into re-development of modified reports later.

Designing visual display output:

Attention should be paid to

i. Physical dimensions of the screen
ii. Degree of resolution (high, medium, low);
iii. Colours available
iv. Methods of highlighting
v. Methods of intensity control
vi. No. of Rows and Columns that can be displayed

(II) Designing systems inputs:

Important factors to be considered in the input design:

(i) **Content:** The analyst is required to consider the types of data that are needed to be gathered to generate the desired user outputs.

(ii) **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.

(iii) 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 work stations, magnetic tapes, magnetic disks, key-boards, optical character recognition, pen-based computers and voice input etc. A suitable medium may be selected depending on the application to be computerized.

(iv) **Format**: 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 requires the assistance of a professional programmer or database administrator.

(v) **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 centralized data entry department using key-to-tape or key-to-disk systems.

Form design:

Forms are pre-printed papers that require people to fill in responses in a standardised way. Forms elicit and capture information required by organisational members that often will be input to the computer. Through this process, forms often serve as source documents for the data entry personnel.

Guidelines for form design: The following guidelines for form design should be observed in order to design useful forms.

1. **Making forms easy to fill**: To reduce errors, speedup completion and facilitate entry of data, it is essential that forms should be easy to fill out. This can be achieved by considering the following factors:

   (a) ***Form flow***: Designing a form with proper flow can minimize time and effort expanded by employees in the form completion. Forms should flow from left to right and top to bottom. Illogical flow takes extra time and can be frustrating for the user. A form that requires people to go directly to the bottom of the form and then skip back to the top for completion exhibits poor flow.

   (b) ***Divide the form in logical sections***: The second technique that makes it easy for people to fill out forms correctly is logical grouping of information. A good form consists of seven main sections namely (I) headings, (ii) identification and access, (iii) instructions, (iv) body (v) signature and verification (vi) totals and (vii) comments.

   The top quarter of the form is devoted to three sections: the heading, the identification and access section and the instruction section. The heading section includes the name and address of the business originating the form. The identification and access section includes codes that may be used to fill the report and gain access to it at a later date. The middle of the form is its body, which composes approximately half of the form. This is the part of the form that requires the most details and development from the person completing it. The bottom quarter of the form is composed of three sections: signature and verification, totals and comments.

   (c) ***Captioning****:* Clear captioning is yet another technique that can make the work of filing up the form easy. Captions tell the persons completing the forms what to put on a blank line, space or box.
2. **Meeting the intended purpose**: Forms are created to serve one or more purposes in the recording, processing, storing and retrieving of information for various businesses. Sometimes, it is desirable to provide different information to different departments or users while still sharing some basic information. This is where specialty forms are useful. The analyst can use his imagination to design such forms which can provide the information required by different departments while avoiding duplication of information.
3. **Ensuring accurate completion**: Error rates typically associated with collecting data can drop sharply when forms are designed to assure accurate completion. Design is important in making people to do the right thing with the form.

Various controls can be embedded in the form design. For example, the form design can provide an internal double check with column totals and row totals, summing to the same number. If the row and column totals do not sum to the same number, the employee filling out the form knows that there is a problem and can correct it on the spot.

4. **Keeping forms attractive:** An aesthetic form draws people into it and encourages proper completion. This means that people who fill out the forms will be more satisfied and that the forms will be completed. Thus, forms should look uncluttered, organised and logical even after they are filled in. Providing enough space for typewriter or for underlining responses will help in this regard. To be attractive, forms should elicit information in the expected order: convention dictates asking for name, address, city, state and pincode in this order. Proper layout and flow contribute to a form's attractiveness. Using different fonts for type within the same form can help in making it attractive for the user. Separate categories and subcategories with thick and thin lines can also encourage interest in the form. Type fonts and lines weights are useful design elements for capturing attention and forcing people to fill in the form correctly.

Coding methods: 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.

Characteristics of a Good Coding Scheme

(i) Individuality – The code must identify each object in a set uniquely and with absolute precision. The code should be universally used over the entire organisation.

(ii) Space - As far as possible code number must be much briefer than description.

(iii) Convenience - The format of code number should facilitate their use by people. This implies that code number should be short and simple and consist of digits and or upper case alphabets. It is better to avoid use of special symbols.

(iv) Expandability – As far as possible, growth in the number of objects in a set should be provided for. Therefore, whilst introducing the scheme, longer number of digits/number than necessary at present may be adopted as the code length. Related items must use similar number.

(v) Suggestiveness - The logic of the coding scheme should be readily understandable. Also, the letter or number should be suggestive of the item characteristics. But this should not be carried too far in lengthening the code since it would defeat the purpose of brevity.

(vi) Permanence – Changing circumstances should not invalidate the scheme or invalidation in future should be kept to minimal.

Designing efficient data entry: Assuring the quality of data input to the information system is critical to assure quality output. The quality of data entered can be improved through attainment of the three major data entry objects: these are, effective and efficient data capture, effective coding and appropriate data-entry methods. As has been discussed earlier, a well designed form to serve as a source document is the first step towards effective data entry. A second way to speed up data entry is through effective use of coding, which puts data in short sequences. Finally, effective data entry can be achieved by giving attention to the input devices being used.

(III) Data Storage: Storing data is often an important decision in the design of an information system. There are two approaches for storing data. The first approach is to store data in individual files, one file for each application. The second approach is to develop a data base that can be shared by many users for a variety of applications as need arises.

The conventional file approach may at times be a more efficient approach since the file can be application oriented. On the other hand, the data base approach may be more appropriate because the same data need to be entered, stored and updated once.

(IV) Design of Data Communications : Most information systems in practice involve the transmission of data between different locations. Data communications technology is advancing rapidly. Systems analysts have a variety of tools

and technologies-from the office telephone to satellite in space to ensure that the needs of users in each environment can be met.

Requirements for data communication system:

The system analysts must select the following components:

1. For communications channels, he may have to make a decision regarding channel selection, transmission rate, leased or dial-up line, type of line, for example, simplex or half-duplex etc.
2. Communications control devices: The analyst is required to select devices such as modems, data service units, multiplexer and concentrator, data switches, etc. In addition the analyst may also select the type of network (LAN or WAN), network topology (point-to-point or multi drop) etc. and the network architecture to be utilized for the proposed project.

System Manual : The basic output of the system design is a description of the task to be performed, complete with layouts and flowcharts. This is called the job specifications manual or system manual. It contains:

(i) General description of the existing system.

(ii) Flow of the existing system.

(iii) Outputs of the existing system - the documents produced by existing system are listed and briefly described, including distribution of copies.

(iv) General description of the new system - its purposes and functions and major differences from the existing system are stated together with a brief justification for the change.

(v) Flow of the new system - this shows the flow of the system from and to the computer operation and the flow within the computer department.

(vi) Output Layouts.

(vii) Output distribution - the distribution of the new output document is indicated and the number of copies, routing and purpose in each department shown. The output distribution is summarized to show what each department will receive as a part of the proposed system.

(viii) Input layouts - the inputs to the new system are described and complete layouts of the input documents and input disks or tapes provided.

(ix) Input responsibility - the source of each input document is indicated as also the user department responsible for each item on the input documents.

(x) Macro-logic-the overall logic of the internal flows will be briefly described by the systems analyst, wherever useful.

(xi) Files to be maintained - the specifications will contain a listing of the tape, disk or other permanent record files to be maintained, and the items of information to be included in each file. There must be complete layouts for intermediate or work file; these may be prepared later by the programmer.

(xii) List of programs - a list of the programs to be written shall be a part of the systems specifications.

(xiii) Timing estimates - a summary of approximate computer timing is provided by the systems analyst.

(xiv) Controls - this shall include type of controls, and the method in which it will be operated.

(xv) Audit trail - a separate section of the systems specifications shows the audit trail for all financial information. It indicates the methods with which errors and defalcation will be prevented or eliminated.

(xvi) Glossary of terms used.

Reporting to Management: After the system design is finished, users have indicated their satisfaction with the design, and the system's benefits and costs are revised to reflect any major changes, the system development team reports the results of these activities to the management. The report should include:

1. description of the application and users source that led to the system.
2. a summary of the results of the requirement analysis.
3. design recommendation.
4. any changes in the costs and benefits of the new system.
5. a plan for the remaining system development activities.

If the management is satisfied with the work the systems developer will proceed to the next phase of the systems

development process.

4.1.6 STAGE IV: SYSTEMS ACQUISITION AND SOFTWARE DEVELOPMENT

After a system is designed, either partially or fully, the next phase of the systems development starts which relates to the acquisition of hardware, software and services. In this section, we will explore how this process takes place.

A) Procuring Computer Hardware

Selecting a computer is a major commitment for any organisation not only because of its high cost but also since a computer has a profound and long range effect on a company's operations. The user depends upon the vendor for support services, systems design, education and training etc, and expansion of computer installation for almost an indefinite period. Hence, selection of a computer may be made after careful appraisal of various factors. Following points may be born in mind at the time of selection of a computer system:

(i) All computer systems offered in the market today have good hardware, competent software and roughly similar facilities. Due to the rapid development of computer technology, the more recent the computer, the better its performance is and the lower its cost. Therefore, as far as possible the latest possible technology should be acquired.

(ii) Computer performance for commercial work is mainly determiend by the speeds 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 instrution execution speed, and repertoire. A comparison along these lines can be made quickly and quite effectively.

(iii) The software supplied by the manufacturer may make a significant difference if it contains a package of special applicability to the jobs envisaged. Experts maintain that since hardware speed and facilities are uniformly good, today the selection of computer should be made on software considerations.

(iv) Modern computers are marketed as series of compatible machines with increasingly powerful central processors and interchangeable peripherals. Thus, the choice of a computer really becomes a choice of a model within a series, based on a long range plan of expansion.

(v) 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.

B) Software acquisition: Make or Buy:

At this stage, the system developers must determine whether the application software should be created in-house or acquired from a vendor. This decision is often called the **make-or-buy** decision. In the past several years, pre-packaged application software or application software packages have become increasingly popular for many business functions, including accounting (for example, payroll and personnel accounting), general ledger, manufacturing, financial planning and numerous other applications. Many of these packages consist of several programs and a complete set of documentation tools. Vendors providing these software packages even impart training about how to use the software to its full potential.

Factors affecting the "make or buy" decision of application software are as follows:

- *Availability of skilled manpower:* If sufficient number of programmers is not available, the organization may be forced to purchase packages that it otherwise would develop.
- *Cost of programming*: In case the cost of developing the software is more than the price of pre-written software, the organization may decide to buy the software.
- *Backlog of program:* The in-house software development takes long time. If there is lot of backlog of programs awaiting development, the organization may choose to buy the software.
- *Suitability of software:* Sometimes the available software may not be suitable for specific needs of the organization. Hence, it may be better to develop software in such instances.
- *Time frame available for implementation:* If the time available for implementation of the new computerized system is very short, the organization may decide to buy the software.
- *Availability of sophisticated software*: In many instances, the programs available for purchase are more

sophisticated than the organization would probably develop. For example, many of the applications programs are fully integrated with other application programs. This integration is a powerful incentive for purchasing rather than developing programs.

C. Advantages of Application Packages : The four most compelling advantages of using prewritten application packages are summarised below :

(i) *Rapid implementation:* Application packages are readily available to implement after they are purchased. In contrast, software developed in-house may take months or even years until it is ready for implementation.

(ii) *Low risk:* Since the application package is available in the finished form, the organization knows what it is going to get for the price it has paid. With in-house developed software, the long development time breeds uncertainty with regard to both the quality of the final product and its final cost.

(iii) *Quality:* The firms engaged in application package developments are typically specialist in their products' niche area. Generally, they have a lot of experience in their specialized application field and hence can provide better software. In contrast, in-house programs often have to work over a wide range of application areas; they may not be possessing expertise for undertaking proposed software development.

(iv) *Cost:* Software vendors can leverage the cost of developing a product by selling the product to several other firms, thereby realising a lower cost from each application user. Thus, an application package generally costs less than an in-house developed package. In addition, many hidden costs are faced by organisations that want to develop applications in-house. Hence, application packages, sometimes, turn out to be cheaper compared to in-house developed software.

D. Sources of packaged software : Today, packaged softwares are available in the market from various sources. Computer manufacturers, large and small software houses and computer retail stores are some of the sources from where these packages can be purchased. Another source of packaged software is user groups or associations of users of a particular computer system. User groups often recognise the need for a specific program, which may be developed by one member organisation and made available to other members. For example, utility program and extensions of existing operating systems are typically developed by a member organisation and distributed through the user group. Buying packaged software is risky. Some are difficult to install. There may be undetected bugs in the software, which may create problem at a later stage for the purchaser. Many packages may not be adequately developed and tested. The best method is to deal only with those suppliers who are known for their reputation and who provide after sales support such as training, answering queries and correcting program defects.

E. Steps involved in Selection of A Computer System : The selection of an appropriate computer system, both hardware and application software package demands a high level of expertise and many organisations use a consultant either to provide guidance to their personnel or to manage this activity.

The steps involved in selection of a computer system are:

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

F. RFP (Request For Proposal): is prepared by the organisation and given to vendors, asking the vendors to prepare a bid and submit it to the organisation. The RFP contains all details that are necessary for a vendor to prepare a fully detailed proposal. Typically, the RFP also contains a deadline for bidding, the length of which depends on the complexity of the project- for example, just a few weeks for hardware, and longer periods of time for systems requiring custom development tasks. After responses to RFP have been received, they are evaluated by the organisation. Meetings are scheduled with each vendor, whose bid is competitive in terms of price and meeting the requirements of the RFP. The

participants at each meeting include representatives from the vendor, representatives from the steering committee, and representatives from the design team. The vendor's role is to present its proposal and to answer questions from the other participants. The evaluation committee's role is to listen to the vendor proposals, provide input to the steering committee about the pros and cons of each one, and perhaps make a recommendation for a preferred vendor.

G. Validation of vendors' proposals: This process consists of evaluating and ranking the proposals submitted by vendors and is quite difficult, expensive and time consuming, but in any case it has to be gone through. This problem is made difficult by the fact that vendors would be offering a variety of configurations. The following factors have to be considered towards rigorous evaluation.

Factors for evaluation of vendors' proposal: Following are the factors contributing to evaluation and validation process of vendors' proposals:

(i) Performance rating of the proposed system in relation to its cost: There are quite a few measures of performance such as speed of processing, response time, number of users supported, system configuration etc. One can use the benchmark tests to study the operating efficiency of the system. In this approach, the vendors are provided with the sample data and the task is performed by each vendor which is subsequently examined for accuracy, consistency as well as processing efficiency.

(ii) Cost Benefits of the Proposed system: In this process, the cost benefit analysis is performed in relation to the performance benefits against the Total Cost of Operations (TCO). The accountant should also examine the various options of financing (Purchase or Leasing etc.) in detail. Based on this realistic Cost Benefit Analysis, the decision is taken.

(iii) Maintainability of the Proposed system: It refers to the flexibility and customization scope inbuilt in the proposed system for effective use in the organization. For example, whether the changes occurring due to the federal tax laws and statutory legal requirements can be incorporated in the package easily or not. The maintenance cost of large systems like **ERP** packages is very high, some times manifolds of the initial purchase cost.

(iv) Compatibility with Existing Systems: The proposed system has to be operated in integration with other existing systems, hardware, operating system, application software, etc., in the organization so that it forms a part of the Integrated Enterprise System.

(v) Vendor Support: Another important aspect in validation is the vendor support. In order to implement any application, training, help in implementation and testing, assistance in maintenance and back-up systems are very significant in measuring the vendor support. The availability of "business-hours-only" support versus "round-the-clock" support is yet another important consideration.

Other factors worth considering are:

1. Vendor's past performance in terms of commitment;

2. Availability, quality and cost of:

- Systems Analysts and Programmers for development and customization;
- Maintenance;
- Support in terms of development, programming and hardware installation during conversion period;
- Training to familiarise the employees with the operating characteristics of the new system.
- Computer facility for emergency back-up purpose;
- Support offices proximity for call response time;
- Availability of wide selection of hardware; and
- Choice of systems software.

H. Methods of Validating the proposal: Mandatory requirements would constitute overriding criteria in that, if a vendor fails to meet them, he would be screened out without any further consideration. The desirable characteristics would surely be more difficult to evaluate because the vendors may ignore them or offer several alternatives. The criteria may be listed in a descending order of importance. After having established and ranked the criteria, next comes the question of validating the vendor's proposals against these. The following are some of the validation methods.

(1) Checklists : It is the most simple and rather a subjective method for validation and evaluation. The various criteria

are put in check list in the form of suitable questions against which the responses of the various vendors are validated. Obviously, then, the vendor who has most cleverly and rhetorically worded, his response is likely to get the award. Below we give an example of a software checklist and a support services checklist.

(a) Example of software validation checklist: A user must determine as a first step in assessing a program, whether, on paper, a particular software package meets the requirement specifications established during system analysis. The following features of a package may be ascertained before purchasing the same:

(i) What is the package designed to do?
(ii) How developed is the software package?
(iii) How is the package organised?
(iv) Is the package operable?
(v) Can the package operate on our hardware configuration?
(vi) Can the program provide the needed reports?
(vii) Does the program have adequate capacity in terms of the number of transactions it can process, the number and length of fields per record it can process, the total file size permitted and so on?
(viii) How many processing runs on the computer are required to complete each data processing job? Some programs will perform several tasks each time they are executed. Others may perform only one task per run and hence a program may have to be executed several times, requiring more operator time and computer processing to complete the job.
(ix) How long does the program take to process? The efficiency of program processing varies considerably among the programs that perform the same task. Some may require much more time compared to other programs.
(x) Will the package require modifications?
(xi) Can the package be modified if necessary?
(xii) Who will modify the package?
(xiii) What are the overall costs?
(xiv) Is comprehensive documentation available ?
(xv) Who will maintain the package?
(xvi) What are the package constraints?
(xvii) Where is the package currently utilised?
(xviii) What is the primary language?
(xix) What input/output techniques are utilised?
(xx) What are the required input/output formats?
(xxi) How must input be organised?
(xxii) What controls are included?
(xxiii)What kind of user training is provided?

(b) Example of Support Service Checklists

(i) *Performance* : What has been the vendor's past performance in terms of his past promises?
(ii) *System development* : Are system analysis and programming consultants available? What are their qualities and cost?
(iii) *Maintenance* : Is equipment maintenance provided? What is the quality and cost?
(iv) *Conversion* : What systems development, programming and hardware installation service will they provide during the conversion period?
(v) *Training* : Is the necessary training of personnel provided? What is its quality and cost?
(vi) *Back-up* : Are several similar computer facilities available for emergency back up purposes?
(vii) *Proximity* : Does the vendor have a local office? Are sales, systems development, programming, and hardware maintenance services provided from the office?
(viii) *Hardware* : Do they have a wide selection of compatible hardware?
(ix) *Software* : Do they have a wide variety of useful systems software application programs? Similar checklists may be developed for hardware compatibility etc. This method, however is generally applied only to minor proposals.

(2) **Point-Scoring Analysis in Vendor Evaluation**: 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.

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.

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?	10	8	8	7
Totals	103	79	90	70

(3) **Public evaluation reports:** Several consultancy agencies compare and contrast the hardware and software performance for various manufacturers and publish their reports in this regard. This method has been frequently and usefully employed by several buyers in the past. For those criteria, however, where published reports are not available, resort would have to be made to other methods of validation. This method is particularly useful where the buying staff has inadequate knowledge of computer facts.

I. Bench marking problem for vendorís 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, tape 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 ad effectiveness of software utilities. Bench marking 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 vendor's proposal. The manager can extrapolate in the light of the results of bench marking problems, the performance of the vendors' proposals on the entire job mix.

J. Test problems: Test problems disregard the actual job mix and are devised to test the true capabilities of the hardware, software or system. For example, test problems may be developed to evaluate the time required to translate the source code (program in an assembly or a high level language) into the object code (machine language), response time for two or more jobs in multi-programming environment, overhead requirements of the operating system in executing a user program, length of time required to execute an instruction, etc. The results, achieved by the machine can be compared and price performance judgement can be made.

K. Hardware Contracts and Software Licenses:

Contract: Suppliers should have been issued with draft contracts as an annex to the operational requirements. Draft contracts should be discussed with the suppliers to ensure that the clauses are acceptable to both supplier and purchaser. This stage ensures that all parties understand their respective responsibilities prior to best and final offers being invited.

Software License: A software license is a license that grants permission to do things with computer software. The usual goal is to authorise activities which are prohibited by default by copyright law, patent law, trademark law and any other intellectual property right. The reason for the license, essentially, is that virtually all intellectual property laws were enacted to encourage disclosure of the intellectual property.

L. SOFTWARE DEVELOPMENT

The development of application software undergoes a life cycle similar to the one used to develop the entire system. An in-house creation of programs commonly involves the following six stages :

(i) **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.

(ii) **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.

(iii) **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.

(iv) **Debug the program:** The process of debugging a program refers to correcting programming language syntax and diagnostic errors so that the program “compiles cleanly”. 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.

(v) **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.

1. A brief narrative description of what the program should do.

2. A description of the output, inputs and processing to be performed by the program.
3. A deadline for finishing the program.
4. The identity of the programming languages to use along with coding standards to follow.
5. A description of the system environment into which the program should fit.
6. A description of the testing required to certify the program for use.
7. A description of documentation that must be generated for users, maintenance programmers and operational personnel.

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

(vi) **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.

4.1.7 STAGE V: SYSTEM TESTING

System-level testing must be conducted prior to installation of an information system. It involves: (a) preparation of realistic test data in accordance with the system test plan, (b) processing the test data using the new equipment, (c) thorough checking of the results of all system tests, and (d) reviewing the results with future users, operators and support personnel. 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. During parallel operations, the mistakes detected are often not those of the new system, but of the old. These differences should be reconciled as far as it is feasible economically.

4.1.8 STAGE VI SYSTEMS IMPLEMENTATION AND MAINTENANCE

I. SYSTEM IMPLEMENTATION

The process of ensuring that the information system is operational and then allowing users to take over its operation for use and evaluation is called systems implementation. Implementation includes all those activities that take place to convert from the old system to the new. The new system may be totally new, replacing an existing manual or automatic system or it may be a major modification in an existing system. The four aspects of implementation are:

♦Equipment installation;
♦Training personnel;
♦Conversion procedures; and
♦Post-implementation evaluation.

A. Equipment Installation: The hardware required to support the new system is selected prior to the implementation phase. The necessary hardware should be ordered in time to allow for installation and testing of equipment during the implementation phase. An installation checklist should be developed at this time with operating advice from the vendor and system development team. In those installations where people are experienced in the installation of the same or similar equipment, adequate time should be scheduled to allow completion of the following activities:

1. **Site preparation:** An appropriate location must he found to provide an operating environment for the equipment that will meet the vendor's temperature, humidity and dust control specifications. It is very important to lay down proper procedures for acquiring and planning space layout in the systems implementation. A bad layout can not only drastically reduce the productivity of the data processing department but also that of the entire organization as a whole. If the system is micro computer, little layout and site preparation work is needed. However, the electric lines should be checked to ensure that they are free of static or power fluctuation. It will be better to install a 'clean' line that is not shared by other equipments. In case of mini computer, or a mainframe, the Project Manager should prepare a rough layout, make cost estimates and get budget approved from the management. Layout planning must be done well in advance in order to permit acquisition for long lead-time items like air-conditioning equipments, etc. The following factors should be taken into consideration for space planning:
   - Space occupied by the equipments

- Space occupied by the people, and
- Movement of equipment and people.

The site-layout should allow ample space for moving the equipment in and setting it for normal operation. Vendors will provide clearance requirement for performing services and maintenance and for air circulation. These requirements must be strictly adhered to otherwise warranties may become void and maintenance discontinued until specifications are met. Carpets etc, should be avoided whenever possible in the computer room since they can create static charge which can cause the introduction of errors in the data or, in some case, accidental erase of data. Highly waxed floors produce the same effect. It is best to have the site preparation completed prior to the delivery of the equipment, since vendors are reluctant to deliver equipment when construction work is still in progress.

2. **Equipment installation:** The equipment must be physically installed by the manufacturer, connected-to the power source and wired to communication lines, if required.
3. **Equipment check out:** The equipment must be turned on for testing under normal operating conditions. Not only the routine 'diagnostic test' should be run by the vendor, but also the implementation team should devise and run extensive tests of its own to ensure that equipments are in proper working condition.

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

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

User training: User training may involve equipment use, particularly in the case where a micro-computer is in use and the individual involved is both operator and user. In these cases, users must he 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. Training in data coding emphasises the methods to be followed in capturing data from transactions or preparing data for decision support activities. Users should be trained on data handling activities such as editing data, formulating inquiries (finding specific records or getting responses to questions) and deleting records of data. From time to time, users will have to prepare disks, load paper into printers, or change ribbons on printers. Some training time should be devoted to such system maintenance activities. If a micro computer or data entry system uses disks, users should be instructed in formatting and testing disks.

C. Conversion and start-up from Manual to Computerised System: Conversion or changeover is the process of changing from the old system (manual system) to the new system. It requires careful planning to establish the basic approach to be used in the actual changeover. There are many conversion strategies available to the analyst who has to take into account several organisational variables in deciding which conversion strategy to use.

The five strategies used for conversion from manual to computerised system are briefly discussed below:

(i) **Direct Changeover:** Conversion by direct changeover means that on a specified date, the old system is dropped and the new system is put into use.

Advantages: The users have no possibility of using the old system other than the new one. Adaptation is a necessity.

Disadvantages: Direct changeover can only be successful if extensive testing is done beforehand. Long delays might ensue if errors occur. Also, users may resent being forced into using an unfamiliar system without recourse. Finally, there is no adequate way to compare new results with old ones.

(ii) **Parallel Conversion:** This refers to running the old systems and the new system at the same time, in parallel. This approach works best when a computerised system replaces a manual one. Both systems are run simultaneously for a specified period of time and the reliability of results is examined. When the same results are gained over time, the new system is put into use and the old one is scrapped.

Advantages: There is a possibility of checking new data against old data in order to catch any errors in the processing of the new system. It also offers a feeling of security to users who are not forced to make an abrupt change to the new system.

Disadvantages: Cost of running two systems at the same time is high. The workload of employees during conversion is almost doubled. In case the system being replaced is a manual one, it is difficult to make comparisons between output of the new system and the old one.

(iii) **Gradual Conversion:** It attempts to combine the best features of the earlier two plans, without incurring the risks. In this plan, the volume of transactions is gradually increased as the system is phased in.

Advantages: It allows users to get involved with the system gradually. It also offers the possibility of detecting and recovering from the errors without a lot of downtime.

Disadvantages: It takes too long to get the new system in place. It is not appropriate for conversion of small, uncomplicated systems.

(iv) **Modular Prototype Conversion:** This approach of conversion uses the building of modular, operational prototypes to change from old system to new in a gradual manner. As each module is modified and accepted, it is put into use.

Advantages: Each module is thoroughly tested before being used. Users become familiar with each module as it becomes operational.

Disadvantages: Many times prototyping is not feasible and hence this conversion method cannot be used for such systems. Further, under this approach, special attention must be paid to interfaces so that the modules being built actually work as a system.

(v) **Distributed Conversion**: This refers to a situation in which many installations of the same system are contemplated, such as in banking. One entire conversion is done using any of the aforesaid four approaches at any one site. When that conversion is successfully completed, other conversions are done for other sites.

Advantages: Problems can be detected and contained at one site rather than inflicting them, in succession, on all sites.

Disadvantages: Even when one conversion is successful, each site will have its own peculiarities to work through and these must be handled.

Activities involved in conversion: Conversion includes all those activities which must be completed to successfully convert from the previous system to the new information system. Fundamentally these activities can be classified as follows:

1. Procedure conversion;
2. File conversion;
3. System conversion;
4. Scheduling personnel and equipment;
5. Alternative plans in case of equipment failure.

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 online files (common data base) or offline 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 backup. 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 online and offline 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 cutoff point is established so that data base and other data requirements can be updated to the cutoff 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 deadlines must be met during the emergency. A written manual of procedures concerning what steps must be undertaken will help expedite the unfavourable situation. Otherwise, panic will result in the least efficient methods when time is of the essence.

D. Post-implementation Review: A Post Implementation review answers the questions "did we achieve what we set out to do in business terms? And if not, what should be done?" Much of what an IT project sets out to achieve will not become apparent until well after system implementation.

The specific aims of a Post Implementation Review are to:

♦ evaluate the project team's achievements against the original objectives set out in the Business Case;

♦ measure and compare actual system performance against that specified;

♦ compare actual incurred project costs against the original estimated costs, and make revised cost projections;

♦ *learn for the future in order to avoid repeating mistakes*.

As mentioned earlier that post implementation review measures and compares actual system performance against that specified. There are two basic dimensions of information systems that should be evaluated. The first dimension is concerned with whether the newly developed system is operating properly. The other dimension is concerned with whether the user is satisfied with the information system with regard to the reports supplied by it.

(1) Development evaluation: Evaluation of the development process is primarily concerned with whether the system was developed on schedule and within budget. This is a rather straightforward evaluation. However, it requires schedules and budgets to be established in advance and that records of actual performance and cost be maintained. However, it may be noted that very few information systems have been developed on schedule and within budget.

In fact, many information systems are developed without clearly defined schedules or budgets. Due to the uncertainty and mystique associated with system development, they are not subjected to traditional management control procedures.

(2) Operation evaluation: The evaluation of the information system's operation pertains to whether the hardware, software and personnel are capable to perform their duties and they do actually perform them so. Operation evaluation answers such questions:

1. Are all transactions processed on time?
2. Are all values computed accurately?
3. Is the system easy to work with and understand?
4. Is terminal response time within acceptable limits?
5. Are reports processed on time?
6. Is there adequate storage capacity for data?

Operation evaluation is relatively straightforward if evaluation criteria are established in advance. For example, if the systems analyst lays down the criterion that a system which is capable of supporting one hundred terminals should give response time of less than two seconds, evaluation of this aspect of system operation can be done easily after the system becomes operational.

(3) Information evaluation: The objective of an information system is to provide information to support the organizational decision system. Therefore, the extent to which information provided by the system is supportive to decision making is the area of concern in evaluating the system. However, it is practically impossible to directly evaluate an information system's support for decision making in an organisation. It must be measured indirectly. A viable approach for indirectly measuring and evaluating the information provided by the system has been proposed by Richard L. Nolan and Henery H. Seward. Their approach is based on the concept that the more frequently a decision maker's information needs are met by a system, the more satisfied he tends to be with the system. Conversely, the more frequently necessary information is not available, the greater are the efforts required to obtain the necessary information, and hence, there will be greater dissatisfaction with the information system. Thus, satisfaction can be used as a measure to evaluate the information provided by an information system. Measurement of user satisfaction can be accomplished using the interview and questionnaire technique discussed earlier. If management is generally satisfied with an information system, it is assumed that the system is meeting the requirements of the organisation. If management is not satisfied, modifications ranging from minor adjustments to complete redesign may be required.

II. SYSTEMS MAINTENANCE

Most information systems require at least some modification after development. The need for modification arises from a failure to anticipate all requirements during system design and/or from changing organisational requirements. The changing organisational requirements continue to impact most information systems as long as they are in operation. Consequently periodic systems maintenance is required for most of the information systems. Systems maintenance involves adding new data elements, modifying reports, adding new reports, changing calculations, etc.

Maintenance can be categorised in the following two ways:

1. Scheduled maintenance is anticipated and can be planned for. For example, the implementation of a new inventory coding scheme can be planned in advance.

2. Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate solution. A system that is properly developed and tested should have few occasions of rescue maintenance. One problem that occurs in systems development and maintenance is that as more and more systems are developed, a greater portion of systems analyst and programmer time is spent on maintenance. An information system may remain in an operational and maintenance mode for several years. The system should be evaluated periodically to ensure that it is operating properly and is still workable for the organisation. When a system becomes obsolete i.e. new opportunities in terms of new technology are available or it no longer satisfies the organisation's needs, the information system may be replaced by a new one generated from a fresh system development process.

4.2 ALTERNATE DEVELOPMENT METHODOLOGY

Various alternative approaches are discussed below:

(i) Prototyping approaches: The traditional approach sometimes may take years to analyse, design and implement a system. In order to avoid such delays, organisations are increasingly using prototyping techniques 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. As users work with the prototype, they make suggestions about the ways to improve it. These suggestions are then incorporated into another prototype, which is also used and evaluated and so on. Finally, when a prototype is developed that satisfies all user requirements, either it is refined and turned into the final system or it is scrapped. If it is scrapped, the knowledge gained from building the prototype is used to develop the real system. Experimenting with the prototype helps users to identify additional requirements and needs that they might have overlooked or forgotten to mention. In addition, with prototyping, users have a clearer visual picture of what the final version will look like and they do not have to sign off on a system which is presented to them in the form of diagrams and specification lists.

Steps involved in prototyping for systems development

Step 1: Identify Information System Requirements: In traditional approach, the system requirements have to be identified before the development process start. However, under prototype approach, the design team needs only fundamental system requirements to build the initial prototype, the process of determining them can be less formal and time-consumingthan when performing traditional systems analysis. (The team can develop the detailed requirements of the system later after users have had time to interact with the prototype and provide feedback.)

Step 2: Develop the Initial Prototype: In this step, the designers create an initial base model – for example, using fourth-general programming languages or CASE tools. In this phase, the goals are “rapid development” and “low cost.” Thus, the designers give little or no consideration to internal controls, but instead emphasize such system characteristics as “simplicity,” “flexibility,” and “ease of use.” These characteristics enable users to interact with tentative versions of data entry display screens, menus, input prompts, and source documents. The users also need to be able to respond to system prompts, make inquiries of the information system, judge response times of the system, and issue commands.

Step 3: Test and Revise: After finishing the initial prototype, the designers first demonstrate the model to users and then give it to them to experiment. At the outset, users must be told that the prototype is incomplete and requires subsequent modifications based on their feedback. Thus, the designers ask users to record their likes and dislikes about the system and recommend changes. Using this feedback, the design team modifies the prototype as necessary and then resubmits the revised model to system users for reevaluation. Thus iterative process of modification and reevaluation continues until the users are satisfied – commonly, through four to six interactions.

Step 4: Obtain User Signoff of the Approved Prototype: At the end of Step 3, users formally approve the final version of the prototype, which commits them to the current design and establishes a contractual obligation about what the system will, and will not, do or provide. Approximately half of these approved prototypes become fully functional systems. The remaining, throwaway prototypes are not developed – typically because the modifications required to make them functional are too costly or in other ways not practical. But this does not mean that type prototyping exercise has been a failure. To the contrary, it signals an impractical system and thus saves an organisation a great deal of time and money!

In general, the procedure is useful when one or more of the following conditions exist:
1. End users do not understand their informational needs very well.
2. System requirements are hard to define.
3. The new system is mission-critical or is needed quickly.
4. Past inter actions have resulted in misunderstandings between end users and designers.
5. The risks associated with developing and implementing the wrong system are high.

Advantages of Prototyping

1. Prototyping requires intensive involvement by the system users. Therefore, it typically results in a better definition of these users' needs and requirements than does the traditional systems development approach.
2. A very short time period (e.g., a week) is normally required to develop and start experimenting with a prototype. This short time period allows system users to immediately evaluate proposed system changes. In contrast, it may take a year or longer before system users can evaluate proposed system changes when the traditional systems development approach is used.
3. Since system users experiment with each version of the prototype through an interactive process, errors are hopefully detected and eliminated early in the developmental process. As a result, the information system ultimately implemented should be more reliable and less costly to develop than when the traditional systems development approach is employed.

Disadvantages of Prototyping

1. Prototyping can only be successful if the system users are willing to devote significant time in experimenting with the prototype and provide the system developers with change suggestions. The users may not be able or willing to spend the amount of time required under the prototyping approach.
2. The interactive process of prototyping causes the prototype to be experimented with quite extensively. Because of this, the system developers are frequently tempted to minimize the testing and documentation process of the ultimately approved information system. Inadequate testing can make the approved system error-prone, and inadequate documentation makes this system difficult to maintain.
3. Prototyping may cause behavioral problems with system users. These problems include dissatisfaction by users if system developers are unable to meet all user demands for improvements as well as dissatisfaction and impatience by users when they have to go through too many interactions of the prototype.

(ii) End user development approach : With the increasing availability of low-cost technology, end user development is becoming popular in many organisations. 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. The number and nature of systems development activities followed by the end-user often differ from those found in formal approaches such as the traditional approach.
The risks involved in this approach include the following:
1. A decline in standards and controls. When an analyst is in-charge of developments, walkthrough will be done and standards and policies will be enforced; these things are unlikely to be carried out to the same degree with end-user computing.
2. Inaccuracy of specification requirements. The end-user will not have the experience of an analyst in completing an accurate specification of system requirements.
3. There would be a *reduction in the quality assurance and stability* of the system due to the lack of adequate specifications
4. An increase in unrelated and incompatible systems: Departments would choose their own software and hardware and incompatibility of systems would result; this would mean that management would have difficulty in obtaining full corporate data.
5. Difficulties in accessing central system, such as the corporate database, could arise with a proliferation of different systems and applications.

(iii) 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. In a very small organisation, no MIS professional may be on the staff. However, this does not mean that it is not possible for them to develop new systems. Many smaller firms have developed good systems by using systematic approach. 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.

In the systematic approach, after information-processing requirements are determined, a search for suitable software becomes the primary focus. Once it is located, hardware is selected and the system is put together and used. It may be noted that managers in organisations employing a large number of MIS professionals may also use a systematic approach to develop the office information systems used in their own immediate work areas.

(iv) Rapid application development (RAD) : As the pace of change has increased the approach to systems analysis and design described above has been criticised on the grounds that it is too slow and too costly. Recent years has seen the introduction of new system design and engineering tools which are intended to speed up the development process; Rapid Application Development or RAD is the term assigned to these new tools and techniques. The principle underlying RAD is that it is possible to satisfy 80% of the functionality required in 20% of the time by concentrating on key business requirements. The danger from the auditor's point of view is that system controls might be overlooked or compromised in the interests of expediency. The key features of the approach can be summarised as cheap, quick and adequate. RAD is particularly suited to rapidly changing business areas where there is a danger that the use of traditional analysis and design methods could lead to delivery of a product after the need for it has passed.

The RAD philosophy is based on several key assumptions:

♦it is impossible to specify requirements accurately without iteration;

♦the application is its own model;

♦design and testing are iterative processes;

♦the application is always complete, but never finished;

♦empowerment of users is crucial to the development of effective information systems -management should concentrate on specifying targets in terms of what should be achieved and let their staff determine how to meet the targets.

RAD Methods : RAD can be seen to be a complete approach to information system development in that it covers the entire information systems development lifecycle, from initiation through to delivery. RAD is more of a philosophy than a precise science. The methods currently available include:

♦ the James Martin method (one of the first methods); and

♦ the Dynamic Systems Development Method (DSDM), which was put together by a consortium and made openly available.

RAD methods typically combine several sub-methods including project management, quality assurance and software testing. RAD does not proposed the adoption of radical development techniques; it adopts components of traditional design and development techniques as and when they are felt to be useful.

RAD components : The fluidity and pragmatism of the approach make it difficult to generalize about RAD. The sections which follow outline some common components.

(a) *Joint Application Development (JAD)* : RAD is characterised by small development teams of between four and eight members. These teams include developers and users and are empowered to make design decisions. The teams combine the developers skills with the users knowledge of the business. The teams are usually expected to come up with fully documented business requirements in three to five days. Further workshops may be scheduled to develop particular aspects of the application.

(b) *Rapidity of development* : Most RAD developments are relatively small scale (based on PC and client server technology) and last a short time (3-6 months). The commonly held view is that projects lasting more than 6 months are

likely to be overtaken by changes in the business environment. Hence the need to get systems in place and operational as soon as possible. Two months is seen as being the typical length of a RAD project. RAD practitioners believe that no more than six man-years of development work should be devoted to any particular RAD project.

(c). *Clean rooms* : JAD workshops usually take place away from the normal office environment which is free from any routine work interruptions. Once in the clean rooms the teams concentrate on highly focused problem solving. The clean rooms need to be supplied with appropriate support facilities such as flip-charts, pens, OHP, coffee, computers etc.

(d). *Timeboxing* : RAD project control involves scoping the project by prioritising and defining delivery deadlines or "timeboxes". If projects start to fall behind schedule the requirements are reduced instead of increasing or putting back the deadline.

(e). *Incremental prototyping:* RAD applications are put together or built in an iterative way. The process is commonly known as incremental prototyping. System developers build working models after some initial investigation. The model is shown to and discussed with users. Amendments and enhancements are agreed and incorporated into the next model. The cycle of inspection, discussion and amendment is repeated several times, each time moving closer to an acceptable system.

RAD tools : RAD makes use of latest development tools e.g. 4GLs, GUI builders, DBMS, and CASE tools. These allow developers to build prototypes as they progress. Most RAD projects involve the construction of applications that are highly interactive, have clearly defined user groups and are not computationally complex. RAD techniques are rarely used for large distributed systems. The infrastructure for large scale complex projects is best put in place before the RAD applications are built so that RAD teams can then concentrate on the application without worrying about the underlying infrastructure. One of the potential problems with the widespread use of RAD is the duplication of corporate information and inconsistency in the way that it is held. This problem can be avoided if the corporate database is centrally administered as a resource shared by RAD teams. For this approach to be adopted the core database has to be established before the RAD teams can build applications that interact with it.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
				2	What is a system development Life-cycle?
				5	Discuss the various activities which are part of the system development life cycle.
				12	Bring out the reasons as to why the organizations fail to achieve their Systems Development Objectives?
				10	What are the various Tangible and Intangible benefits that can result from the development of a computerised system ?
				5	What are the fact finding techniques used by a system analyst?
				5	Describe any five functional areas of a system which needs to be analyzed by system analyst for detailed investigation of the present system.
				10	Describe briefly four categories of the major tools that are used for system development.
				5	Write short note : Data Dictionary
				10	What are the six important factors which should be considered while designing the user outputs?
				10	What are the factors considered to design the ideal layout of a printed output?
				10	What are the major factors to be considered in

					designing User inputs? Explain.
				5	Suggest suitable guidelines to be followed for efficient form design.
				5	Discuss the desired characteristics of a good coding system.
				4	Write Short Note : System Manual
				2	What is application software?
				4	Discuss the factors upon which "Make or Buy" decision of application software depends.
				4	Enumerate the advantages of prewritten application software packages.
				5	List the various sources of acquiring the software.
				5	State the steps involved in selection of computer systems.
				10	What is Vendor evaluation? Define the process for the same.
				5	Briefly discuss about various factors which should be considered for evaluating the vendor proposal for supply of computer system.
				4	Write Short Note : Point Scoring analysis in Vendor Evaluation
				5	Discuss Bench marking problem on vendor's proposal.
				10	Discuss various stages through which an in-house creation of program has to pass.
				5	Write short note: Program documentation.
				10	What is prototyping approaches to systems development? Describe its advantages and disadvantages also.
				8	Discuss the four steps of the prototyping approach in system development
				5	End user development approach in system development
				5	Briefly describe various steps involved in system testing.
				10	Why is personnel training important for the successful implementation of information system? What type of training should be imparted to (i) systems operator and (ii) users
				5	Why is personnel training important? What type of training should be imparted to users?
				10	Describe various steps that should be taken for successful installation of the equipment during the implementation phase.
				5	Explain the different conversion strategies used for conversion from a manual to a computerized system.

				3	Discuss briefly the advantages and disadvantages of any one conversion strategy.
				5	Describe various strategies for change over from manual system to computerised.
				10	Explain briefly various activities that should be completed for successful conversion of an existing system to the new information system.
				10	"The final step of the system implementation is its evaluation." What functions are being served by the system evaluation? Discuss development, operation and information evaluations.
				5	Write short note : System Maintenance
				4	If you are the Project Manager of a Software Company with the responsibility for developing a break-through product, combining state of the art hardware and software, will you opt for prototyping as a process model for a product meant for the intensely competitive entertainment market?
Nov-08	[2(a)]	2		10	State and briefly explain the six stages of System Development Life Cycle (SDLC).
Nov-08	[7(a)]	2		5	Advantages of Application Packages
Nov-08	[7(d)]	2		5	Information System Maintenance.
Jun-09	[2(a)]	2		10	The top management of company has decided to develop a computer information system for its operations. Is it essential to conduct the feasibility study of system before implementing it? If answer is yes, state the reasons. Also discuss three different angles through which the feasibility study of the system is to be conducted.
Jun-09	[7(a)]	2		5	System Manual

3 - CONTROL OBJECTIVES

1. NEED FOR CONTROL

Everyone is aware of the need for information security in today's highly networked business environment. Information is arguably among an enterprise's most valuable assets, so its protection from predators from both within and outside has taken center stage as an IT priority. Hence, there is a need to institute strong control environment.

2. EFFECT OF COMPUTERS ON INTERNAL AUDIT

Since the 1970s, around the world there has been a large increase in the number of organisations using computers to process transactions and prepare their financial statements. The move towards more automated financial systems has had an impact in the way auditors carry out their work. The impact can be summarised under four main headings:

(i) changes in the audit trail and audit evidence;

(ii) change in the internal controls environments;

(iii) new opportunities and mechanisms for fraud and error; and

(iv) new audit procedures.

Each of these effects are discussed in these notes.

(i) Changes in the audit trail and audit evidence: The existence of an audit trail is a key financial audit requirement, since without an audit trail, the financial auditor may have extreme difficulty in gathering sufficient, appropriate audit evidence to validate the figures in the client's accounts.

(a) Data retention and storage: A client's storage capabilities may restrict the amount of historical data that can be retained "on-line" and readily accessible to the auditor. If the client has insufficient data retention capacities the auditor may not be able to review a whole reporting period's transactions on the computer system.

(b) *Absence of input documents*: Transaction data may be entered into the computer directly without the presence of supporting documentation, e.g. input of telephone orders into a telesales system. The increasing use of EDI will result in less paperwork being available for audit examination.

(c) Lack of a visible audit trail: The audit trails in some computer systems may exist for only a short period of time. The absence of an audit trail will make the auditor's job very difficult and may call for an audit approach which involves auditing around the computer system by seeking other sources of evidence to provide assurance that the computer input has been correctly processed and output.

(d). Lack of visible output: The results of transaction processing may not produce a hard copy form of output, i.e. a printed record. In the absence of physical output it may be necessary for the auditor to directly access the electronic data retained on the client's computer. This is normally achieved by having the client provide a computer terminal and being granted "read" access to the required data files. (See chapter 9 for an explanation of access permissions such as 'read').

(e) Audit evidence. Certain transactions may be generated automatically by the computer system. For example, a fixed asset system may automatically calculate depreciation on assets at the end of each calendar month. The depreciation charge may be automatically transferred (journalised) from the fixed assets register to the depreciation account and hence to the client's income and expenditure account. Where transactions are system generated, the process of formal transaction authorisation may not have been explicitly provided in the same way as in a manual environment, i.e. each transaction is not supported by the signature of a manager, supervisor or budget holder. This may alter the risk that transactions may be irregular or ultra vires.

(f) Legal issues: The use of computers to carry out trading activities is also increasing. More organisations in both the public and private sector intend to make use of EDI and electronic trading over the Internet. This can create problems with contracts, e.g. when is the contract made, where is it made (legal jurisdiction), what are the terms of the contract and who are the parties to the contract.

(ii) Change in the type and nature of internal controls: The internal controls within a client's financial systems, both

manual and computerised, can be divided into several categories.
• *Personnel* : Whether or not staff are trustworthy, if they know what they are doing and, if they have the appropriate skills and training to carry out their jobs to a competent standard.
• *Segregation of duties*: a key control in any financial system. Segregation basically means that the stages in the processing of a transaction are split between different people, such that one person cannot process a transaction through from start to finish. The various stages in the transaction cycle are spread between two or more individuals.
• *Authorisation procedures*: to ensure that transactions are approved. In some on-line transaction systems written evidence of individual data entry authorisation, e.g. a supervisor's signature, may be replaced by computerised authorisation controls such as automated controls written into the computer programs (e.g. programmed credit limit approvals).
• *Record keeping*: the controls over the protection and storage of documents, transaction details, audit trails etc.
• *Access to assets and records:* In the past manual systems could be protected from unauthorised access through the use of locked doors and filing cabinets. Computerised financial systems have not changed the need to protect the data. A client's financial data and computer programs are vulnerable to unauthorised amendment at the computer or from remote locations. The use of wide area networks, including the Internet, has increased the risk of unauthorised access. The nature and types of control available have changed to address these new risks.
• *Management supervision and review*: Management's supervision and review helps to deter and detect both errors and fraud.

(iii) New causes and sources of error

(a) System generated transactions: Financial systems may have the ability to initiate, approve and record financial transactions. This is likely to become increasingly common as more organisations begin to install expert systems and electronic data interchange (EDI) trading systems. Automated transaction processing systems can cause the auditor problems. For example when gaining assurance that a transaction was properly authorised or in accordance with delegated authorities. The auditor may need to look at the application's programming to determine if the programmed levels of authority are appropriate.

(b) Systematic Error **:** Computers are designed to carry out processing on a consistent basis. Given the same inputs and programming, they invariably produce the same output. This consistency can be viewed in both a positive and a negative manner. If the computer is doing the right thing, then with all other things being equal, it will continue to do the right thing every time. Similarly, if the computer is doing the wrong thing and processing a type of transaction incorrectly, it will continue to handle the same type of transactions incorrectly every time. Therefore, whenever an auditor finds an error in a computer processed transaction, s(he) should be thorough in determining the underlying reason for the error. If the error is due to a systematic problem, the computer may have processed hundreds or thousands of similar transactions incorrectly

(iv) New audit processes : Within a computerised environment the auditor may be required to adopt a different audit approach to gain sufficient audit evidence to provide an opinion on the financial statements. For example, new procedures to cope with different internal controls, new causes of errors or the different nature of audit trails.

3. RESPONSIBILITY OF CONTROLS

Management is responsible for establishing and maintaining control to achieve the objectives of effective and efficient operations, and reliable information systems. Management should consistently apply the internal control standards to meet each of the internal control objectives and to assess internal control effectiveness. The information system managers must take systematic and proactive measures to

(i) Develop and implement appropriate, cost-effective internal control for results-oriented management;

(ii) Assess the adequacy of internal control in programs and operations;

(iii) Separately assess and document internal control over information systems consistent with the information security policy of the organization

(iv) Identify needed improvements;

(v) Take corresponding corrective action; and

(vi) Report annually on internal control through management assurance statements.

4. COST EFFECTIVENESS OF CONTROL PROCEDURE

The benefit of an internal control must not exceed its cost. For example, at one of the multinational company, data errors occasionally required the entire payroll to be reprocessed, at a cost of $ 10,000. Management determined that a data validation step would reduce error risk from 15 per cent to 1 per cent, at a cost of $600 per pay period. The cost-benefit analysis that management used to determine if the validation step should be employed is as below:

If the proposed payroll validation procedure is not utilised, then the expected loss to the company is $1,500. Because the expected loss with the validation step is $100, the control provides an expected benefit of $1,400. After deducting the control costs of $600, the validation step provides a net benefit of $800 and clearly should be implemented.

5. CONTROL OBJECTIVES FOR INFORMATION RELATED TECHNOLOGY(COBIT)

The Information Systems Audit and control Foundation (ISACF) developed the Control Objectives for Information and related Technology (COBIT). COBIT is a framework of generally applicable information systems security and control practices for IT control. The framework allows

(1) management to benchmark the security and control practices of IT environments,

(2) users of IT services to be assured that adequate security and control exist, and

(3) auditors to substantiate their opinions on internal control and to advise on IT security and control matters.

The framework addresses the issue of control from three vantage points, or dimensions:

1. *Business Objectives*. To satisfy business objectives, information must conform to certain criteria that COBIT refers to as business requirements for information. The criteria are divided into seven distinct yet overlapping categories that map into the COSO objectives: effectiveness (relevant, pertinent, and timely), efficiency, confidentiality, integrity, availability, compliance with legal requirements, and reliability.
2. *IT resources*, while include people, application systems, technology, facilities, and data.
3. *IT processes*, which are broken into four domains: planning and organization, acquisition and implementation, delivery and support, and monitoring.

COBIT, which consolidates standards from 36 different sources into a single framework, is having a big impact on the information systems profession. It is helping managers learn how to balance risk and control investment in an information system environment. It provides users with greater assurance that the security and IT controls provided by internal and third parties are adequate. It guides auditors as they substantiate their opinions and as they provide advice to management on internal controls.

6. INFORMATION SYSTEMS CONTROL TECHNIQUES

The basic purpose of information system controls in an organization is to ensure that the business objectives are achieved and undesired risk events are prevented or detected and corrected. This is achieved by designing and effective information control framework, which comprise policies, procedures, practices, and organization structure that gives reasonable assurances that the business objectives will be achieved. When reviewing a client's control systems, the auditor will be able to identify three components of internal control. Each component is aimed at achieving different objectives.

The information system auditor will be most familiar with:

• Accounting controls, i.e. those controls which are intended *to safeguard the client's assets and ensure the reliability of the financial records;*

The other two types of control likely to be encountered are:

• Operational controls: These deal with *the day to day operations, functions and activities to ensure that the operational activities are contributing to business objectives;*

• Administrative controls*:* These are concerned with *ensuring efficiency and compliance with management policies, including the operational controls.*

6.1 Auditor's categorisation of controls : When we look at financial or accounting controls we examine them to see if

they reduce the likelihood of the financial statements containing material errors. We put the controls into categories depending on when they act.
We categorise the controls into following four groups:
(i). Preventive Controls: Preventive controls are those inputs, which are designed to prevent an error, omission or malicious act occurring. An example of a preventive control is the use of passwords to gain access to a financial system. The broad characteristics of preventive controls are:
(i) A clear-cut understanding about the vulnerabilities of the asset
(ii) Understanding probable threats
(iii) Provision of necessary controls for probable threats from materializing
Any control can be implemented in both a manual and computerized environment for the same purpose. Only, the implementation methodology may differ from one environment to the other. Now let us discuss the examples of preventive controls and how the same control is implemented in different environments.
Examples of preventive controls
• Employ qualified personnel
• Segregation of duties
• Access control
• Vaccination against diseases
• Documentation
• Prescribing appropriate books for a course
• Training and retraining of staff
• Authorization of transaction
• Validation, edit checks in the application
• Firewalls
• Anti-virus software (sometimes this acts like a corrective control also), etc
• Passwords
The above list in no way is exhaustive, but is a mix of manual and computerized, preventive controls. The following table shows how the same purpose is achieved by using manual and computerized controls.
(ii). Detective Control: These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. An example of a detective control would be the use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend. The main characteristics of such controls are as follows:
• Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc.
• An established mechanism to refer the reported unlawful activities to the appropriate person or group
• Interaction with the preventive control to prevent such acts from occurring
• Surprise checks by supervisor
Examples of detective controls include
• Hash totals
• Check points in production jobs
• Echo control in telecommunications
• Error message over tape labels
• Duplicate checking of calculations
• Periodic performance reporting with variances
• Past-due accounts report
• The internal audit functions
• Intrusion detection system
• Cash counts and bank reconciliation
• Monitoring expenditures against budgeted amount
(iii). Corrective Controls: Corrective controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the

incorrect date. A business continuity plan is considered to be a significant corrective control. The main characteristics of the corrective controls are:
• Minimize the impact of the threat
• Identify the cause of the problem
• Remedy problems discovered by detective controls
• Get feedback from preventive and detective controls
• Correct error arising from a problem
• Modify the processing systems to minimize future occurrences of the problem
Examples of Corrective Controls
• Contingency planning
• Backup procedure
• Rerun procedures
• Treatment procedures for a disease
• Change input value to an application system
• Investigate budget variance and report violations.
(Iv). Compensatory Controls: Controls are basically designed to reduce the probability of threats, which can exploit the vulnerabilities of an asset and cause a loss to that asset. While designing the appropriate control one thing should be kept in mind—*the cost of the lock should not be more than the cost of the assets it protects*. Sometimes while designing and implementing controls, organizations because of different constraints like financial, administrative or operational, may not be able to implement appropriate controls. In such a scenario, there should be adequate compensatory measures which may although not be as efficient as the appropriate control, can indubitably reduce the probability of threats to the assets. Such measures are called compensatory controls.

6.2 Audit Trails: Audit trails are logs that can be designed to record activity at the system, application, and user level. When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives. Many operating systems allow management to select the level of auditing to be provided by the system. This determines which events will be recorded in the log. An effective audit policy will capture all significant events without cluttering the log with trivial activity.
Audit Trail Objectives : Audit trails can be used to support security objectives in three ways:
• Detecting unauthorized access to the system,
• Facilitating the reconstruction of events, and
• Promoting personal accountability.
Each of these is described below:
(1) Detecting Unauthorized Access: Detecting unauthorized access can occur in real time or after the fact. The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls. A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by a virus or worm. Depending upon how much activity is being logged and reviewed, real-time detection can impose a significant overhead on the operating system, which can degrade operational performance. After-the-fact detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.
(2) Reconstructing Events: Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors. Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future. Audit trail analysis also plays an important role in accounting control. For example, by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.
(3) Personal Accountability: Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behavior. Individual are likely to violate an organisation's security policy if they know that their actions are recorded in an audit log.

6.3 User Controls: Validity of computer application systems output lies ultimately with the user. The user is responsible for data submission and for correction of errors that are the result of inaccurately submitted data. User controls over data being processed should include:

(a). User instruction manuals defining responsibilities and actions;

- Input controls that identify all data entering the processing cycle;
- Processing control information that includes edits, error handling, audit trails and master file changes;
- Output controls that define how to verify the correctness of the reports;
- Separation of duties between preparing the input and balancing the output

6.4 Error Correction

1. Identify all data and processing errors that can be identified, either through edits or routine processing.
2. Determine the impact data and processing errors have on processing (errors must be corrected before processing continues, errors are segregated from processing so good transactions may continue to be processed while errors are corrected).
3. Determine if errors are segregated onto a suspense file. Determine if the error suspense file is cumulative or non-cumulative.
4. Review the error reports to determine if they are of reasonable length.
5. Determine how errors are corrected.
6. Determine if the corrected transactions are authorized.
7. Verify that the corrected transactions are reintroduced into mainstream processing either at the original point of input or through a special error correction process.
8. Determine if the error correction process removes the items from the error suspense file
9. Determine the timeliness of error correction.
10. Identify how end-users monitor the remaining errors and conduct timely further investigations.
11. Is there an appropriate separation of duties (custody, authorization, recording, and periodic reconciliations) for those authorized to update data?
12. Determine if all reconciliation and error correction procedures are documented in the end-user documentation.
13. Is an exception report generated for long-outstanding error transactions, with an aging analysis?

7. SYSTEM DEVELOPMENT AND ACQUISITION CONTROLS

Summary of Key Maintainability Controls

Control Category	**Threats/Risks**	**Controls**
System development and acquisition controls	System development projects consume excessive resources.	Long-range strategic master plan, data processing schedules, assignment of each project to a manage and team, project development plan, project milestones, performance evaluations, system performance measurements (throughput, utilization, response time), and post-implementation reviews.
Change management controls	Systems development projects consume excessive resources, unauthorised systems changes.	Change management control policies andprocedures, periodic review of all systems for needed changes, standardized format for changes, log and review change requests, assess impact of changes on system reliability, categorise and rank all, changes, procedures to handle urgent matters, communicate changes to management and users, management approval of changes, assign specific

		responsibilities while maintaining adequate segregation of duties, control go through all appropriate steps, these all changes, develop plan for backing out of mission-critical system changes, implement a quality assurance functions and update documentation and procedures

System development and acquisition control include the following key elements:
1. ***Strategic master plan***. There is a need for a strategic master plan.
2. ***Project controls*****.** A project development plan shows how a project will be completed, including the modules or tasks to be performed, who will perform them, the dates they should be completed, and the cost of each. The plan should specify project milestones or significant points when progress is reviewed and actual and estimated completion times are compared.ch project should be assigned to a manager and team who should be held responsible for the success or failure of the project. A performance evaluation of the project team members should be done as each plan is completed.
3. **Data processing schedule.** To maximize the use of scarce computer resources, all data processing tasks should be organized according to a data processing schedule**.**
4. ***System performance measurements*****.** For a system to be evaluated properly, it must be assessed using system performance measurements. Common measurements include throughput (Output per unit of time), Utilization (Percentage of time the system is being productively used, and response time (how long it takes the system to respond).
5. ***Post-implementation review*****.** After a development project is completed a post implementation review should be performed to determine if the anticipated benefits were achieved. Reviews help to control project development activities and to encourage accurate and objective initial cost and benefit estimates.

8. CONTROLS OVER SYSTEM IMPLEMENTATION

8.1 Acceptance testing: Acceptance testing is a complete end-to-end test of the operational system including all manual procedures. It aims to provide the system users with confirmation that:-
• the User Requirement Specification (including system performance criteria) has been met;
• end user and operational documentation is accurate, comprehensive, and usable;
• supporting clerical procedures work effectively;
• Help Desk and other ancillary support functions operate correctly and as expected;
• back-up and recovery procedures work effectively.

Deferent type of acceptance testing:

(*i). Performance testing should address:-*

 average response time: usually defined as the time between the user depressing the transmit key, and the first character of the reply appearing on the screen, with a further maximum time specified for the screen to be completed;
 maximum response time: the response time that must not be exceeded;
 other response times: for example the time to:-
• load an application;
• load a major application;
• accept or move between fields on the screen;
• perform a single update;
• perform a multiple update;
• run a complex enquiry

(ii). Volume testing: subjects the system to heavy volumes of data to test whether it can handle the volume of data specified in an acceptable time-frame;
(iii). Stress testing: subjects the system to heavy loads or stresses (a heavy stress is a peak volume of data encountered over a short period).
(iv). Security testing: attempts to subvert the system's security and internal control checks;

(v). Clerical procedures checking: aims to confirm that all supporting clerical procedures have been documented and work effectively;

(vii). Back-up and recovery: aims to confirm that software, configuration files, data and transaction logs can be backed up, either completely or selectively; and also restored from backup;

(viii). Parallel operation

8.2 Role of IS Auditor: An illustrative list of the different issues that the auditor might need to consider when reviewing the various stages of testing is given below. Note that issues vary with the nature and scale of the development project.

a) Has a manager(s) with adequate authority been appointed to take overall charge of the data conversion and acceptance testing programmes?

b) Has a Data Conversion Plan been drawn up?

c) Does the Data Conversion Plan :-

• describe the data conversion strategy to be followed (e.g. the procedures for reconciling differing charts of accounts; the sequence of files to be converted; the conversion timetable; keeping converted data up-to-date)?

• allocate staff to each task (the users should be fully involved) and define specific roles and responsibilities, including that of signing off successful completion of each task?

• set out the criteria for identifying and resolving problems on the quality of the existing data (e.g. undertake file interrogation to identify missing or incompatible data items in the existing system; define procedures to deal with the correction of data rejected by the new system)?

• acceptance test any bespoke software that has been developed to support the data conversion task?

• define the controls that are to give assurance that data has been transferred completely and accurately, and correctly posted (e.g. hash and control totals, and record counts; checking a sample of detailed records back to the old system; reconciling balances between the two systems)?

• implement an effective separation of roles between those involved in transferring data and those involved in verifying that it has been correctly transferred (information security should not be neglected, particularly where financial data is involved)?

• define procedures to ensure that converted data is kept up-to-date following its transfer to the new system?

• define back up and recovery procedures for the converted data on the new system (these procedures will not relate to any processing cycle so they may differ from the eventual operational procedures)?

• define how the audit trail is to be preserved after cut over; also, how archived data from the old system will be processed after de-commissioning?

d) What arrangements have been made to ensure that the system has been correctly built (installed, configured, loaded, etc) before user acceptance testing commences?

e) Has an Acceptance Test Plan been drawn up to cover all aspects of testing?

f) Will user acceptance testing sufficiently exercise the live environment? (where testing takes place in a development environment, it is unlikely that this will provide adequate assurance that the new system will run correctly in its intended environment. This applies particularly to distributed systems that comprise extensive telecommunication networks);

g) Does the Acceptance Test Plan :-

• *allocate adequate resources* in terms of manpower, time and equipment to acceptance testing? (A common problem in IT projects is to reduce the time available for acceptance testing in order to recover from slippage in the overall project timetable. This can easily result in the implementation of an inadequately tested system and defective system);

• *allocate individual roles and responsibilities* for :-

♦ managing the test environment? (i.e. environment design; configuration management; operation and maintenance)

♦ undertaking individual tests and test cycles?

♦ recording test result?

♦ analysing test results and prioritising errors?

• fully *involve the end-users* in the design and execution of the acceptance testing programme?

• include ancillary procedures? (e.g. clerical control checks, the Help Desk, Network Support, System Administration);

• require the *manager in charge to sign off* individual tests and test cycles on successful completion?
h) Has a *Configuration Manager* been appointed to perform such tasks as :-
• keeping test plans, documents and test suites in step with software versions?
• providing management reports on the status of items under test?
• ensuring that change management procedures are observed?
i) Is there an *adequate separation of roles* to help guard against unauthorized changes taking place during testing and error correction? (e.g. between individuals involved in building and modifying configuration items; those involved in testing them; and those involved in releasing them into live use);
j) Are there *adequate access controls* in place to prevent unauthorized changes being made to configuration items during testing and error correction?
k) Have *test data been prepared for each test*? Have the anticipated results for each test been fully defined?
l) Do tests cover events that ought not to happen, as well as those that should? (e.g. dothey include out of range tests; tests on processing acceptable items occurring in unacceptable combinations; duplicate transaction processing; incomplete master and standing data files);
m) Does user the Acceptance Testing Plan cover all aspects of the User Requirements Specification?
n) Are changes to defective configuration items managed in accordance with the project's change management procedures?
o) Is an adequate audit trail of changes maintained? (is it possible to back-track on a change to see how it occurred and whether it was correctly authorised?)
p) Are regression tests carried out to ensure that previously accepted areas of the new system continue to work after significant changes have been implemented?
q) Has the acceptance-testing programme been signed off by the Project Board on successful completion? If not, is appropriate remedial action being taken?

8.3 The Post Implementation Review (PIR): The Overall, the PIR should establish in an impartial manner whether a new system has met its:-
• *business objectives (delivered within budget and deadline; is producing predicted savings and benefits, etc.)*
• *user expectations (user friendly, carries the workload, produces the required outputs, good response time, reliable, good ergonomics, etc.);*
• *technical requirements (capable of expansion, easy to operate and maintain, interfaces with other systems, low running cost, etc.).*

Activities to be undertaken : During a PIR, the team should, according to their terms of reference, review:-
• *the main functionality of the operational system against the User Requirements Specification;*
• *system performance and operation;*
• *the development techniques and methodologies employed;*
• *estimated time-scales and budgets, and identify reasons for variations;*
• *changes to requirements, and confirm that they were considered, authorised and implemented in accordance with change and configuration management standards;*
• *set out findings, conclusions and recommendations in a report for the authorizing authority to consider.*
• *In addition to reviewing the functionality delivered by the new system, the review team will also need to look back to the Business Case on which the system was originally based to confirm that all the anticipated benefits, both tangible and intangible, have been delivered.*

Control considerations : The following issues should be considered when judging the effectiveness either of a PIR, or to form the basis for the auditor to undertake one.
a) Interview business users in each functional area covered by the system, and assess their satisfaction with, and overall use of, the system.
b) Interview security, operations and maintenance staff and, within the context of their particular responsibilities, assess

their reactions to the system.

c) Based on the User Requirements Specification, determine whether the system's requirements have been met. Identify the reason(s) why any requirements are not to be provided, are yet to be delivered, or which do not work properly.

d) Confirm that the previous system has been de-commissioned or establish the reason(s) why it remains in use.

e) Review system problem reports and change proposals to establish the number and nature (routine, significant, major) of problems, and changes being made to remedy them. The volume of system change activity can provide an indicator of the quality of systems development.

f) Confirm that adequate internal controls have been built into the system, that these are adequately documented, and that they are being operated correctly. Review the number and nature of internal control rejections to determine whether there are any underlying system design weaknesses.

g) Confirm that an adequate Service Level Agreement has been drawn up and implemented. Identify and report on any area where service delivery either falls below the level specified, or is inadequate in terms of what was specified.

h) Confirm that the system is being backed up in accordance with user requirements, and that it has been successfully restored from backup media.

i) Review the Business Case and determine whether:-

- anticipate benefits have/are been achieved;
- any unplanned benefits have been identified;
- costs are in line with those estimated;
- benefits and costs are falling with the anticipated time-frame.

j) Review trends in transaction throughput and growth in storage use to identify the anticipated growth of the system is in line with that forecast

9. CONTROL OVER SYSTEM AND PROGRAM CHANGES

9.1 Change Management Controls: To properly control information system changes, companies need formal change management control policies and procedure. These controls should include the following:

- Periodically review all systems for needed changes.
- Require all requests to be submitted in a standardized format.
- Log and review requests from authorised users for changes and additions to systems.
- Assess the impact of requested changes on system reliability objectives, policies and standards.
- Categorize and rank all changes using established priorities.
- Implement specific procedures to handle urgent matter, such as logging all emergency changes that required deviations from standard procedures and having management review and approve them after the fact. Make sure there is as audit trail for all urgent matters.
- Communication all changes to management and keep change requestors informed of the status of their requested changes.
- Require IT management to review, monitor, and approve all changes to hardware, software, and personnel responsibilities.
- Assign specific responsibilities to those involved in the change and monitor their work. Make sure that the specific assignments result in an adequate segregation of duties.
- Control system access rights to avoid unauthorised systems and date access.
- Make sure all changes go through the appropriate steps (development, testing, and implementation).
- Test all changes to hardware, infrastructure, and software extensively in a separate, non production environment before placing it into live production mode.
- Make sure there is a plan for backing out of any changes to mission-critical systems in the event that it does not work or does not operate properly.
- Implement a quality assurance function to ensure that all standards and procedures are followed and to assess if change activities achieve their stated objectives. These findings should be communicated to user departments, information systems management, and top management.
- Update all documentation and procedures when changes are implemented.

9.2 Authorization controls : Authorization controls ensure all information and data entered or used in processing is:
• authorized by management, and
• representative of events that actually occurred.

1. If transactions are manually authorized, what controls ensure that no unauthorized modifications take place after authorization, but prior to establishing input controls? Determine if the proper level of management is authorizing the transaction activity.
2. If transaction authorization is facilitated by logical access restrictions, select a sample of access rules applying to transaction input and update, and verify the appropriate people have these capabilities.
3. Identify any allowable overrides or bypasses of data validation and edit checks (authorization, monitoring, etc.). Determine who can do the overrides and verify that they are in a management position that should have this authority. Are all uses of the override features automatically logged so these actions can be subsequently analyzed for appropriateness?

9.3 Documentation controls. The documentation contains descriptions of the hardware, software, policies, standards, procedures, and approvals related to the system and formalize the system's security controls. Assessing documentation involves evaluating OJP's efforts to complete the following critical procedures:
• There is sufficient documentation that explains how software/hardware is to be used.
• There are documented formal security and operational procedures.

9.4 Testing and Quality Controls: Testing commences during the design phase, during which designs and specifications should be subject to quality reviews (non-computer testing), and continues during the system development and acceptance testing phases of the SDLC.
The overall objective of the testing process is therefore to ensure that the delivered system is of adequate quality. To meet this objective it will be necessary to confirm that the new system:-
• conforms with the organisation’s technical policies and standards;
• performs all the required functions;
• can be used by the staff for whom it is intended;
• meets it performance objectives;
• is reliable in operation.
Other important principles that should govern testing - and indeed any quality control - activities are that there is :-
• no testing without measurable objectives;
• no testing without recording;
• no recording without analysis;
• no analysis without action.

Quality control : ISO 9000 defines quality control as the “operational techniques and activities that are used to fulfill requirements for quality”.
As quality control is concerned with the quality of individual products produced during the project - in other words confirming that they fit for their intended purpose - it follows that it is the responsibility of the Project Manager to ensure that effective quality control is carried out.

Quality reviews: Quality review cover various non-computer testing activities. For example, it determine whether a product is:-
• complete and free from cosmetic and mechanical defects;
• is correct (e.g. a specification or plan), is sufficiently comprehensive and is targeted at the appropriate skill level for each category of user;
• complies with relevant standards.

IS Auditor's Role: Some of the activities that take place during system design and development are technically complex. If the auditor intends to carry out detailed reviews of, for example, logical design, it will probably be necessary either to employ expert assistance, or to undertake training in the particular technical skills required.
The following are the general questions that the auditor will need to consider for quality control:-
a) does system design follow a defined and acceptable standard?
b) are completed designs discussed and agreed with the users?
c) does the project's quality assurance procedures ensure that project documentation (e.g. design documents, specifications, test and installation plans) is reviewed against the organisation's technical standards and policies, and the User Requirements Specification;
d) do quality reviews follow a defined and acceptable standard?
e) are quality reviews are carried out under the direction of a technically competent person who is managerially independent from the design team;
f) are auditors/security staff invited to comment on the internal control aspects of system designs and development specifications?
g) are statistics of defects uncovered during quality reviews and other forms of quality control maintained and analysed for trends? Is the outcome of trend analysis fed back into the project to improve the quality of other deliverables?
h) are defects uncovered during quality reviews always corrected?
i) does the production of development specifications also include the production of relevant acceptance criteria?
j) has a Configuration Manager been appointed? Has the configuration management role been adequately defined?
k) are all configuration items (hardware, software, documentation) that have passed quality review been placed under configuration management and version control?
l) has sufficient IT (in the form of spreadsheets, databases, and specialist configuration management support tools) been provided to assist with the configuration management task?
m) are effective procedures in place for recording, analysing and reporting failures uncovered during testing?
n) are effective change management procedures are in place to control changes to configuration items?
o) has a System Installation Plan been developed and quality reviewed?
p) has a Training Plan been developed and quality reviewed? Has sufficient time and resources been allocated to its delivery? (to avoid "skills stagnation", the delivery of training will need to be carefully scheduled);
q) has an Acceptance Testing Plan been drawn up? Is it to an acceptable standard? Does it cover all aspects of the User Requirements Specification?
r) does the Acceptance Test Plan clearly allocate roles and responsibilities for undertaking and reviewing the results of acceptance testing?
s) has the Acceptance Test Plan been discussed with, and signed off by, the prospective System Owner?
t) is the system development environment is regularly backed up with copies of backed up configuration items held securely at a remote location?
u) has the development environment been recovered from backup media?
v) are contingency plans commensurate (in terms of time to implement) with the criticality of the project?
w) do regular Project Board meetings take place to review project progress against budget and deadline?
x) is the Business Case regularly updated to ensure that the project remains viable?

10. CONTROL OVER DATA INTEGRITY, PRIVACY AND SECURITY

10.1 Information Classification: Does not follow any predefined rules. It is a conscious decision to assign a certain sensitivity level to information that is being created, amended, updated, stored, or transmitted. The sensitivity level depends upon the nature of business in an organization and the market influence. The classification of information further determines the level of control and security requirements. Classification of information is essential to understand and differentiate between the value of an asset and its sensitivity and confidentiality. When data is stored, whether received, created or amended, it should always be classified into an appropriate sensitivity level to ensure adequate security. For many organizations, a very simple classification criteria is as follows:

Top Secret : The information is classified as Top Secret/ confidential that can *cause serious damage to the organisation if lost or made public.* Information is relating to pending mergers or acquisitions; investment strategies; plans or designs etc. is highly sensitive. Many restrictions are imposed on the usage of such information and is protected at the highest level of security possible.
Highly Confidential : This class of information, is *considered critical for the ongoing business operations and can cause serious impediment, if shared around the organization* e.g. sensitive customer information of bank's, solicitors and accountants etc., patient's medical records and similar highly sensitive data. It should not be copied or removed without the consent of appropriate authority and must be kept under operational vigilance. Security at this level should be very high.
Proprietary: Information relating to Procedures, operational work routines, project plans, designs and specifications are of propriety in nature. Such information is for proprietary *use to authorised personnel only*. Security at this level is high.
Internal Use only : This class of information cannot be circulated outside the organization where its loss would inconvenience the organisation or management but disclosure is unlikely to result in financial loss or serious damage to credibility. Internal memos, minutes of meetings, internal project reports are examples of such information. Security at this level is controlled but normal.
Public Documents: This Information is published in the public domain; annual reports, press statements etc.; which has been approved for public use. Security at this level is minimal.

10.2 Data Integrity. Once the information is classified, the organization has to decide about various data integrity controls to be implemented. The primary objective of data integrity control techniques is to prevent, detect, and correct errors in transactions as they flow through the various stages of a specific date processing program**.** Data integrity controls protect data from accidental or malicious alteration or destruction and provide assurance to the user that the information meets expectations about its quality and integrity.
There are six categories of integrity controls: source data controls input validation routines, on-line date entry controls, data processing and data storage controls, output controls, and data transmission controls. These integrity controls are summarized in following Table .

Control Category	Threats/Risks	Controls
Source data control	Invalid, incomplete, or inaccurate source data input	Forms design; sequentially prenumbered forms, turnaround documents; cancellation and storage of documents, review for appropriate authorisation; segregation of duties, visual scanning; check-digit verification; and key verification.
Input validation routines	Invalid or inaccurate data in computer-processed transaction files	As transaction files are processed, edit programs check key data fields using these edit checks, sequence, field, sign, validity, limit, range, reasonableness, redundant data, and capacity checks. Enter exceptions in an error log; investigate, correct, and resubmit chem. On a timely basis; re-edit them, and prepare a summary error report.
On-line data entry controls	Invalid or inaccurate transaction input entered through on-line terminals	Field, limit, range, reasonableness, sign, validity, and redundant data checks; user Ids and passwords; compatibility tests; automatic system date entry; prompting operators during data entry, preformatting, completeness test; closed-loop verification; a transaction log maintained by the system; clear error

		messages, and data retention sufficient to satisfy legal requirements.
Data processing and storage controls	Inaccurate or incomplete data in computer-processed master files	Policies and procedures (governing the activities of data processing and storage personnel; data security and confidentiality, audit trails, and confidentiality agreements); monitoring and expediting data entry by data control personnel; reconciliation of system updates with control accounts or reports; reconciliation of database totals with externally maintained totals; exception reporting, data currency checks, default values, data marching; data security (data library and librarian, backup copies of data files stored at a secure off-site location, protection against conditions that could harm stored data); use of file labels and write protection mechanisms, database protection mechanisms (datewise administrators, date dictionaries, and concurrent update controls); and data conversion controls.
Output controls	Inaccurate or incomplete computer output	Procedures to ensure that system outputs conform to the organisation's integrity objectives, policies, and standards, visual review of computer output, reconciliation of batch totals; proper distribution of output; confidential outputs being delivered are protected from unauthorised accesss, modification, and misrouting; sensitive or confidential output stored in a secure area; users review computer output for completeness and accuracy, shred confidential output no longer needed; error and exception reports.
Data transmission controls	Unauthorised access to data being transmitted or to the system itself; system failures; errors in data transmission	Monitor network to detect week points, backup components, design network to handle peak processing, multiple communication paths between network components, preventive maintenance, data encryption, routing verification (header labels, mutual authentication schemes, callback systems), party checking; and message acknowledgement procedures (echo checks, trailer labels, numbered batches).

11. LOGICAL ACCESS CONTROLS

Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. Assessing logical access controls involves evaluating the following critical procedures:

- Logical access controls restrict users to authorized transactions and functions.
- There are logical controls over network access.
- There are controls implemented to protect the integrity of the application and the confidence of the public when the public accesses the system.

11.1 Remote and distributed data processing applications can be controlled in many ways.

• Remote access to computer and data files through the network should be implemented.
• Having a terminal lock can assure physical security to some extent.
• Applications that can be remotely accessed via modems and other devices should be controlled appropriately.
• Terminal and computer operations at remote locations should be monitored carefully and frequently for violations.
• In order to prevent the unauthorized users gain entry into the system, there should be proper control mechanisms over system documentation and manuals.
• Data transmission over remote locations should be controlled. The location which sends data should attach needed control information that helps the receiving location to verify the genuineness and integrity.
• When replicated copies of files exist at multiple locations it must be ensured that all are identical copies contain the same information and checks are also done to ensure that duplicate data does not exist.

11.2 Role of an IS auditor in evaluating logical access controls: An IS auditor should keep the following points in mind while working with logical access control mechanisms.
• Reviewing the relevant documents pertaining go logical facilities and risk assessment and evaluation techniques and understanding the security risks facing the information processing system.
• The potential access paths into the system must be evaluated by the auditor and documented to assess their sufficiency.
• Deficiencies or redundancies must be identified and evaluated.
• By supplying appropriate audit techniques, he must be in a position to verify test controls over access paths to determine its effective functioning.
• He has to evaluate the access control mechanism, analyse the test results and other auditing evidences and verify whether the control objectives has been achieved.
• The auditor should compare security policies and practices of other organizations with the policies of their organization and assess its adequacy.

Security Policies: Every organization should have a security policy that defines acceptable behaviours and the reaction of the organisation when such behaviors are violated. Security policies are not unique and might differ from organization to organization. The electronic trading, viruses affecting organisation's security documents and the misuse of credit cards have increased and this has augmented the need for security management.

11.3 Logical Access Issues and Exposures: Controls that reduce the risk of misuse (intentional or unintentional), theft, alteration or destruction should be used to protect unauthorised and unnecessary access to computer files. Restricting and monitoring computer operator activities in a batch-processing environment provides this control. The avenues of access or more complex and direct in an online system and hence the level of control for this system must be more complex.
Access control mechanisms should be applied not only to computer operators but also to end users programmers, security administrators, management or any other authorized user.
Access control mechanisms should provide security to the following applications:
• Access control software
• Application software
• Data
• Data dictionary/directory
• Dial-up lines
• Libraries
• Logging files
• Operator systems exists
• Password library
• Procedure libraries
• Spool queues

• System software
• Tape files
• Telecommunication lines
• Temporary disk files.
• Utilities.

The above-mentioned utilities should be properly secured to assure security to data.

11.4 Logical Access Paths

Online Terminals -To access an online terminal a user has to provide a valid logon-ID and password. If additional authentication mechanisms are added along with the password, it will strengthen the security.

Operator Console – The operator console is one of the crucial places where any intruders can play a havoc. Hence, access to operator console must be restricted. This can be done by

• Keeping the operator console at a place, that is visible to all.
• By keeping the operator console in a protected room accessible to selected personnel.

Batch Job Processing – In a batch processing environment all jobs are processed in a batch. These batches are processed at regular intervals. The jobs are accumulated and sent as batches. Thus during an accumulation there is a possibility of an unknown job entering into a batch which may challenge security of the data. To avoid this access should be granted only to authorized people

Dial-up Ports : Using a dial up port user at one location can connect remotely to another computer present at an unknown location via a telecommunication media. A modem is a device, which can convert the digital data transmitted to analog data (the one that the telecommunication device uses). Thus the modem can act as an interface between remote terminal and the telephone line. Security is achieved by providing a means of identifying the remote user to determine authorization to access. A dial back line ensures security by confirming the presence and exactness of the data sent.

Telecommunication Network **–** In a Telecommunication network a number of computer terminals, Personal Computers etc. are linked to the host computer through network or telecommunication lines. Whether the telecommunication lines could be private (i.e., dedicated to one user) or public, security is provided in the same manner as it is applied to online terminals.

11.5 Issues and Revelations related to Logical Access: Logical access controls are used to increase the organisation's potential for the losses that result due to exposures that may lead to the total shutdown of the computer functions. Intentional or accidental exposure of logical access control encourage technical exposures and computer crimes.

(a) Technical Exposures*:* Technical exposures include unauthorized implementation or modification of data and software. Technical exposures include the following:

(i) Data Diddling: Data diddling involves the change of data before or as they are entered into the system. A limited technical knowledge is required to data diddle and the worst part with this is that it occurs before computer security can protect data.

(ii) Bombs: Bomb is a piece of bad code deliberately planted by an insider or supplier of a program. An event, which is logical, triggers a bomb or time based. The bombs explode when the conditions of explosion get fulfilled causing the damage immediately. However, these programs cannot infect other programs. Since these programs do not circulate by infecting other programs, chances of a widespread epidemic are relatively slim. Bombs are generally of the following two types:

• *Time Bomb:* The computer time bomb causes a perverse activity, such as, disruption of computer system, modifications, or destructions of stored information etc. on a particular date and time for which it has been developed. The computer clock initiates it.

• *Logic Bomb:* Logic bombs are activated by combination of events. For example, a code like; "If a file named DELETENOT is deleted then destroy the memory contents by writing ones." This code segment, on execution, may cause destruction of the contents of the memory on deleting a file named DELETENOT. These bombs can be set to go off at a

future time or event.

(iii). Trojan Horse: These are malicious programs that are hidden under any authorized program. Typically, a Trojan horse is an illicit coding contained in a legitimate program, and causes an illegitimate action. The concept of Trojan is similar to bombs but a computer clock or particular circumstances do not necessarily activate it. A Trojan-may

- Change or steal the password or
- May modify records in protected files or
- May allow illicit users to use the systems.

Trojan Horses hide in a host and generally do not damage the host program. Trojans cannot copy themselves to other software in the same or other systems. The Trojans may get activated only if the illicit program is called explicitly. It can be transferred to other system only if an unsuspecting user copies the Trojan program.

(iv). Worms: A worm does not require a host program like a Trojan to relocate itself. Thus, a Worm program copies itself to another machine on the network. Since worms are standalone programs, they can be detected easily in comparison to Trojans and computer viruses. Worms can help to sabotage systems yet they can also be used to perform some useful tasks. For example, worms can be used in the installation of a network. A worm can be inserted in a network and we can check for its presence at each node. A node, which does not indicate the presence of the worm for quite some time, can be assumed as not connected to the network.

(v). Rounding Down: This refers to rounding of small fractions of a denomination and transferring these small fractions into an authorized account. As the amount is small it gets rarely noticed.

(vi). Salami Techniques: This involves slicing of small amounts of money from a computerized transaction or account and is similar to the rounding down technique. A Salami technique is slightly different from a rounding technique in the sense only last few digits are rounded off here.

Trap Doors: Trap doors allow the They are exists out of an authorized program and allow insertion of specific logic, such as program interrupts that permit a review of data. They also permit insertion of unauthorized logic.

(b). Asynchronous Attacks: They occur in many environments where data can be moved asynchronously across telecommunication lines. Numerous transmissions must wait for the clearance of the line before data being transmitted. Data that are waiting to be transmitted are liable to unauthorized access called asynchronous attack. These attacks are hard to detect because they are usually very small pin like insertions. There are many forms of asynchronous attacks.

(i). Data Leakage: Data is critical resource for an organization to function effectively. Data leakage involves leaking information out of the computer by means of dumping files to paper on stealing computer reports and tape.

(ii). Wire-tapping: This involves spying on information being transmitted over telecommunication network.

(iii). Piggybacking: This is the act of following an authorized person through a secured door or electronically attaching to an authorised telecommunication link that intercepts and alters transmissions. This involves intercepting communication communications between the operating system and the user and modifying them or substituting new messages. A special terminal is tapped into the communication for this purpose.

(iv). Shut Down of the Computer/Denial of Service: This is initiated through terminals or microcomputers that are directly or indirectly connected to the computer. Individuals who know the high-level systems log on-ID initiate shutting down process. This security measure will function effectively only if there are appropriate access controls on the logging on through a telecommunication network. When overloading happens some systems have been proved to be vulnerable to shutting themselves. Hackers use this technique to shut down computer systems over the Internet.

(c). **Computer Crime Exposures :** Computers can be utilized both constructively and destructively. Computer systems are used to steal money, goods, software or corporate information. Crimes are also committed when false data or unauthorized transaction is made. Crimes that are committed using computers and the information they contain can damage the reputation, morale and very existence of an organization. Computer crimes generally result in Loss of customers, embarrassment to management and legal actions against the organizations.

(i). Financial Loss: Financial losses may be direct like loss of electronic funds or indirect like expenditure towards repair of damaged electronic components.

(ii). Legal Repercussions: An organization has to adhere to many human rights laws while developing security policies

and procedures. These laws protect both the perpetrator and organization from trial. The organizations will be exposed to lawsuits from investors and insurers if there are no proper security measures. The IS auditor should take legal counsel while reviewing the issues associated with computer security.
(iii). Loss of Credibility or Competitive Edge: In order to maintain competitive edge, many companies, especially service firms such as banks and investment firms, needs credibility and public trust. This credibility will be shattered resulting in loss of business and prestige if security violation occurs.
(iv). Blackmail/Industrial Espionage – By knowing the confidential information, the perpetrator can obtain money from the organization by threatening and exploiting the security violation.
(v). Disclosure of Confidential, Sensitive or Embarrassing Information: These events can spoil the reputation of the organization. Legal or regulatory actions against the company are also a result of disclosure.
(vi). Sabotage: People who may not be interested in financial gain but who want to spoil the credibility of the company or to will involve in such activities. They do it because of their dislike towards the organization or for their intemperance.
(vi). Spoofing **–** A spoofing attack involves forging one's source address. One machine is used to impersonate the other in spoofing technique. Spoofing occurs only after a particular machine has been identified as vulnerable. A penetrator makes the user think that he is interacting with the operating system. For example, a penetrator duplicates the logon procedure, captures the user's password, attempts for a system crash and makes the user login again. It is only the second time the user actually logs into the system.

Physical and Environmental Protection. Physical security and environmental security are the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. Assessing physical and environmental protection involves evaluating the following critical procedures:
• Adequate physical security controls have been implemented and are commensurate with the risks of physical damage or access.
• Data is protected from interception.
• Mobile and portable systems are protected.

12. PHYSICAL ACCESS CONTROLS
This section enumerates the losses that are incurred as result of perpetrations, accidental or intentional violation of access paths. The following issues are discussed:
• Physical Access Issues and Exposures
• Physical Access Controls
• Audit and evaluation techniques for physical access

12.1 Physical Access Issues and Exposures: The following points elucidate the results due to accidental or intentional violation of the access paths:
• Abuse of data processing resources.
• Blackmail
• Embezzlement
• Damage, vandalism or theft to equipments or documents.
• Modification of semester equipment and information.
• Public disclosure of sensitive information.
• Unauthenticated entry

Access control Mechanisms : An access control mechanism associates with identified, authorized users the resources they are allowable to access and action privileges. The mechanism processes the users request for resources in three steps.
• Identification
• Authentication
• Authorisation

The following is the sequence in which access control mechanisms operate:

• First and foremost, the users have to identify themselves, thereby indicating their intent to request the usage of system resources.

• Secondly, the users must authenticate themselves and the mechanism must authenticate itself.

• Third, the users request for specific resources, their need for those resources and their areas of usage of these resources.

The mechanism accesses previously stored information about users, the resources they can access, and the action privileges they have with respect to these resources; it then permits or denies the request.

Identification and Authentication : Users identify themselves to access control mechanism by providing information such a name or account number. To validate the user, his entry is matched with the entry in the authentication file. The authentication process then proceeds on the basis of information contained in the entry, the user having to indicate prior knowledge of the information.

Users may provide four classes of authentication information as described below:

Remembered information → Name, Account number, passwords

Objects Possessed by the user → Badge, plastic card, key

Personal characteristics → Finger print, voice print, signature

Dialog → Through/around computer

Authorisation : There are two approaches to implementing the authorization module in an access control mechanism:

(a) a "ticket oriented approach"

(b) a "list oriented approach"

Considering the authorization function in terms of a matrix where rows represent the users and columns represent the resources and the element represents the users privilege on the resources we can see the distinction between these two approaches.

In a *ticket-oriented approach* to authorization, the access control mechanism assigns users a ticket for each resource they are permitted to access. Ticket oriented approach operates via a row in the matrix. Each row along with the user resources holds the action privileges specific to that user.

In a *list-oriented approach,* the mechanism associates with each resource a list of users who can access the resource and the action privileges that each user has with respect to the resource.

The *primary advantage of the ticket oriented* or capability system is its run-time efficiency. When a user process is executing, its capability list can be stored in some fast memory device. When the process seeks access to a resource, the access control mechanism simply looks up the capability list to determine if the resource is present in the list and whether if the user is permitted to take the desired action.

The *advantage of list-oriented system* is that it allows efficient administration of capabilities. Each user process has a pointer to the access control list for a resource. Thus the capabilities for a resource can be controlled since they are stored in one place. It is enough to examine the access control list just to know who has access over the resource and similarly to revoke access to a resource, a user's entry in the access control list simply needs to be deleted.

12.2 **Physical Access Controls**: Physical access controls are designed to protect the organisation from unauthorized access or in other words, to prevent illegal entry. These controls should be designed in such a way that it allows access only to authorized persons. The authorization given by the management may be explicit, as in a door lock for which management has authorized us to have a key; or implicit, like a job description which confirms the need to access confidential reports and documents. Some of the more common access control techniques are discussed categorically as follows:

(a) Locks on Doors

Cipher locks (Combination Door Locks)- The cipher lock consists of a pushbutton panel that is mounted near the door

outside of a secured area. There are ten numbered buttons on the panel. To enter, a person presses a four digit number sequence, and the door will unlock for a predetermined period of time, usually ten to thirty seconds. Cipher locks are used in low security situations or when a large number of entrances and exits must be usable all the time. More sophisticated and expensive cipher locks can be computer coded with a person's handprint. A matching handprint unlocks the door.

Bolting Door Locks – A special metal key is used to gain entry when the lock is a bolting door lock. To avoid illegal entry the keys should be not be duplicated.

Electronic Door Locks – A magnetic or embedded chip-based plastics card key or token may be entered into a sensor reader to gain access in these systems. The sensor device upon reading the special code that is internally stored within the card activates the door locking mechanism. The following points list the advantages of electronic door locks over bolting and combinational locks.

• Through the special internal code, cards can be made to identity the correct individual.

• Individuals access needs can be restricted through the special internal code and sensor devices. Restrictions can be assigned to particular doors or to particular hours of the day.

• Degree of duplication is reduced.

• Card entry can be easily deactivated in the event an employee is terminated or a card is lost or stolen. If unauthorized entry is attempted silent or audible alarms can be automatically activated.

• An administrative process, which may deal with Issuing, accounting for and retrieving the card keys, are also parts of security. The card key becomes an important item to retrieve when an employee leaves the firm.

Biometric Door Locks **–** These locks are extremely secure where an individual's unique body features, such as voice, retina, fingerprint or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected, such as in the military.

(b). Physical identification medium

Personal Identification numbers (PIN) **–** A secret number will be assigned to the individual, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual. The visitor will be asked to log on by inserting a card in some device and then enter their PIN via a PIN keypad for authentication. His entry will be matched with the PIN number available in the security database.

Plastic Cards- These cards are used for identification purposes. Controls over card seek to ensure that customers safeguard their card so it does not fall into unauthorized hands.

Cryptographic Control- These types of controls help a lot in scheming Unauthorised access to data. Cryptography deals with transformation of data into codes that are meaningless to anyone who does not possess the system for recovering initial data. Only a crypto analyst can do the translation.

Identification Badges-special identification badges can be issued to personnel as well as visitors. For easy identification purposes their colour of the badge can be changed. Sophisticated photo IDs can also be utilized as electronic card keys. In Issuing, accounting for and retrieving the badges administrative prices are incurred that must carefully controlled.

(c) Logging on utilities

Manual Logging- All visitors should be prompted to sign a visitor's log indicating their name, company represented, their purpose of visit, and person to see. Logging may happen at both the front reception and entrance to the computer room. A valid and acceptable identification such as a driver's license, business card or vendor identification tag may also be asked for before gaining entry inside the company.

Electronic Logging – This feature is a combination of electronic and biometric security systems. The users logging in can be monitored and the unsuccessful attempts being highlighted.

(d). Other means of controlling Physical Access

Video Cameras **–** Cameras should be placed at specific locations and monitored by security guards. Refined video cameras can be activated by motion. The video supervision recording must be retained for possible future play back.

Security Guards – Extra security can be provided by appointing guards aided with video cameras and locked doors. Guards supplied by an external agency should be made to sign a bond to protect the organisation from loss.

Controlled Visitor Access – A responsible employee should escort all visitors. Visitors may be friends, maintenance personnel, computer vendors, consultants and external auditors.

Bonded Personnel – All service contract personnel, such as cleaning people and off-site storage services, should be asked to sign a bond. This may not be a measure to improve physical security but to a certain extent can limit the financial exposure of the organisation.

Dead man Doors – These systems encompasses are a pair of doors that are typically found in entries to facilities such as computer rooms and document stations. The first entry door must close and lock, for the second door to operate, with the only person permitted in the holding area. Only a single person is permitted at a given point of time and this will surely reduce the risk of piggybacking, when an unauthorized person follows an authorized person through a secured entry.

Non–exposure of Sensitive Facilities – There should be no explicit indication such as presence of windows of directional signs hinting the presence of facilities such as computer rooms. Only the general location of the information processing facility should be identifiable.

Computer Terminal Locks – These locks ensure that the device to the desk is not turned on or disengaged by unauthorized persons.

Controlled Single Entry Point – All incoming personnel can use controlled Single Entry Point. A controlled entry point is monitored by a receptionist. Multiple entry points increase the chances of unauthorized entry. Unnecessary or unused entry points should be eliminated or deadlocked.

Alarm System – Illegal entry can be avoided by linking alarm system to inactive entry point motion detectors and the reverse flows of enter or exit only doors, so as to avoid illegal entry. Security personnel should be able to hear the alarm when activated.

Perimeter Fencing – Fencing at boundary of the facility may also enhance the security mechanism.

Control of out of hours of employee-employees- Employees who are out of office for a longer duration during the office hours should be monitored carefully. Their movements must be noted and reported to the concerned officials frequently Secured Report/Document Distribution Cart- Secured carts, such as mail carts, must be covered and locked and should always be attended.

Accounting Audit Trial: All the activities taken at the boundary sub systems should be properly recorded in the accounting audit trial so the source and nature of all changes to the database can be identified. The following sorts of data must be kept:

- Action privileges requested.
- Action privileges allowed/deprived of.
- Authentication information supplied.
- Identity of the would-be user of the system.
- Number of log-on attempts.
- Resources requested.
- Resources provided/denied.
- Start and finish time.
- Terminal identifier.

This data allows management or auditor to recreate the time series of events that occurs when a user attempts so gain access to system resources. Periodical evaluation of the audit trial should happen to detect any control weaknesses in the system.

12.3 Audit and Evaluation Techniques for Physical Access: Information Systems Processing Facility (IPF) is used to gain

an overall understanding and perception of the installation being reviewed. This expedition provides the opportunity to being reviewing the physical access restriction.

The facility/computer room should include the following related facilities:
• Computer storage rooms (this includes equipment, paper and supply rooms
• Location of all communication equipment identified on the network diagram.
• Location of all operator consoles.
• Off-site backup storage facility.
• Printer rooms.
• Tape library.
• UPS/generator.
To do thorough testing, we have to look above the ceiling panels and below the raised floor in the computer operations centre. Keen observation is done on smoke and water detectors, and special emphasis is given to general cleanliness and walls that extend all the way to the real ceiling.
The following paths of physical entry should be evaluated for proper security.
• All entrance points.
• Glass windows and walls
• Movable walls and modular cubicles.
• Above suspended ceilings and beneath raised floors.
• Ventilation systems.
These security points must be properly governed to avoid illegal entry.

13. ENVIRONMENTAL CONTROLS
This section deals with the external factors in the Information System and Preventive measures to overcome these conflicts. Issues covered are:
• Environmental Issues and exposures
• Audit and Evaluation Techniques for Environmental Controls

13.1 Environmental Issues and Exposures: Environmental exposures are primarily due to elements of nature. However, with proper controls, exposure to these rudiments can be reduced.
Common occurrences are:
• Fire
• Natural disasters-earthquake, volcano, hurricane, tornado.
• Power spike
• Air conditioning failure
• Electrical shock
• Equipment failure
• Water damage/flooding-even with facilities located on upper floors of high buildings. Water damage is a risk, usually from broken water pipes
• Bomb threat/attack
Other environmental issues and revelations include the following:
• Is the power supply to the compiler equipment properly controlled so as to ensure that it remains within the manufacturer's specification?
• Are the air conditioning, humidity and ventilation control systems protected against the effects of electricity using static rug or anti-static spray?
• Is consumption of food, beverage and tobacco products prohibited, by policy, around computer equipment?
• Are backup media protected from damage due to variation in temperatures or are they guarded against strong magnetic fields and water damage?
• Is the computer equipment kept free of dust, smoke and other particulate matter?

13.2 Controls for Environmental Exposures

Water Detectors: In the computer room, even if the room is on high floor, water detectors should be placed under the raised floor and near drain holes. Water detectors should be present near any unattended equipment storage facilities. When activated, the detectors should produce an audible alarm that can be heard by security and control personnel. For easy identification and reach, the location of the water detectors should be marked on the raised computer room floor. A remedial action must be instantiated on hearing the alarm by notifying the specific individuals and allotting the responsibility for investigating the cause. Other staff should be made aware of the risk of a possible electrocution.

Hand-Held Fire Extinguishers: Fire extinguishers should be in calculated locations throughout the area. They should be tagged for inspection and inspected at least annually.

Manual Fire Alarms : Hand-pull fire alarms should be purposefully placed throughout the facility. The resulting audible alarm should be linked to a monitored guard station.

Smoke Detectors : Smoke detectors are positioned at places above and below the ceiling tiles. Upon activation, these detectors should produce an audible alarm and must be linked to a monitored station (for example a fire station). Fire repression systems should be supplemented and not replaced by smoke detectors.

Fire Suppression Systems : These alarms are activated when extensive heat is generated due to fire. Like smoke alarms they are designed to produce audible alarms when activated and should be regularly monitored. In addition to precautionary measures, the system should be segmented so that fire in one part of a large facility does not activate the entire system.
The fire suppression techniques vary depending upon the situation but its usually one of the following:
• Dry-Pipe sprinkling systems are typically referred to as sprinkler systems. These pipes remain dry and upon activation by the electronic fire alarm water is sent through the pipe.
Dry pipe systems have the advantage that any failure in the pipe will not result in water leaking into sensitive equipment.
• Water based systems also function similar to the sprinkler systems. These systems are effective but also are unpopular because they damage equipment and property. Changed systems are more reliable but the disadvantage is that in the case of leakage or breakage of pipes facilities are exposed to extensive water damage,
• An alternative method can be usage of Halon. Halon systems contain pressurized halon gases that remove oxygen from the air. Halon is preferred to others because of its inertness and it does not damage equipment like water does. There should be an audible alarm and brief delay before discharge to permit personnel time to evacuate the area or to override and disconnect the system. The drawback is, since halon adversely affects the ozone layer, its usage is restricted to some extent and alternative suppression methods are being explored.

Strategically Locating the Computer Room : The reduce the risk of flooding, the computer room should not be located in the basement of a multi-storeyed building. Studies reveal that the computer room located in the top floors are less prone to the risk of fire, smoke and water.

Regular Inspection by Fire Department : An annual inspection by the fire department should be carried out to ensure that all fire detection systems act in accordance with building codes. Also, the fire department should be notified of the location of the computer room, so it should be equipped with tools and appropriate electrical fires.

Fireproof Walls, Floors and Ceilings surrounding the Computer Room **:** Information processing facility should be surrounded by walls that should control or block fire from spreading. The surrounding walls should have at least a more than one-two-hour fire resistance rating.

Electrical Surge Protectors : The risk of damage due to power spikes can be reduced to a great extent using electrical surge protectors. The incoming current is measured by the voltage regulator and depending upon the intensity of electric current regulators can increase or decrease the charge of electricity and ensures that a consistent current passes through. Such protectors are typically built into the Uninterruptible Power Supply (UPS) system.

Uninterruptible Power Supply (UPS) / Generator : A UPS system consists of a battery or gasoline powered generator that interfaces between the electrical power entering the facility and the electrical power entering the computer. The system typically cleanses the power to ensure wattage into the computer is consistent. In case of a power failure, the UPS provides the back up by providing electrical power from the generator to the computer for a certain span of time. Depending on the sophistication of the UPS, electrical power supply could continue to flow for days or for just a few minutes to permit an orderly computer shutdown. A UPS system can be inbuilt or can be an external piece of equipment.

Power Leads from Two Substations : Electrical power lines that are exposed to many environmental dangers – such as waters fire, lightning, cutting due to careless digging etc. To avoid these types of events, redundant power links should feed into the facility. Interruption of one power supply does not adversely affect electrical supply.

Emergency Power-Off Switch **:** When there arises a necessity of immediate power shut down during situations like a computer room fire or an emergency evacuation, a two emergency power-off switch one at computer room and other near but outside the computer room would serve the purpose. They should be easily accessible and yet secured from unauthorized people.

Wiring Placed in Electrical Panels and Conduit : Electrical fires are always a risk. To reduce the risk of such a fire occurring and spreading, wiring should be placed in the fire resistant panels and conduit. This conduit generally lies under the fire-resistant raised computer room floor.

*Prohibitions Against Eating, Drinking and Smoking within the Information Processing Facility***:** These things should be prohibited from the information processing facility. This prohibition should be clear, e.g. a sign on the entry door.

Fire Resistant Office Materials **:** The materials used in the information processing facility such as Wastebaskets, curtains, desks, cabinets and other general office materials should be fire pool.

Documented and Tested Emergency Evacuation Plans : Relocation plans should emphasise human safety, but should not leave information processing facilities physically unsecured. Procedures should exist for a controlled shutdown of the computer in an emergency situation.

Audit and Evaluation techniques for Environmental Controls :

Water and Smoke Detectors **:** The presence of water and smoke detectors are verified on visiting the computer room. Also checks relating to adequacy of power supply to these detectors are done. A visual verification is done to test if the locations are clearly marked.
Hand-Held Fire Extinguishers : The presence of fire extinguishers in strategic locations throughout the facility is checked for.
Fire Suppressions Systems : Testing of suppressions system becomes more expensive, hence reviewing documentation that has been inspected and tested within the last year ensures it.
Regular Inspection by Fire Department : The person responsible for fire equipment maintenance is contacted and also the employees are queried, whether, fire department inspector has been invited to tour and inspected the facilities present in the organisation.

Fireproof Walls, Floors and Ceilings Surrounding the Computer Room : The assistance of building management is taken and checks relating to the location and the documentation that identifies the fire rating of the walls surrounding the information processing facility are done. These walls should have at least a two-hour fire resistance rating.

Electrical Surge Protectors : In this part the presence of electrical surge protectors for sensitive and expensive computer equipment is observed.

Power Leads from Two Substations : Checking the location and documentation concerning the use and replacement of redundant power lines into the information processing facility is performed.

Fully Documented and Tested Business Continuity Plan :

Wiring Placed in Electrical Panels and Conduit: Checking of whether the wiring in the information processing facility is placed in the fire-resistant panels and conduit is done.

Documented and Tested Emergency Evacuation Plans : A direct interview of the employees is conducted to test whether the emergency plans are posted throughout the facilities, whether in an organising manner, that does not leave the facilities physically unsecured.

Humidity/Temperature Control : Visit the information processing facility to visit on regular intervals and physically determine if temperature and humidity are adequate.

14. SECURITY CONCEPTS AND TECHNIQUES

(1) Cryptosystems : A cryptosystem refers to a suite of algorithms needed to implement a particular form of encryption and decryption. Typically, a cryptosystem consists of three algorithms: one for key generation, one for encryption, and one for decryption. The term *cipher* (sometimes *cypher*) is often used to refer to a pair of algorithms, one for encryption and one for decryption. Therefore, the term "cryptosystem" is most often used when the key generation algorithm is important. For this reason, the term "cryptosystem" is commonly used to refer to public key techniques; however both "cipher" and "cryptosystem" are used for symmetric key techniques.

(2) Data Encryption Standard (**DES**): The Data Encryption Standard (DES) is a cipher (a method for encrypting information) selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976, and which has subsequently enjoyed widespread use internationally. It is a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key. Authorized users of encrypted computer data must have the key that was used to encipher the data in order to decrypt it. The encryption algorithm specified in this standard is commonly known among those using the standard. DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small; DES keys have been broken in less than 24 hours.

(3) Public Key Infrastructure (PKI) : Public key infrastructure, if properly implemented and maintained, can provide a strong means of authentication. By combining a variety of hardware components, system software, policies, practices, and standards, PKI can provide for authentication, data integrity, defenses against customer repudiation, and confidentiality. The system is based on public key cryptography in which each user has a key pair—a unique electronic value called a ***public key*** and a mathematically related ***private ke***y. The ***public key*** is made available to those who need to verify the user's identity. The *private key* is stored on the user's computer or a separate device such as a smart card. When the key pair is created with strong encryption algorithms and input variables, the probability of deriving the private key from the public key is extremely remote. The private key must be stored in encrypted text and protected with a password or PIN to avoid compromise or disclosure. The private key is used to create an electronic identifier called a *digital signature* that uniquely identifies the holder of the private key and can only be authenticated with the corresponding public key. The *certificate authority* (CA), which may be the financial institution or its service provider, plays a key role by attesting with a

digital certificate that a particular public key and the corresponding private key belongs to a specific user or system. It is important when issuing a digital certificate that the registration process for initially verifying the identity of users is adequately controlled. The CA attests to the individual user's identity by signing the digital certificate with its own private key, known as the *root ke*y.

(4) Firewalls : A firewall is a collection of components (computers, routers, and software) that mediate access between different security domains. All traffic between the security domains must pass through the firewall, regardless of the direction of the flow. Since the firewall serves as an access control point for traffic between security domains, they are ideally situated to inspect and block traffic and coordinate activities with network intrusion detection systems (IDSs).Typically, firewalls block or allow traffic based on rules configured by the administrator. Rule sets can be static or dynamic. A static ruleset is an unchanging statement to be applied to packet header, such as blocking all incoming traffic with certain source addresses. A dynamic ruleset often is the result of coordinating a firewall and an IDS. Firewalls are subject to failure. When firewalls fail, they typically should fail closed, blocking all traffic, rather than failing open and allowing all traffic to pass.

Types of Firewalls :- There are four primary firewall types from which to choose: packet filtering, stateful inspection, proxy servers, and application-level firewalls. Any product may have characteristics of one or more firewall types. The selection of firewall type is dependent on many characteristics of the security zone, such as the amount of traffic, the sensitivity of the systems and data, and applications.

(i) Packet Filter Firewalls : Packet filter firewalls evaluate the headers of each incoming and outgoing packet to ensure it has a valid internal address, originates from a permitted external address, connects to an authorized protocol or service, and contains valid basic header instructions. If the packet does not match the pre-defined policy for allowed traffic, then the firewall drops the packet. Packet filters generally do not analyze the packet contents beyond the header information. Many routers contain access control lists (ACLs) that allow for packet-filtering capabilities. Weaknesses associated with packet filtering firewalls include the following:

- The system is unable to prevent attacks that exploit application-specific vulnerabilities and functions because the packet filter does not examine packet contents.
- Logging functionality is limited to the same information used to make access control decisions.
- Most do not support advanced user authentication schemes.
- Firewalls are generally vulnerable to attacks and exploitation that take advantage of vulnerabilities in network protocols.
- The firewalls are easy to misconfigure, which allows traffic to pass that should be blocked.

(ii) Stateful Inspection Firewalls: Stateful inspection firewalls are packet filters that monitor the state of the TCP connection. Each TCP session starts with an initial "handshake" communicated through TCP flags in the header information. When a connection is established the firewall adds the connection information to a table. The firewall can then compare future packets to the connection or state table. This essentially verifies that inbound traffic is in response to requests initiated from inside the firewall.

(iii) Proxy Server Firewalls: Proxy servers act as an intermediary between internal and external IP addresses and block direct access to the internal network. Essentially, they rewrite packet headers to substitute the IP of the proxy server for the IP of the internal machine and forward packets to and from the internal and external machines. Due to that limited capability, proxy servers are commonly employed behind other firewall devices. The primary firewall receives all traffic, determines which application is being targeted, and hands off the traffic to the appropriate proxy server. Common proxy servers are the domain name server (DNS), Web server (HTTP), and mail (SMTP) server. Proxy servers frequently cache requests and responses, providing potential performance benefits.

(iv) Application-Level Firewalls: Application-level firewalls perform application-level screening, typically including the filtering capabilities of packet filter firewalls with additional validation of the packet content based on the application. Application-level firewalls capture and compare packets to state information in the connection tables. Unlike a packet filter firewall, an application-level firewall continues to examine each packet after the initial connection is established for specific application or services such as telnet, FTP, HTTP, SMTP, etc. The application-level firewall can provide additional screening of the packet payload for commands, protocols, packet length, authorization, content, or invalid headers. Application level firewalls provide the strongest level of security, but are slower and require greater expertise to administer properly. The primary disadvantages of application-level firewalls are as follows:

• The time required to read and interpret each packet slows network traffic. Traffic of certain types may have to be split off before the application-level firewall and passed through different access controls.

• Any particular firewall may provide only limited support for new network applications and protocols. They also simply may allow traffic from those applications and protocols to go through the firewall.

15. DATA SECURITY AND PUBLIC NETWORKS:

To answer the question "how do you provide a low-cost, secure electronic network for your organization?"

One solution is a virtual private network (VPN): a collection of technologies that creates secure connections or "tunnels" over regular Internet lines-connections that can be easily used by anybody logging in from anywhere. Key advantages offered by a VPN include universal connectivity, security, and low cost.

16. DATA PRIVACY

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

• Health information.
• Criminal justice.
• Financial information.
• Genetic information.
• Location information.

16.1 Protecting data privacy in information systems:

There are several technologies to address privacy protection in enterprise IT systems. These fall into two categories:

(a) Policy Communication

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

(b) Policy Enforcement

• XACML - The eXtensible Access Control Markup Language together with its Privacy Profile is a standard for expressing privacy policies in a machine-readable language which a software system can use to enforce the policy in enterprise IT systems.

• EPAL - The Enterprise Privacy Authorization Language is very similar to XACML, but is not yet a standard.

• WS-Privacy - "Web Service Privacy" will be a specification for communicating privacy policy in web services. For example, it may specify how privacy policy information can be embedded in the SOAP envelope of a web service message.

17. UNAUTHORISED INTRUSION

Intrusion detection, is the attempt to monitor and possibly prevent attempts to intrude into or otherwise compromise the system and network resources of an organization.

17.1 Why use Intrusion Detection? : The underlying reasons why one might use intrusion detection systems are relatively straightforward: One wants to protect the data and systems integrity. The fact that one cannot always protect

that data integrity from outside intruders in today's Internet environment using mechanisms such as ordinary password and file security, leads to a range of issues. Adequate system security is of course the first step in ensuring data protection.

17.2 What types of Intrusion Detection systems are there? : These fall into two broad categories. They are:

• *Network based systems.* These types of systems are placed on the network, nearby the system or systems being monitored. They examine the network traffic and determine whether it falls within acceptable boundaries.

• *Host based systems.* These types of systems actually run on the system being monitored. These examine the system to determine whether the activity on the system is acceptable.

18. HACKING?

Hacking is an act of penetrating computer systems to gain knowledge about the system and how it works.

Who are Hackers? Technically, a hacker is someone who is enthusiastic about computer programming and all things relating to the technical workings of a computer. However, most people understand a hacker to be what is more accurately known as a 'cracker'.

Who are Crackers? :Crackers are people who try to gain unauthorized access to computers. This is normally done through the use of a 'backdoor' program installed on the machine. A lot of crackers also try to gain access to resources through the use of password cracking software, which tries billions of passwords to find the correct one for accessing a computer.

What damage can a Hacker do? This depends upon what backdoor program(s) are hiding on the PC. Different programs can do different amounts of damage. However, most allow a hacker to smuggle another program onto your PC. This means that if a hacker can't do something using the backdoor program, he can easily put something else onto your computer.

How do Hackers hack? : There are many ways in which a hacker can hack. Some are as follows –

(i) NetBIOS : NetBIOS hackers are the worst kind, since they don't require you to have any hidden backdoor program running on your computer. This kind of hack exploits a bug in Windows 9x. NetBIOS is meant to be used on local area networks, so machines on that network can share information. Unfortunately, the bug is that NetBIOS can also be used across the Internet - so a hacker can access your machine remotely.

(ii). ICMP 'Ping' (Internet Control Message Protocol): ICMP is one of the main protocols that make the Internet work. It stands for Internet Control Message Protocol. 'Ping' is one of the commands that can be sent to a computer using ICMP. Ordinarily, a computer would respond to this ping, telling the sender that the computer does exist. This is all pings are meant to do. Pings may seem harmless enough, but a large number of pings can make a Denial-of-Service attack, which overloads a computer. Also, hackers can use pings to see if a computer exists and does not have a firewall (firewalls can block pings). If a computer responds to a ping, then the hacker could launch a more serious form of attack against a computer.

(iii) FTP (File Transfer Protocol) :FTP is a standard Internet protocol, standing for File Transfer Protocol. It can be used for file downloads from some websites. If you have a web page of your own, you may use FTP to upload it from your home computer to the web server. However, FTP can also be used by some hackers. FTP normally requires some form of authentication for access to private files, or for writing to files. FTP backdoor programs, such as- • Doly Trojan • Fore

• Blade Runner simply turn your computer into an FTP server, without any authentication.

(iv) RPC statd : This is a problem specific to Linux and Unix. The problem is the infamous unchecked buffer overflow problem. This is where a fixed amount of memory is set aside for storage of data. If data is received that is larger than this buffer, the program should truncate the data or send back an error, or at least do something other than ignore the problem. Unfortunately, the data overflows the memory that has been allocated to it, and the data is written into parts of memory it shouldn't be in. This can cause crashes of various different kinds. However, a skilled hacker could write bits of program code into memory that may be executed to perform the hacker's evil deeds.

(v) HTTP – HTTP stands for Hypertext Transfer Protocol: HTTP hacks can only be harmful if you are using Microsoft web server software, such as Personal Web Server. There is a bug in this software called an 'unchecked buffer overflow'. If a

user makes a request for a file on the web server with a very long name, part of the request gets written into parts of memory that contain active program code. A malicious user could use this to run any program they want on the server.

19. CONTROLLING AGAINST VIRUSES AND OTHER DESTRUCTIVE PROGRAMS

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. One common technique is for the virus to simply replicate itself over and over within the main memory, thus destroying whatever data or programs are resident. One of the most insidious aspects of a virus is its ability to spread throughout the system and to other systems before perpetrating its destructive acts. Typically, a virus will have a built-in counter that will inhibit its destructive role until the virus has copied itself a specified number of times to other programs and systems. The virus thus grows geometrically, which makes tracing its origin extremely difficult.

Virus programs usually attach themselves to the following types of files:

1. An .EXE or .COM program file
2. The .OVL (overlay) program file
3. The boot sector of a disk
4. A device driver program

19.1 Anti-virus Software : Among the counter measures against virus attacks, anti-virus software are the most widely used techniques to detect viruses, and prevent their further propagation and harm. There are three types of anti-virus software.

(i) Scanners: The software looks for a sequence of bits called virus signatures that are characteristic of virus codes. They check memory, disk boot sectors, executables and systems fillies to find matching bit patterns. In this context it may be noted that on an average 1500 newer viruses emerge every month. Hence, it is necessary to frequently update the scanners with the data on virus code patterns for the scanners to be reasonably effective.

(ii) Active Monitor and Heuristic Scanner: This looks for critical interrupt calls and critical operating systems functions such as OS calls and BIOS calls, which resemble virus action. However this also makes them inefficient since they cannot differentiate between genuine systems calls and virus action. These could be annoying and generally do not serve the purpose.

(iii) Integrity Checkers: These can detect any unauthorised changes to files on the system. They require the software to "take stock" of all files resident on the system and compute a binary check data called the Cyclic Redundancy Check (CRC). When a program is called for execution, the software computes the CRC again and checks with the parameter stored on the disk. However, such checks assume that frequent changes to applications and systems utilities do not occur.

19.2 Recommended policy and procedure controls

• The Security Policy should address the virus threats, systems vulnerabilities and controls. A separate section on anti-virus is appropriate to address the various degrees of risks and suitable controls thereof.

• Anti-virus awareness and training on symptoms of attacks, methods of reducing damage, cleaning and quarantining should be given to all employees.

• Hardware installations and associated computing devices should be periodically verified for parameter settings.

• As part of SDLC Controls the develo0ment area should be free of viruses and sufficient safeguards must be in place to secure the area from viruses.

• Provision of derives to read media should be restricted to certain controlled terminals and should be write-protected.

• Network access to the Internet should be restricted preferably to stand-alone computers.

• Networks should be protected by means of firewalls that can prevent entry of known viruses.

• The servers and all terminals must have rated anti-virus software installed with sufficient number of user licences.

• Procedures should ensure that systematic updates are applied to all anti-virus installations at frequent intervals.

• External media such as disks, CDs, tapes need to be avoided. If necessary such media should be scanned on a stand-alone machine and certified b y the Department.

• Vendors and consultants should not be allowed to run their demonstrations and presentations on organizational systems.
• All new software acquisitions should follow a controlled procedure of centralized acquisition and testing for viruses.
• Patches to operating systems and other software and upgrades thereof should be acquired from authentic sources and scanned before installation.
• Reporting and incident handling procedures should be in place to suitably handle virus incidents and eradicate them at the earliest.
• An effective backup plan must be implemented and monitored to ensure that back-up media is not infected and preferably encrypted. Only new media must be used for backup purposes.

20. ROLE OF IS AUDITOR IN ACCESS CONTROLS

(a) Role of IS Auditor in Physical Access Controls: Auditing physical access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls. This involves the following:

(i) *Risk assessment*: The auditor must satisfy himself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures therefrom.

(ii) *Controls assessment*: The auditor based on the risk profile evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks.

(iii) *Planning for review of physical access controls.* It requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams.

(iv) *Testing of controls*: The auditor should review physical access controls to satisfy for their effectiveness. This involves:
• Tour of organizational facilities including outsourced and offsite facilities.
• Physical inventory of computing equipment and supporting infrastructure.
• Interviewing personnel can also provide information on the awareness and knowledge of procedures.
• Observation of safeguards and physical access procedures. This would also include inspection of:
(i) Core computing facilities
(ii) Computer storage rooms
(iii) Communication closets
(iv) Backup and off site facilities
(v) Printer rooms
(vi) Disposal yards and bins
(vii) Inventory of supplies and consumables.
• Review of physical access procedures including user registration and authorization, authorization for special access, logging, review, supervision etc.
• Examination of physical access logs and reports. This includes examination of incident reporting logs, problem resolution reports.

(b) Role of Auditor in Environmental Controls

The IS auditor should satisfy not only the effectiveness of various technical controls but that the overall controls assure safeguarding the business against environmental risks. Some of the critical audit considerations that an IS auditor should take into account while conducting his audit are given below:

Audit planning and assessment: As part of risk assessment
• The risk profile should include the different kinds of environmental risks that the organization is exposed to. These should comprise both natural and man-made threats.
The profile should be periodically reviewed to ensure updation with newer risks that may arise.
• The controls assessment must ascertain that controls safeguard the organisation against all acceptable risks including probable ones are in place.

• The security policy of the organization should be reviewed to assess policies and procedures that safeguard the organization against environmental risks.
• Building plans and wiring plans need to be reviewed to determine the appropriateness of location of IPF, review of surroundings, power and cable wiring etc.
• The IS auditor should interview relevant personnel to satisfy himself about employees' awareness of environmental threats and controls, role of the interviewee in environmental control procedures such as prohibited activities in IPF, incident handling, and evacuation procedures to determine if adequate incident reporting procedures exist.
• Administrative procedures such as preventive maintenance plans and their implementation, incident reporting and handling procedures, inspection and testing plan and procedures need to be reviewed.

Audit of technical controls: Audit of environmental controls requires the IS auditor to conduct physical inspections and observe practices. He must verify:
• The IPF and the construction with regard to the type of materials used for construction.
• The presence of water and smoke detectors, power supply arrangements to such devices, and testing logs.
• The location of fire extinguishers, fire fighting equipment and refilling date of fire extinguishers.
• Emergency procedures, evacuation plans and marking of fire exists. If necessary, the IS Auditor may also use a mock drill to test the preparedness with respect to disaster.
• Documents for compliance with legal and regulatory requirements with regards to fire safety equipment, external inspection certificate and shortcomings pointed out by other inspectors/auditors.
• Power sources and conduct tests to assure the quality of power, effectiveness of the power conditioning equipment, and generators. Also the power supply interruptions must be checked to test the effectiveness of the back-up power.
• Environmental control equipment such as air-conditioning, dehumidifiers, heaters, ionisers etc.
• Compliant logs and maintenance logs to assess if MTBF and MTTR are within acceptable levels.
• Activities in the IPF. Identify undesired activities such as smoking, consumption of eatables etc.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-08	[3(a)]	3	3.26 -3.28	10	*What do you understand by classification of information? Explain different classifications of information.*
Nov-08	[3(c)]	3	3.22 – 3.23	5	*Briefly explain the formal change management policies, and procedures to have control over system and program changes.*
Nov-08	[7(b)]	3	3.14 – 3.15	5	*Key elements in System Development and Acquisition Control*
Jun-09	[2(b)]	3	3.8	5	"While reviewing a client's control system, an information system auditor will identify three components of internal control." State and briefly explain these three components.
Jun-09	[3(a)]	3	3.7 & 3.9	10	*A company is engaged in the stores taking data activities. Whenever, input data error occurs, the entire stock data is to be reprocessed at a cost of Rs. 50,000. The management has decided to introduce a data validation step that would reduce errors from 12% to 0.5% at a cost of Rs. 2,000 per stock taking period. The time taken for validation causes an additional cost of Rs. 200. (i) Evaluate the percentage of cost benefit effectiveness of the decision taken by the management and (ii) suggest preventive control measures to avoid errors for improvement.*
Jun-09	[3(b)]	3	3.21 – 3.22	5	*What are the issues that should be considered by a system*

					auditor at post implementation review stage before preparing the audit report?
Jun-09	[7(c)]	3	3.53	5	*Firewalls*

4 - TESTING – GENERAL AND AUTOMATED CONTROLS

1. Testing is a process used to identify the correctness, completeness and quality of developed computer software. In other words testing is nothing but CRITICISM or COMPARISON, i.e. comparing the actual value with expected one.
One definition of testing is "the process of questioning a product in order to evaluate it", where the "questions" are things the tester tries to do with the product, and the product answers with its behaviour in reaction to the probing of the tester. Although most of the intellectual processes of testing are nearly identical to that of review or inspection, the word testing is connoted to mean the dynamic analysis of the product—putting the product through its paces. Testing helps in verifying and validating if the software is working as it is intended to be working.

2.1 Objectives of software testing includes:
• Testing is a process of executing a program with the intent of finding an error.
• A good test case is one that has a high probability of finding a yet undiscovered error.
• A successful test is one that uncovers a yet undiscovered error.
The data collected through testing can also provide an indication of the software's reliability and quality. However, testing cannot show the absence of defect, it can only show that software defects are present.

2.2 When testing should start: Testing early in the life cycle reduces the errors. Test deliverables are associated with every phase of development. The goal of software tester is to find bugs, find them as early as possible, and make sure that they are fixed.

2.3 Causes of Bugs:
(i) The number one cause of software bugs is the **specification**. There are several reasons why specifications are the largest bug producer. In many instances a specification simply isn't written. Other reasons may be that the specification isn't thorough enough, it is constantly changing, or it is not communicated well to the entire team. Planning of the software is vitally important. If it is not done correctly, bugs will be created.
(ii) The next largest source of bugs is the **design**; this is the stage where the programmers lay the plan for their Software. Compare it to an architect creating the blue print for the building. Bugs occur here for the same reason they occur in the specification i.e. when the design is rushed, changed, or not well communicated.
(iii) Coding errors: Typically these can be traced to the software complexity, poor documentation, schedule pressure or just plain dump mistakes. It is important to note that many bugs that appear on the surface to be programming errors can really be traced to specification.
The other category is the catch-all for what is left. Some bugs can be blamed for false positives, conditions that were thought to be bugs but really weren't. There may be duplicate bugs, multiple ones that resulted from the square root cause. Some bugs can be traced to testing errors.

2.4 When to Stop Testing: This can be difficult to determine. Many modern software applications are so complex, and run in such an interdependent environment, that complete testing can never be done. "When to stop testing" is one of the most difficult questions to a test engineer. Common factors in deciding when to stop are:
• Deadlines (release deadlines, testing deadlines.)
• Test cases completed with certain percentages passed
• Test budget depleted
• Coverage of code/functionality/requirements reaches a specified point
• The rate at which bugs are found is too small
• Beta or Alpha Testing period ends
• The risk in the project is under acceptable limit.

2.5 Test Strategy

A test strategy is the plan to cover the product in such a way so as to develop an adequate assessment of quality. A good test strategy is:

- Specific
- Practical
- Justified

(I) Test Plan - Why

- Identify Risks and Assumptions up front to reduce surprises later.
- Communicate objectives to all team members.
- Foundation for Test Spec, Test Cases, and ultimately the Bugs we find.

Failing to plan = planning to fail.

(II) Test Plan - What

- Derived from Test Approach, Requirements, Project Plan, Functional Spec., and Design Spec.
- Details out project-specific Test Approach.
- Lists general (high level) Test Case areas.
- Include testing Risk Assessment.
- Include preliminary Test Schedule
- Lists Resource requirements.

3. Test Plan: The test strategy identifies multiple test levels, which are going to be performed for the project. Activities at each level must be planned well in advance and it has to be formally documented. Based on the individual plans only, the individual test levels are carried out. Test Plans may be of different types e.g.

- Unit test Plan
- Integration test Plan
- System test Plan
- Acceptance Test Plan

(i) UNIT TEST PLAN {UTP}: The unit test plan is the overall plan to carry out the unit test activities. The lead tester prepares it and it is distributed to the individual testers, which contains the following sections.

- **What is to be tested?** Normally *the basic input/output of the units along with their basic functionality will be tested.* In this case mostly the input units will be tested for the format, alignment, accuracy and the totals. The UTP will clearly give the rules of what data types are present in the system, their format and their boundary conditions. This list may not be exhaustive; but it is better to have a complete list of these details.
- **Sequence of Testing:** This includes, whether to execute positive test cases first or negative test cases first, to execute test cases based on the priority, to execute test cases based on test groups etc. Positive test cases prove that the system performs what is supposed to do; negative test cases prove that the system does not perform what is not supposed to do. Testing the screens, files, database etc., are to be given in proper sequence.
- **Basic Functionality of Units:** The interface part i.e. any communication between the unit and other units is out of scope of this test level. Apart from the above sections, the following sections are addressed, very specific to unit testing.
- Unit Testing Tools
- Priority of Program units
- Naming convention for test cases
- Status reporting mechanism
- Regression test approach

(ii) INTEGRATION TEST PLAN: The integration test plan is the overall plan for carrying out the activities in the integration test level, which contains the following sections.

• **What is to be tested?** This section clearly specifies the kinds of interfaces which fall under the scope of testing viz., internal and external interfaces.

• **Sequence of Integration:** When there are multiple modules present in an application, the sequence in which they are to be integrated will be specified in this section. In this, the dependencies between the modules play a vital role. If a unit B has to be executed, it may need the data that is fed by unit A and unit X. In this case, the units A and X have to be integrated and then using that data, the unit B has to be tested. This has to be stated to the whole set of units in the program. Given this correctly, the testing activities will lead to the product, slowly building the product, unit by unit and then integrating them.

(iii) SYSTEM TEST PLAN {STP}: The system test plan is the overall plan carrying out the system test level activities. In the system test, apart from testing the functional aspects of the system, there are some special testing activities carried out, such as stress testing etc. The following are the sections normally present in system test plan.

• **What is to be tested?** This section defines the scope of system testing, very specific to the project. Normally, the system testing is based on the requirements. All requirements are to be verified in the scope of system testing. This covers the functionality of the product. Apart from this what special testing is performed are also stated here.

• **Functional Groups and the Sequence:** The requirements can be grouped in terms of the functionality. Based on this, there may also be priorities among the functional groups.

For example, in a banking application, anything related to customer accounts can be grouped into one area, anything related to inter-branch transactions may be grouped into one area etc. Same way for the product being tested, these areas are to be mentioned here and the suggested sequences of testing of these areas, based on the priorities are to be described.

(iv) ACCEPTANCE TEST PLAN {ATP}: The client at their place performs the acceptance testing. It will be very similar to the system test performed by the software development unit. Since the client is the one who decides the format and testing methods as part of acceptance testing, there is no specific clue on the way they will carry out the testing. However, but it will not differ much from the system testing. It can be assumed that all the rules, which are applicable to system test, can be implemented to acceptance testing also. Since this is just one level of testing done by the client for the overall product, it may include test cases including the unit and integration test level details.

4. TEST PLAN OUTLINE

A sample Test Plan Outline along with their description is as shown below:

• **BACKGROUND –** This item summarises the functions of the application system and the tests to be performed.

• **INTRODUCTION**

• **ASSUMPTIONS –** Indicates any anticipated assumptions which will be made while testing the application.

• **TEST ITEMS** - List each of the items (programs) to be tested.

• **FEATURES TO BE TESTED** - List each of the features (functions or requirements) which will be tested or demonstrated by the test.

• **FEATURES NOT TO BE TESTED** - Explicitly lists each feature, function, or requirement which won't be tested and why not.

• **APPROACH** - Describe the data flows and test philosophy, simulation or live execution, etc. This section also mentions all the approaches which will be followed at the various stages of the test execution.

• **ITEM PASS/FAIL CRITERIA** - Blanket statement - Itemised list of expected output and tolerances

• **SUSPENSION/RESUMPTION CRITERIA** - Must the test run from start to completion? Under what circumstances it may be resumed in the middle? Establish check-points in long tests.

• **TEST DELIVERABLES** - What, besides software, will be delivered? Test report Test software

• **TESTING TASKS** - Functional tasks (e.g., equipment set up) Administrative tasks

• **ENVIRONMENTAL NEEDS** - Security clearance Office space & equipment Hardware/software requirements

• **RESPONSIBILITIES** - Who does the tasks? What does the user do?

• **STAFFING & TRAINING**

• **SCHEDULE**

- **RESOURCES**
- **RISKS & CONTINGENCIES**
- **APPROVALS**

5. TYPES OF SOFTWARE TESTING

• **Static testing:** The verification activities fall into the category of Static Testing. During static testing, you have a checklist to check whether the work you are doing is going as per the set standards of the organisation. These standards can be for Coding, Integrating and Deployment. Reviews, Inspections and Walkthroughs are static testing methodologies.

• **Dynamic Testing:** Dynamic Testing involves working with the software, giving input values and checking if the output is as expected. These are the Validation activities. Unit Tests, Integration Tests, System Tests and Acceptance Tests are few of the Dynamic Testing methodologies. As we go further, let us understand the various Test Life Cycle's and get to know the Testing Terminologies.

TESTING METHODOLOGIES

Testing could be classified based on the methodology involved. Some of the common testing methodologies are described below.

6. BLACK BOX TESTING

Black box testing attempts to derive sets of inputs that will fully exercise all the functional requirements of a system. It is not an alternative to white box testing. This type of testing attempts to find errors in the following categories:

1. incorrect or missing functions,
2. interface errors,
3. errors in data structures or external database access,
4. performance errors, and
5. initialisation and termination errors.

Tests are designed to answer the following questions:

- How is the function's validity tested?
- What classes of input will make good test cases?
- Is the system particularly sensitive to certain input values?
- How are the boundaries of a data class isolated?
- What data rates and data volume can the system tolerate?
- What effect will specific combinations of data have on system operation?

Equivalence Partitioning: This method divides the input domain of a program into classes of data from which test cases can be derived. Equivalence partitioning strives to define a test case that uncovers classes of errors and thereby reduces the number of test cases needed. It is based on an evaluation of equivalence classes for an input condition. An equivalence class represents a set of valid or invalid states for input conditions. Equivalence classes may be defined according to the following guidelines:

1. If an input condition specifies a range, one valid and two invalid equivalence classes are defined.
2. If an input condition requires a specific value, then one valid and two invalid equivalence classes are defined.
3. If an input condition specifies a member of a set, then one valid and one invalid equivalence class are defined.
4. If an input condition is Boolean, then one valid and one invalid equivalence class are defined.

Boundary Value Analysis (BVA): This method leads to a selection of test cases that exercise boundary values. It complements equivalence partitioning since it selects test cases at the edges of a class. Rather than focusing on input conditions solely, BVA derives test cases from the output domain also. BVA guidelines include:

1. For input ranges bounded by a and b, test cases should include values a and b and just above and just below a and b respectively.

2. If an input condition specifies a number of values, test cases should be developed to exercise the minimum and maximum numbers and values just above and below these limits.
3. Apply guidelines 1 and 2 to the output.
4. If internal data structures have prescribed boundaries, a test case should be designed to exercise the data structure at its boundary.

Cause-Effect Graphing Techniques: Cause-effect graphing is a technique that provides a concise representation of logical conditions and corresponding actions. There are four steps:
1. Causes (input conditions) and effects (actions) are listed for a module and an identifier is assigned to each.
2. A cause-effect graph is developed.
3. The graph is converted to a decision table.
4. Decision table rules are converted to test cases.

7. WHITE BOX TESTING

White box testing is a test case design method that uses the control structure of the procedural design to derive test cases. Test cases can be derived that
• guarantee that all independent paths within a module have been exercised at least once,
• exercise all logical decisions on their true and false sides,
• execute all loops at their boundaries and within their operational bounds, and
• exercise internal data structures to ensure their validity.

7.1 The Nature of Software Defects: Logic errors and incorrect assumptions are inversely proportional to the probability that a program path will be executed. General processing tends to be well understood while special case processing tends to be prone to errors. We often believe that a logical path is not likely to be executed when it may be executed on a regular basis. Our unconscious assumptions about control flow and data lead to design errors that can only be detected by path testing. Typographical errors are random.
7.2 Basis Path Testing: This method enables the designer to derive a logical complexity measure of a procedural design and use it as a guide for defining a basis set of execution paths. Test cases that exercise the basis set are guaranteed to execute every statement in the program at least once during testing.
7.3 Flow Graphs: Flow graphs can be used to represent control flow in a program and can help in the derivation of the basis set. Each flow graph node represents one or more procedural statements. The edges between nodes represent flow of control. An edge must terminate at a node, even if the node does not represent any useful procedural statements. A region in a flow graph is an area bounded by edges and nodes. Each node that contains a condition is called a predicate node.
7.4 Loop Testing: This white box technique focuses exclusively on the validity of loop constructs. Four different classes of loops can be defined:
• **Simple loops**: The following tests should be applied to simple loops where n is the maximum number of allowable passes through the loop:
1. skip the loop entirely,
2. only pass once through the loop,
3. m passes through the loop where m < n,
4. n - 1, n, n + 1 passes through the loop.
• **Nested loops**: The testing of nested loops cannot simply extend the technique of simple loops since this would result in geometrically increasing number of test cases. One approach for nested loops:
1. Start at the innermost loop. Set all other loops to minimum values.
2. Conduct simple loop tests for the innermost loop while holding the outer loops at their minimums. Add tests for out-of-range or excluded values.
3. Work outward, conducting tests for the next loop while keeping all other outer loops at minimums and other nested loops to typical values.

4. Continue until all loops have been tested.

• **Concatenated loops:** Concatenated loops can be tested as simple loops if each loop is independent of the others. If they are not independent (e.g. the loop counter for one is the loop counter for the other), then the nested approach can be used.

• **Unstructured loops:** This type of loop should be redesigned not tested!!!

Other white box testing techniques include:

1. Condition testing exercises the logical conditions in a program.
2. Data flow testing selects test paths according to the locations of definitions and uses of variables in the program.

8. UNIT TESTING

In computer programming, a unit test is a method of testing the correctness of a particular module of source code. The idea is to write test cases for every non-trivial function or method in the module so that each test case is separate from the others if possible. This type of testing is mostly done by the developers.

8.1 Benefits: The goal of unit testing is to isolate each part of the program and show that the individual parts are correct. It provides a written contract that the piece must satisfy. This isolated testing provides following main benefits:

• **Encourages change:** Unit testing allows the programmer to re-factor code at a later date, and make sure the module still works correctly (regression testing). This provides the benefit of encouraging programmers to make changes to the code since it is easy for the programmer to check if the piece is still working properly.

• **Simplifies Integration:** Unit testing helps eliminate uncertainty in the pieces themselves and can be used in a bottom-up testing style approach. By testing the parts of a program first and then testing the sum of its parts will make integration testing easier.

• **Documents the code**: Unit testing provides a sort of "living document" for the class being tested. Clients wishing to learn to use the class can look at the unit tests to determine how to use the class to fit their needs.

8.2 Limitations: It is important to realise that unit-testing will not catch every error in the program. By definition, it only tests the functionality of the units themselves. Therefore, it will not catch integration errors, performance problems and any other system-wide issues. In addition, it may not be trivial to anticipate all special cases of input the program unit under study may receive in reality. Unit testing is only effective if it is used in conjunction with other software testing activities.

9. REQUIREMENT TESTING

Usage

• To ensure that system performs correctly

• To ensure that correctness can be sustained for a considerable period of time.

• System can be tested for correctness through all phases of SDLC but incase of reliability the programs should be in place to make system operational.

Objectives

• Successful implementation of user requirements,

• Correctness maintained over considerable period of time

• Processing of the application complies with the organisation's policies and procedures.

• Secondary users needs are fulfilled: Security officer, DBA, Internal auditors, Record retention, Comptroller

How to Use:

• These test conditions are generalised ones, which becomes test cases as the SDLC progresses until system is fully operational.

• Test conditions are more effective when created from user's requirements.

• It must be noted that if test conditions are created from documents then in case of any error in the documents, these errors are likely to get incorporated in Test conditions and consequently testing would not be able to find those errors.

• Test conditions, if created from other sources (other than documents), makes error trapping more effective.

• Functional Checklist created.

When to Use

• Every application should be Requirement tested
• Should start at Requirements phase and should progress till operations and maintenance phase.
• The method used to carry requirement testing and the extent of it is important.

10. REGRESSION TESTING

Usage

• All aspects of system remain functional after testing.
• Change in one segment does not change the functionality of other segment.

Objectives

• System documents remain current
• System test data and test conditions remain current
• Previously tested system functions properly without getting effected though changes are made in some other segment of application system.

How to Use

• Test cases, which were used previously for the already tested segment, are re-run to ensure that the results of the segment tested currently and the results of same segment tested earlier are same.
• Test automation is needed to carry out the test transactions (test condition execution) else the process is very time consuming and tedious.
• In this case of testing cost/benefit should be carefully evaluated else the efforts spend on testing would be more and payback would be minimum.

When to Use

• When there is high risk that the new changes may affect the unchanged areas of application system.
• In development process: Regression testing should be carried out after the predetermined changes are incorporated in the application system.
• In Maintenance phase : regression testing should be carried out if there is a high risk that loss may occur when the changes are made to the system

11. ERROR HANDLING TESTING

Usage

• It determines the ability of applications system to process the incorrect transactions properly
• Errors encompass all unexpected conditions.
• In some systems a large part of programming effort will be devoted to handling error condition.

Objectives

The objective of error handling testing is to determine that:
• Application system recognises all expected error conditions
• Accountability of processing errors has been assigned and procedures provide a high probability that errors will be properly corrected
• During correction process reasonable control is maintained over errors.

How to Use

• A group of knowledgeable people is required to anticipate what can go wrong in the application system.
• It is needed that all the application knowledgeable people assemble to integrate their knowledge of user area, auditing and error tracking.
• Then logical test error conditions should be created based on this assimilated information.

When to Use

• Throughout SDLC.
• Impact from errors should be identified and should be corrected to reduce the errors to acceptable level.
• Used to assist in error management process of system development and maintenance.

12. MANUAL SUPPORT TESTING

Usage

• It involves testing of all the functions performed by the people while preparing the data and using these data from automated system.

Objectives

• Verify that manual support documents and procedures are correct.
• Determine that manual support responsibility is correct
• Determine that manual support people are adequately trained.
• Determine that manual support and automated segment are properly interfaced.

How to Use

• Process evaluated in all segments of SDLC.
• Execution can be done in conjunction with normal system testing.
• Instead of preparing, execution and entering actual test transactions the clerical and supervisory personnel can use the results of processing from application system.
• To test people it requires testing the interface between the people and application system.

When to Use

• Verification that manual systems function properly should be conducted throughout the SDLC.
• Should not be done at later stages of SDLC.
• Best done at installation stage so that the clerical people do not get used to the actual system just before system goes to production.

13. INTER SYSTEM TESTING

Usage

• To ensure interconnection between application functions correctly.

Objective

• Proper parameters and data are correctly passed between the applications
• Documentation for involved system is correct and accurate.
• Proper timing and coordination of functions exists between the application systems.

How to Use

• Operations of multiple systems are tested.
• Multiple systems are run from one another to check that they are acceptable and processed properly.

When to Use

• When there is change in parameters in application system
• The parameters, which are erroneous then risk associated to such parameters, would decide the extent of testing and type of testing.
• Intersystem parameters would be checked / verified after the change or new application is placed in the production.

14. CONTROL TESTING

Usage

• Control is a management tool to ensure that processing is performed in accordance to what management desire or intents of management.

Objective

• Accurate and complete data
• Authorised transactions
• Maintenance of adequate audit trail of information.
• Efficient, effective and economical process.
• Process meeting the needs of the user.

How to Use

• To test controls risks must be identified.

• Testers should have negative approach i.e. should determine or anticipate what can go wrong in the application system.
• Develop risk matrix, which identifies the risks, controls; segment within application system in which control resides.

When to Use

• Should be tested with other system tests.

15. PARALLEL TESTING

Usage

• To ensure that the processing of new application (new version) is consistent with respect to the processing of previous application version.

Objective:

• Conducting redundant processing to ensure that the new version or application performs correctly.
• Demonstrating consistency and inconsistency between 2 versions of the application.

How to Use

• Same input data should be run through 2 versions of same application system.
• Parallel testing can be done with whole system or part of system (segment).

When to Use

• When there is uncertainty regarding correctness of processing of new application where the new and old version are similar.
• In financial applications like banking where there are many similar applications the processing can be verified for old and new version through parallel testing.

16. VOLUME TESTING

It is the testing of the behaviour when the maximum number of users is concurrently active and when the database contains the greatest data volume.

The creation of a volume test environment requires considerable effort. It is essential that the correct level of complexity exists in terms of the data within the database and the range of transactions and data used by the scripted users, if the tests are to reliably reflect the production environment. Once the test environment is built it must be fully utilised. Volume tests offer much more than simple service delivery measurement. The exercise should seek to answer the following questions:

1. What service level can be guaranteed? How can it be specified and monitored?
2. Are changes in user behaviour likely? What impact will such changes have on resource consumption and service delivery?
3. Which transactions/processes is resource hungry in relation to their tasks?
4. What are the resource bottlenecks? Can they be addressed?
5. How much spare capacity is there?

The purpose of volume testing is to find weaknesses in the system with respect to its handling of large amount of data during extended time periods

17. STRESS TESTING

The purpose of stress testing is to find defects in the system capacity of handling large numbers of transactions during peak periods. For example, a script might require users to login and proceed with their daily activities while, at the same time, requiring that a series of workstations emulating a large number of other systems are running recorded scripts that add, update, or delete from the database.

18. PERFORMANCE TESTING

System performance is generally assessed in terms of response time and throughput rates under differing processing and configuration conditions. To attack the performance problems, there are several questions should be asked first:

1. How much application logic should be remotely executed?

2. How much updating should be done to the database server over the network from the client workstation?
3. How much data should be sent in each transaction?

19. CONCURRENT OR CONTINUOUS AUDIT AND EMBEDDED AUDIT MODULES

Types of audit tools: Different types of continuous audit techniques may be used. Some modules for obtaining data, audit trails and evidences may be built into the programs. Audit software is available which could be used for selecting and testing data. Many audit tools are also available some of which are described below:

(I) Snapshots: Tracing a transaction is a computerised system can be performed with the help of snapshots or extended records. The snapshot software is built into the system at those points where material processing occurs which takes images of the flow of any transaction as it moves through the application. These images can be utilised to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction. The main areas to dwell upon while involving such a system are 1) to locate the snapshot points based on materiality of transactions 2) when the snapshot will be captured and 3) the reporting system design and implementation to present data in a meaningful way.

(II) Integrated Test Facility (ITF): The ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness. This test data would be included with the normal production data used as input to the application system. In such cases the auditor has to decide what would be the method to be used to enter test data and the methodology for removal of the effects of the ITF transactions.

(III) System Control Audit Review File (SCARF): The system control audit review file (SCARF) technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written onto a special audit file- the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities.

Auditors might use SCARF to collect the following types of information:

• **Application system errors** - SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.

• **Policy and procedural variances** - Organisations have to adhere to the policies, procedures and standards of the organisation and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.

• **System exception** - SCARF can be used to monitor different types of application system exceptions. For example, salespersons might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.

• **Statistical sample** -Some embedded audit routines might be statistical sampling routines, SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.

• **Snapshots and extended records** - Snapshots and extended records can be written into the SCARF file and printed when required.

• **Profiling data** - Auditors can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.

• **Performance measurement** - Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.

(IV) Continuous and Intermittent Simulation (CIS): This is a variation of the SCARF continuous audit technique. This technique can be used to trap exceptions whenever the application system uses a database management system. During application system processing, CIS executes in the following way:

• The database management system reads an application system transaction. It is passed to CIS. CIS then determines whether it wants to examine the transaction further. If yes, the next steps are performed or otherwise it waits to receive further data from the database management system.
• CIS replicates or simulates the application system processing.
• Every update to the database that arises from processing the selected transaction will be checked by CIS to determine whether discrepancies exist between the results it produces and those the application system produces.
• Exceptions identified by CIS are written to a exception log file.
• The advantage of CIS is that it does not require modifications to the application system and yet provides an online auditing capability.

Advantages and Disadvantages of Continuous Auditing: Continuous auditing enables auditors to shift their focus from the traditional "transaction" audit to the "system and operations" audit. Continuous auditing has a number of potential benefits including:
(1) reducing the cost of the basic audit assignment by enabling auditors to test a larger sample (up to 100 percent) of client's transactions and examine data faster and more efficiently than the manual testing required when auditing around the computer;
(2) reducing the amount of time and costs auditors traditionally spend on manual examination of transactions;
(3) increasing the quality of audits by allowing auditors to focus more on understanding a client's business and industry and its internal control structure; and
(4) specifying transaction selection criteria to choose transactions and perform both tests of controls and substantive tests throughout the year on an ongoing basis.

Some of the advantages of continuous audit techniques are as under:
• *Timely, comprehensive and detailed auditing* – Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analysed rather than examining the inputs and the outputs only.
• *Surprise test capability* – As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.
• *Information to system staff on meeting of objectives* - Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
• Training for new users – Using the ITFs new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.
The following are some of the disadvantages and limitations of the use of the continuous audit system:
• Auditors should be able to obtain resources required from the organisation to support development, implementation, operation, and maintenance of continuous audit techniques.
• Continuous audit techniques are more likely to be used if auditors are involved in the development work associated with a new application system.
• Auditors need the knowledge and experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.
• Continuous auditing techniques are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.
• Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.

20. HARDWARE TESTING
Hardware testing may be done to the entire system against the Functional Requirement Specification(s) (FRS) and/or the System Requirement Specification (SRS). Focus is to have almost a destructive attitude and test not only the design, but

also the behaviour and even the believed expectations. It is also intended to test up to and beyond the bounds defined in the software/hardware requirements specification(s).

Types of Hardware Testing

- Functional testing
- User Interface testing
- Usability testing
- Compatibility testing
- Model Based testing
- Error exit testing
- User help testing
- Security testing
- Capacity testing
- Performance testing
- Reliability testing
- Recovery testing
- Installation testing
- Maintenance testing
- Accessibility testing

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-08	[3(b)]	4		5	*Explain software testing and state its objectives.*
Jun-09	[2(c)]	4		5	While testing a software, how will you involve the people working in the system Areas?
Jun-09	[7(d)]	4		5	*White Box Testing.*

5 - RISK ASSESSMENT METHODOLOGIES AND APPLICATIONS

RISK, THREAT, EXPOSURE, AND VULNERABILITY

1. Risk: A **risk** is the likelihood that an organisation would face a vulnerability being exploited or a threat becoming harmful. Information systems can generate many direct and indirect risks. These risks lead to a gap between the need to protect systems and the degree of protection applied. The gap is caused by:

(a) Widespread use of technology.
(b) Interconnectivity of systems.
(c) Elimination of distance, time and space as constraints.
(d) Unevenness of technological changes.
(e) Devolution of management and control.
(f) Attractiveness of conducting unconventional electronic attacks against organisations.
(g) External factors such as legislative, legal and regulatory requirements or technological developments.

This means there are new risk areas that could have a significant impact on critical business operations, such as:
(a) External dangers from hackers, leading to denial of service and virus attacks, extortion and leakage of corporate information.
(b) Growing potential for misuse and abuse of information system affecting privacy and ethical values.
(c) Increasing requirements for availability and robustness.

A **threat** is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organisation. Threat is any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data and denial of services

Vulnerability is the weakness in the system safeguards that exposes the system to threats. It may be weakness in an information system, cryptographic system (security systems), or other components (e.g. system security procedures, hardware design, internal controls) that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system.

An exposure is the extent of loss the organisation has to face when a risk materialises. It is not just the immediate impact, but the real harm that occurs in the long run. For example, loss of business, failure to perform the system's mission, loss of reputation, violation of privacy, loss of resources.

Attack is a set of actions designed to compromise confidentiality, integrity, availability or any other desired feature of an information system. Simply, it is the act of trying to defeat IS safeguards. The type of attack and its degree of success will determine the consequence of the attack.

Residual Risk. Any risk still remaining after the counter measures are analysed and implemented is called residual risk. An organisation's management of risk should consider these two areas: acceptance of residual risk and selection of safeguards. Even when safeguards are applied, there is probably going to be some residual risk. The risk can be minimised, but it can seldom be eliminated. It must be kept at a minimal, acceptable level.

2. THREATS TO THE COMPUTERISED ENVIRONMENT

Any computerised environment is dependent on people. They are a critical links in making the entire enterprise computing happen. As such threats emanate from people themselves. The special skill sets such as IT operational team, programmers, data administrator, etc. are key links in ensuring that the IT infrastructure delivers to the user

requirements. Social engineering risks target key persons to get sensitive information to exploit the information resources of the enterprise. A few common threats to the computerised environment can be:

(a) **Power Loss:** Power failure can cause disruption of entire computing equipments since computing equipments depends on power supply.
(b) **Communication failure:** Failure of communication lines result in inability to transfer data which primarily travel over communication lines. Where the organisation depends on public communication lines e.g. for e-banking communication failure present a significant threat that will have a direct impact on operations.
(c) **Disgruntled Employees:** A disgruntled employee presents a threat since, with access to sensitive information of the organisation, he may cause intentional harm to the information processing facilities or sabotage operations.
(d) **Errors:** Errors which may result from technical reasons, negligence or otherwise can cause significant integrity issues. A wrong parameter setting at the firewall to "allow" attachments instead of "deny" may result in the entire organisation network being compromised with virus attacks.
(e) **Malicious Code:** Malicious code such as viruses and worms which freely access the unprotected networks may affect organisational and business networks that use these unprotected networks.
(f) **Abuse of access privileges by employees:** The security policy of the company authorises employees based on their job responsibilities to access and execute select functions in critical applications.
(g) **Natural disasters:** Natural disasters such as earthquakes, lighting, floods, tornado, tsunami, etc. can adversely affect the functioning of the IS operations due to damage to IS facilities.
(h) **Theft or destruction of computing resources:** Since the computing equipment forms the back-bone of information processing, any theft or destruction of the resource can result in compromising the competitive advantage of the organisation.
(i) **Downtime due to technology failure:** IS facilities may become unavailable due to technical glitches or equipment failure and hence the computing infrastructure may not be available for short or extended periods of time. However the period for which the facilities are not available may vary in criticality depending on the nature of business and the critical business process that the technology supports.
(j) **Fire, etc.:** Fire due to electric short circuit or due to riots, war or such other reasons can cause irreversible damage to the IS infrastructure.

3. THREATS DUE TO CYBER CRIMES

• *Embezzlement*: It is unlawful misappropriation of money or other things of value, by the person to whom it was entrusted (typically an employee), for his/her own use or purpose.
• *Fraud*: It occurs on account of intentional misrepresentation of information or identity to deceive others, the unlawful use of credit/debit card or ATM, or the use of electronic means to transmit deceptive information, to obtain money or other things of value. Fraud may be committed by someone inside or outside the company.
• *Theft of proprietary information*: It is the illegal obtaining of designs, plans, blueprints, codes, computer programs, formulas, recipes, trade secrets, graphics, copyrighted material, data, forms, files, lists, and personal or financial information, usually by electronic copying.
• *Denial of service*: There can be disruption or degradation of service that is dependent on external infrastructure. Problems may erupt through internet connection or e-mail service that results in an interruption of the normal flow of information. Denial of service is usually caused by events such as ping attacks, port scanning probes, and excessive amounts of incoming data.
• *Vandalism or sabotage*: It is the deliberate or malicious, damage, defacement, destruction or other alteration of electronic files, data, web pages, and programs.
• *Computer virus*: Viruses are hidden fragments of computer code which propagates by inserting itself into or modifying other programs.
• *Other*: Threat includes several other cases such as intrusions, breaches and compromises of the respondent's computer networks (such as hacking or sniffing) regardless of whether damage or loss were sustained as a result.

4. RISK ASSESSMENT

4.1 Risk assessment is a critical step in disaster and business continuity planning. Risk assessment is necessary for developing a well tested contingency plan. Risk assessment is the analysis of threats to resources (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status in the minimum time in case of a disaster. Disasters may lead to vulnerable data and crucial information suddenly becoming unavailable. The unavailability of data may be due to the non-existence or inadequate testing of the existing plan. Risk assessment is a useful technique to assess the risks involved in the event of unavailability of information, to prioritise applications, identify exposures and develop recovery scenarios.

Various areas that are to be explained to determine the risk are briefly discussed below:-

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

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

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

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

(d) *Determining recovery time-frame*: Critical recovery time period is the period of time in which business processing must be resumed before the organisation incurs severe losses. This critical time depends upon the nature of operations.

(e) *Assess Insurance coverage*: The information system insurance policy should be a multiperil policy, designed to provide various types of coverage. Depending on the individual organisation and the extent of coverage required, suitable modifications may be made to the comprehensive list provided below:

(i) **Hardware and facilities:** The equipment should be covered adequately. Provision should be made for the replacement of all equipment with a new one by the same vendor.

(iI) **Software reconstruction:** In addition to the cost of media, programming costs for recreating the software should also be covered.

(iii) **Extra expenses:** The cost incurred for continuing the operations till the original facility is restored should also be covered.

(iv) **Business interruption:** This applies mainly to centres performing outsourced jobs of clients. The loss of profit caused by the damaged computer media should be covered.

(v) **Valuable paper and records:** The actual cost of valuable papers and records stored in the insured premises should be covered.

(vi) **Errors and omissions:** This cover is against the legal liability arising out of errors and omissions committed by system analysts, programmers and other information system personnel.

(vii) **Fidelity coverage:** This coverage is for acts of employees, more so in the case of financial institutions which use their own computers for providing services to clients.

(viii) **Media transportation:** The potential loss or damage to media while being transported to off-site storage/premises should be covered.

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

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

5. RISK MANAGEMENT

One needs to classify the risks as systematic and unsystematic.

(1) **Systematic risks** are unavoidable risks - these are constant across majority of technologies and applications. For example the probability of power outage is not dependant on the industry but is dependant on external factors. Systematic risks would remain, no matter what technology is used. Thus effort to seek technological solution to reduce systematic risks would essentially be unfruitful activity and needs to be avoided. Thus a systematic risk can be mitigated not by technology but by management process.

(2) **Unsystematic risks** are those which are peculiar to the specific applications or technology. One of the major characteristics of these risks would be that they can be generally mitigated by using an advanced technology or system. For example one can use a computer system with automatic mirroring to reduce the exposure to loss arising out of data loss in the event of failure of host computer. Thus by making additional investment one can mitigate these unsystematic risks.

5.1 Risk Management Process: The broad process of risk management will be as follows:

1. Identify the technology related risks under the gamut of operational risks.
2. Assess the identified risks in terms of probability and exposure.
3. Classify the risks as systematic and unsystematic.
4. Identify various managerial actions that can reduce exposure to systematic risks and the cost of implementing the same.
5. Look out for technological solutions available to mitigate unsystematic risks
6. Identify the contribution of the technology in reducing the overall risk exposure. The analysis should not be restricted to the instant area of application of the technology but should be extended across the entire organisation. This is necessary since manytechnologies may mitigate a specific type of risk but can introduce other kinds of risks.
7. Evaluate the technology risk premium on the available solutions and compare the same with the possible value of loss from the exposure.
8. Match the analysis with the management policy on risk appetite and decide on induction of the same.

5.2 The Risk Management Cycle: It is a process involving the following steps: identifying assets, vulnerabilities and threats; assessing the risks; developing a risk management plan; implementing risk management actions, and re-evaluating the risks.

These steps are categorised into three primary functions –

(i) Risk Identification,
(ii) Risk Assessment and
(iii) Risk Mitigation.

Risk assessment is the process of analysing and measuring risk and it helps a manager identify and quantify risks to the system. **Risk mitigation** involves the implementation of measures designed to reduce or eliminate some or all of those identified risks.

6. RISK IDENTIFICATION

A risk is anything that could jeopardize the achievement of an objective. For each of the department's objectives, risks should be identified. Asking the following questions helps to identify risks:

- What could go wrong?
- How could we fail?
- What must go right for us to succeed?
- Where are we vulnerable?
- What assets do we need to protect?
- Do we have liquid assets or assets with alternative uses?
- How could someone steal from the department?
- How could someone disrupt our operations?

• How do we know whether we are achieving our objectives?
• On what information do we most rely?
• On what do we spend the most money?
• How do we bill and collect our revenue?
• What decisions require the most judgment?
• What activities are most complex?
• What activities are regulated?
• What is our greatest legal exposure?

It is important that risk identification be comprehensive, at the department level and at the activity or process level, for operations, financial reporting, and compliance objectives. Both external and internal risk factors need to be considered. Usually, several risks can be identified for each objective.

In addition, the risk evaluation of the information technology interface would itself be a part of the audit report on information technology system.

The two primary questions to consider when evaluating the risk inherent in a business function are:

• What is the probability that things can go wrong? (**Probability**) This view will have to be taken strictly on the technical point of view and should not be mixed up with past experience. While deciding on the class to be accorded, one has to focus on the available measures that can prevent such happening.

• What is the cost if what can go wrong does go wrong? (**Exposure**)

Risk is evaluated by answering the above questions for various risk factors and assessing the probability of failure and the impact of exposure for each risk factor. Risk is the probability times the exposure.

The purposes of a risk evaluation is to

(1) identify the probabilities of failures and threats,

(2) calculate the exposure, i.e., the damage or loss to assets, and

(3) make control recommendations keeping the cost-benefit analysis in mind.

6.1 Techniques for Risk Evaluation : Following are some of the techniques that are available to assess and evaluate risks.

• Judgement and intuition
• The Delphi approach
• Scoring
• Quantitative Techniques

(a) In many situations the auditors have to use their **judgement and intuition** for risk assessment. This mainly depends on the personal and professional experience of the auditors and their understanding of the system and its environment. Together with it is required a systematic education and ongoing professional updating.

(b) The **Delphi Technique** was first used by the Rand Corporation for obtaining a consensus opinion. Here a panel of experts is appointed. Each expert gives his opinion in a written and independent manner. They enlist the estimate of the cost, benefits and the reasons why a particular system should be chosen, the risks and the exposures of the system. These estimates are then compiled together. The estimates within a pre-decided acceptable range are taken. The process may be repeated four times for revising the estimates falling beyond the range. Then a curve is drawn taking all the estimates as points on the graph. The median is drawn and this is the consensus opinion.

(c) In the **Scoring approach** the risks in the system and their respective exposures are listed. Weights are then assigned to the risk and to the exposures depending on the severity, impact on occurrence, and costs involved. The product of the risk weight with the exposure weight of every characteristic gives us the weighted score. The sum of these weighted score gives us the risk and exposure score of the system. System risk and exposure is then ranked according to the scores obtained.

(d) Quantitative techniques involve the calculating an annual loss exposure value based on the probability of the event and the exposure in terms of estimated costs. This helps the organisation to select cost effective solutions. It is the

assessment of potential damage in the event of occurrence of unfavourable events, keeping in mind how often such an event may occur.

7. RISK RANKING

The planning process should identify and measure the likelihood of all potential risks and the impact on the organisation if threat occurred. To do this, each department should be analysed separately. Although the main computer system may be the single greatest risk, it is not the only important concern. Even in the most automated organisations, some departments may not be computerised or automated at all. In fully automated departments, important records remain outside the system, such as legal files, computer data, software stored on diskettes, or supporting documentation for data entry. Organisations have to devise their own ranking methods. For example, the impact can be rated as: 0 = No impact or interruption in operations, 1 = Noticeable impact, interruption in operations for up to 8 hours, 2 = Damage to equipment and/or facilities, interruption in operations for 8 - 48 hours, 3 = Major damage to the equipment and/or facilities, interruption in operations for more than 48 hours. All main office and/or computer centre functions must be relocated.

5.7.1 Considerations in analysing risk include:

1. Investigating the frequency of particular types of disasters (often versus seldom).
2. Determining the degree of predictability of the disaster.
3. Analysing speed of onset of the disaster (sudden versus gradual).
4. Determining the amount of forewarning associated with the disaster.
5. Estimating the duration of the disaster.
6. Considering the impact of a disaster based on two scenarios:
a. Vital records are destroyed.
b. Vital records are not destroyed.
7. Identifying the consequences of a disaster, such as:
a. Personnel availability.
b. Personal injuries.
c. Loss of operating capability.
d. Loss of assets.
e. Facility damage.
8. Determining the existing and required redundancy levels throughout the organisation to accommodate critical systems and functions, including:
a. Hardware.
b. Information.
c. Communication.
d. Personnel.
e. Services.
9. Estimating potential loss:
a. Increased operating costs.
b. Loss of business opportunities.
c. Loss of financial management capability.
d. Loss of assets.
e. Negative media coverage.
f. Loss of stockholder's confidence.
g. Loss of goodwill.
h. Loss of income.
i. Loss of competitive edge.
j. Legal actions.

10. Estimating potential losses for each business function based on the financial and service impact and the length of time the organisation can operate without this business function. The impact of a disaster related to a business function depends on the type of outage that occurs and the time that elapses before normal operations can be resumed.
11. Determining the cost of contingency planning.

7.2 How to perform Risk Assessment : The risk assessment should be performed by facility. To measure the potential risks, a weighted point rating system can be used. Each level of probability can be assigned points as follows:

Probability	**Points**
High	10
Medium	5
Low	1

To obtain a weighted risk rating, probability points should be multiplied by the highest impact rating for each facility. For example, if the probability of hurricanes is high (10 points) and the impact rating to a facility is "3" (indicating that a move to alternate facilities would be required), then the weighted risk factor is 30 (10 x 3). Based on this rating method, threats that pose the greatest risk (e.g., 15 points and above) can be identified.

8. RISK MITIGATION

Factor or casual analysis can help relate characteristics of an event to the probability and severity of the operational losses. This will enable the organisation to decide whether or not to invest in information system or people (hazards) so events (frequency) or the effect of events (severity) can be minimised.
Cause models help in the implementation of risk mitigation measures. Cause analysis identifies events and their impact on losses. In addition to establishing causal relationship, other risk mitigation measures are:

- Self assessment.
- Calculating reserves and capital requirements.
- Creating culture supportive of risk mitigation.
- Strengthening internal controls, including internal and external audit of systems, processes and controls, including IS audit and assurance).
- Setting up operational risks limits (so business will have to reduce one or more of frequency of loss, severity of loss or size of operations).
- Setting up independent operational risk management departments.
- Establishing a disaster recovery plan and backup systems.
- Insurance.
- Outsourcing operations with strict service level agreements so operational risk is transferred.

8.1 Common risk mitigation techniques: Mitigation and measurement techniques are applied according to the event's losses, and are measured and classified according to the loss type. Some of the common risk mitigation techniques are as under:
1. **Insurance**: An organisation may buy insurance to mitigate such risk. Under the scheme of the insurance, the loss is transferred from the insured entity to the insurance company in exchange of a premium. However while selecting such an insurance policy one has to look into the exclusion clause to assess the effective coverage of the policy.

2. **Outsourcing**: The organisation may transfer some of the functions to an outside agency and transfer some of the associated risks to the agency. One must make careful assessment of whether such outsourcing is transferring the risk or is merely transferring the management process.

3. **Service Level Agreements**: Some of risks can be mitigated by designing the service level agreement. This may be entered into with the external suppliers as well as with the customers and users. The service agreement with the customers and users may clearly exclude or limit responsibility of the organisation for any loss suffered by the customer and user consequent to the technological failure. It must be recognised that the organisation should not be so obsessed

with mitigating the risk that it seeks to reduce the systematic risk - the risk of being in business. The risk mitigation tools available should not eat so much into the economics of business that the organization may find itself in a position where it is not earning adequate against the efforts and investments made.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-08	[5(a)]	5		10	*Explain the following terms with reference to Information Systems:* *(i) Risk* *(ii) Threat* *(iii) Vulnerability* *(iv) Exposure* *(v) Attack*
Nov-08	[5(b)]	5		5	*"There always exist some Common threats to the computerized environment." Explain these threats.*
Nov-08	[5(c)]	5		5	*What do you understand by "Risk Assessment"? Discuss the various areas that are to be explored to determine the risk.*
Jun-09	[3(c)]	5		5	*"Always, there exist some threats due to Cyber Crimes." Explain these threats.*
Jun-09	[4(b)]	5		5	*State and explain four commonly used techniques to assess and evaluate risks.*

6 - BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

1. BUSINESS CONTINUITY PLANNING :- The business continuity plan is a guiding documents that allows the management team to continue operations. It is a plan for running the business under stressful and time compressed situations. The plan lays out steps to be initiated on occurrence of a disaster, combating it and returning to normal operations including the quantification of the resources needed to support the operational commitments.

Business continuity covers the following areas:

• *Business resumption planning*- The operation's piece of business continuity planning.

• *Disaster recovery planning*- The technological aspect of business continuity planning, the advance planning and preparation necessary to minimise losses and ensure continuity of critical business functions of the organisation in the event of disaster.

• *Crisis management*- The overall co-ordination of an organisation's response to a crisis in an effective timely manner, with the goal of avoiding or minimising damage to the organisation's profitability, reputation or ability to operate.

The business continuity life cycle is broken down into four broad and sequential sections:

• risk assessment,
• determination of recovery alternatives,
• recovery plan implementation, and
• recovery plan validation

1.1 Objectives and Goals of Business Continuity Planning

The primary objective of a business continuity planning is to enable an organisation to survive a disaster and to reestablish normal business operations. In order to survive, the organisation must assure that critical operations can resume normal processing within a reasonable time frame. The key objectives of the contingency plan should be to:

(i) Provide for the safety and well-being of people on the premises at the time of disaster;
(ii) Continue critical business operations;
(iii) Minimise the duration of a serious disruption to operations and resources (both information processing and other resources);
(iv) Minimise immediate damage and losses;
(v) Establish management succession and emergency powers;
(vi) Facilitate effective co-ordination of recovery tasks;
(vii) Reduce the complexity of the recovery effort;
(viii) Identify critical lines of business and supporting functions.

Therefore, the goals of the business continuity plan should be to:

(i.) Identify weaknesses and implement a disaster prevention program;
(ii.) minimise the duration of a serious disruption to business operations;
(iii.) facilitate effective co-ordination of recovery tasks; and
(iv.) reduce the complexity of the recovery effort

2. DEVELOPING A BUSINESS CONTINUITY PLAN

The methodology for developing a business continuity plan can be sub-divided into eight different phases. The extent of applicability of each of the phases has to be tailored to the respective organisation. The **methodology** emphasises on the following:

(i.) Providing management with a comprehensive understanding of the total efforts required to develop and maintain an

effective recovery plan;
(ii.) Obtaining commitment from appropriate management to support and participate in the effort;
(iii.) Defining recovery requirements from the perspective of business functions;
(iv.) Documenting the impact of an extended loss to operations and key business functions;
(v.) Focusing appropriately on disaster prevention and impact minimisation, as well as orderly recovery;
(vi.) Selecting business continuity teams that ensure the proper balance required for plan development;
(vii.) Developing a business continuity plan that is understandable, easy to use and maintain; and
(viii.) Defining how business continuity considerations must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.

Phases of Business continuity planning :

The eight phases are described in detail in the following **:**
(i.) Pre-Planning Activities (Business continuity plan Initiation)
(ii.) Vulnerability Assessment and General Definition of Requirements
(iii.) Business Impact Analysis
(iv.) Detailed Definition of Requirements
(v.) Plan Development
(vi.) Testing Program
(vii.) Maintenance Program
(viii.) Initial Plan Testing and Plan Implementation

2.1 Pre-Planning Activity: In phase 1, we obtain an understanding of the existing and projected systems environment of the organisation. This enables us to refine the scope of business continuity planning and the associated work program; develop schedules; and identify and address issues that could have an impact on the delivery and the success of the plan. Two other key deliverables of this phase are: the development of a policy to support the recovery programs; and an awareness program to educate management and senior individuals who will be required to participate in the business continuity program.

2.2 Vulnerability Assessment and definition of Requirement : Security and control within an organisation is a continuing concern. It is preferable, from an economic and business strategy perspective, to concentrate on activities that have the effect of reducing the possibility of disaster occurrence, rather than concentrating primarily on minimising the impact of an actual disaster. This phase addresses measures to reduce the probability of occurrence. This phase will include the following tasks:
(i.) A thorough Security Assessment of the system and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security; insurance; security planning and administration; application controls; and personal computers.
(ii.) The Security Assessment will enable the business continuity team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.
(iii.) Present findings and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.
(iv.) Define the scope of the planning effort.
(v.) Analyse, recommend and purchase recovery planning and maintenance software required to support the development and maintenance of the plans.
(vi.) Develop a Plan Framework.
(vii.) Assemble business continuity team and conduct awareness sessions.

2.3 Business Impact Analysis: Business Impact Analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. It enables the business continuity team to identify critical systems, processes and functions, assess the economic impact of incidents and disasters that result in a denial of access to the system, services and facilities, and assess the "pain threshold," that is, the length of time business units can survive without access to the system, services and facilities. The business impact analysis is intended to help understand the degree of potential loss (and various other unwanted effects) which could occur. This will cover not just direct financial loss, but other issues, such as reputation damage, regulatory effects, etc.

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

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

(ii.) Identify critical business processes.

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

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

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

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

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

There are a number of ways to obtain this information:

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

The BIA Report should be presented to the Steering Committee. This report identifies critical service functions and the timeframe in which they must be recovered after interruption. The BIA Report should then be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities.

2.4 Detailed Definition of requirements: During this phase, a profile of recovery requirements is developed. This profile is to be used as a basis for analysing alternative recovery strategies. The profile is developed by identifying resources required to support critical functions identified in Phase 3. This profile should include hardware (mainframe, data and voice communication and personal computers), software (vendor supplied, in-house developed, etc.), documentation (DP, user, procedures), outside support (public networks, DP services, etc.), facilities (office space, office equipments, etc.) and personnel for each business unit. Recovery Strategies will be based on short term, intermediate term and long term outages. Another key deliverable of this phase is the definition of the plan scope, objectives and assumptions.

2.5 Plan Development: The objective of this phase is to determine the available options and formulation of appropriate alternative operating strategies to provide timely recovery for all critical processes and their dependencies.

The recovery strategies may be two-tiered:

- Business - Logistics, accounting, human resources, etc.
- Technical - Information Technology (e.g. desktop, client-server, midrange, mainframe computers, data and voice networks).

2.6 Testing the Plan: The plan Testing/Exercising Program is developed during this phase. Testing/Exercising goals are established and alternative testing strategies are evaluated. Testing strategies tailored to the environment should be selected and an on-going testing program should be established. Unless the plan is tested on a regular basis, there is no assurance that in the event the plan is activated, the organisation will survive a disaster.

The objectives of performing BCP tests are to ensure that:

• The recovery procedures are complete and workable.
• The competence of personnel in their performance of recovery procedures can be evaluated.
• The resources such as business processes, IS systems, personnel, facilities and data are obtainable and operational to perform recovery processes.
• The manual recovery procedures and IT backup system/s are current and can either be operational or restored.
• The success or failure of the business continuity training program is monitored.

2.7 Maintenance Program: Maintenance of the plans is critical to the success of actual recovery. The plans must reflect changes to the environment. It is critical that existing change management processes are revised to take recovery plan maintenance into account. In areas where change management does not exist, change management procedures will be recommended and implemented. The tasks undertaken in this phase are:
• Determine the ownership and responsibility for maintaining the various BCP strategies within the organisation
• Identify the BCP maintenance triggers to ensure that any organisational, operational, and structural changes are communicated to the personnel who are accountable for ensuring that the plan remains up-to-date.
• Determine the maintenance regime to ensure the plan remains up-to-date.
• Determine the maintenance processes to update the plan.
• Implement version control procedures to ensure that the plan is maintained up-to-date.

2.8 Testing and Implementation: Once plans are developed, initial tests of the plans are conducted and any necessary modifications to the plans are made based on an analysis of the test results. Specific activities of this phase include the following:
• Defining the test purpose/approach;
• Identifying test teams;
• Structuring the test;
• Conducting the test;
• Analysing test results; and
• Modifying the plans as appropriate.

3. TYPES OF PLANS

There are various kinds of plans that need to be designed. They include the following:

(1) Emergency Plan: The emergency plan specifies the actions to be undertaken immediately when a disaster occurs. Management must identify those situations that require the plan to be invoked for example, major fire, major structural damage, and terrorist attack. The actions to be initiated can vary depending on the nature of the disaster that occurs.
When the situations that evoke the plan have been identified four aspects of the emergency plan must be articulated.

(1) the plan must show who is to be notified immediately when the disaster occurs - management, police, fire department, medicos, and so on.
(2) the plan must show actions to be undertaken, such as shutdown of equipment, removal of files, and termination of power.
(3) any evacuation procedures required must be specified.
(4) return procedures (e.g., conditions that must be met before the site is considered safe) must be designated. In all cases, the personnel responsible for the actions must be identified, and the protocols to be followed must be specified clearly.

(2) Back-up Plan: The backup plan specifies the type of backup to be kept, frequency with which backup is to be undertaken, procedures for making backup, location of backup resources, site where these resources can be assembled and operations restarted, personnel who are responsible for gathering backup resources and restarting operations, priorities to be assigned to recovering the various systems, and a time frame for recovery of each system. For some resources, the procedures specified in the backup plan might be straightforward.

(3) Recovery Plan: Whereas the backup plan is intended to restore operations quickly so the information system function can continue to service an organisation, recovery plans set out procedures to restore full information system capabilities. Recovery plans should identify a recovery committee that will be responsible for working out the specifics of the recovery to be undertaken. The plan should specify the responsibilities of the committee and provide guidelines on priorities to be followed. The plan might also indicate which applications are to be recovered first. Members of a recovery committee must understand their responsibilities. Again, the problem is that they will be required to undertake unfamiliar tasks.

4. TEST PLAN: The final component of a disaster recovery plan is a test plan. The purpose of the test plan is to identify deficiencies in the emergency, backup, or recovery plans or in the preparedness of an organisation and its personnel for facing a disaster. It must enable a range of disasters to be simulated and specify the criteria by which the emergency, backup, and recovery plans can be deemed satisfactory. Periodically, test plans must be invoked. Unfortunately, top managers are often unwilling to carry out a test because daily operations are disrupted. They also fear a real disaster could arise as a result of the test procedures.

5. THREATS AND RISK MANAGEMENT

To minimise threats to the confidentiality, integrity, and availability, of data and computer systems and for successful business continuity, it can be useful to evaluate potential threats to computer systems. Discussed hereunder are various threats, risks and exposures to computer systems and suggested control measures.

(1) Lack of integrity – Control measures to ensure integrity include implementation of security policies, procedures and standards, use of encryption techniques and digital signatures, inclusion of data validation, editing, and reconciliation techniques for inputs, processes and outputs, updated antivirus software, division of job and layered control to prevent impersonation, use of disk repair utility, implementation of user identification, authentication and access control techniques, backup of system and data, security awareness programs and training of employees, installation of audit trails , audit of adequacy of data integrity.

(2) Lack of confidentiality – Control measures to ensure confidentiality include use of encryption techniques and digital signatures, implementation of a system of accountability by logging and journaling system activity, development of a security policy procedure and standard, employee awareness and training, requiring employees to sign a non-disclosure undertaking, implementation of physical and logical access controls, use of passwords and other authentication techniques, establishment of a documentation and distribution schedule, secure storage of important media and data files, installation of audit trails , audit of confidentiality of data.

(3) Lack of system availability – Control measures to ensure availability include implementation of software configuration controls, a fault tolerant hardware and software for continuous usage and an asset management software to control inventory of hardware and software, insurance coverage, system backup procedure to be implemented, implementation of physical and logical access controls, use of passwords and other authentication techniques, incident logging and report procedure, backup power supply, updated antivirus software, security awareness programs and training of employees, installation of audit trails , audit of adequacy of availability safeguards.

(4) Unauthorised users attempt to gain access to the system and system resources – Control measures to stop unauthorised users to gain access to system and system resources include identification and authentication mechanism such as passwords, biometric recognition devices, tokens, logical and physical access controls, smart cards, disallowing the sharing of passwords, use of encryption and checksum, display of warning messages and regular audit programs.

(5) Disgruntled employees – Control measures to include installation of physical and logical access controls, logging and notification of unsuccessful logins, use of a disconnect feature on multiple unsuccessful logins, protection of modem and network devices, installation of one time use only passwords, security awareness programs and training of employees,

application of motivation theories, job enrichment and job rotation.

(6) Hackers and computer crimes – Control measures to include installation of firewall and intrusion detection systems, change of passwords frequently, installation of one time use passwords, discontinuance of use of installed and vendor installed passwords, use of encryption techniques while storage and transmission of data, use of digital signatures, security of modem lines with dial back modems, use of message authentication code mechanisms, installation of programs that control change procedures, and prevent unauthorised changes to programs, installation of logging features and audit trails for sensitive information.

(7) Terrorism and industrial espionage – Control measures to include usage of traffic padding and flooding techniques to confuse intruders, use of encryption during program and data storage, use of network configuration controls, implementation of security labels on sensitive files, usage of real-time user identification to detect masquerading, installation of intrusion detection programs.

5.1 Single Points of Failure Analysis: The objective is to identify any single point of failure within the organisation's infrastructure, in particular the information technology infrastructure. Single point's of failure have increased significantly due to the continued growth in the complexity in the organisation's IS environment. This growth has occurred due to changes in technology and customer's demands for new channels in the delivery service and/or products, for example E-Commerce. Organisations have failed to respond to increase in the exposure from single point of failure by not implementing risk mitigation strategies. One common area of risk from single point of failure is the telecommunication infrastructure. Because of its transparency, this potential risk is often overlooked. While the resiliency of network and the mean average failures of communication devices, e.g. routers, have improved, it is still a single point of failure in an organisation that may lead to disaster being declared. To ensure single point failures are identified within the organisations IS architecture at the earliest possible stage, it is essential, as part of any project, a technology risk assessment be performed.
The objectives of risk assessment are to:
• Identify Information Technology risks
• Determine the level of risk
• Identify the risk factors
• Develop risk mitigation strategies
The benefits of performing a technology risk assessment are:
• A business-driven process to identify, quantify and manage risks while detailing future suggestions for improvement in technical delivery.
• A framework that governs technical choice and delivery processes with cyclic checkpoints during the project lifecycle.
• Interpretation and communication of potential risk impact and where appropriate, risk reduction to a perceived acceptable level.
• Implementation of strict disciplines for active risk management during the project lifecycle.

6. SOFTWARE AND DATA BACK-UP TECHNIQUES
6.1 Types of Back-ups: When the back-ups are taken of the system and data together, they are called total system's back-up. System back-up may be a full back-up, an incremental back-up or a differential back-up.

(i) Full Backup: Every backup generation contains every file in the backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data. This is the simplest form of backup with a single restoring session for restoring all backed-up files.

(ii) Differential Backup: It contains all the files that have changed since the last full backup. This is in contrast to incremental backup generation, which holds all the files that were modified since the last full or incremental backup. It is faster and more economical in using the backup space, as only the files that have changed since the last full backup are

saved.

(iii) Incremental Backup: Only the files that have changed since the last full backup / differential backup / or incremental backup are saved. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space. Normally, it is difficult to restore as you have to start with recovering the last full backup, and then recovering from every incremental backup taken since.

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

7. ALTERNATE PROCESSING FACILITY ARRANGEMENTS

Security administrators should consider the following backup options:

(i). Cold site: If an organisation can tolerate some downtime, cold-site backup might be appropriate. A cold site has all the facilities needed to install a mainframe system-raised floors, air conditioning, power, communication lines, and so on. The mainframe is not present, it must be provided by the organisation wanting to use the cold site. An organisation can establish its own cold-site facility or enter into an agreement with another organisation to provide a cold-site facility.

(ii). Hot site: If fast recovery is critical, an organisation might need hot site backup. All hardware and operations facilities will be available at the hot site. In some cases, software, data and supplies might also be stored there. A hot site is expensive to maintain. They are usually shared with other organisations that have hot-site needs.

(iii). Warm site: A warm site provides an intermediate level of backup. It has all cold-site facilities plus hardware that might be difficult to obtain or install. For example, a swarm site might contain selected peripheral equipment plus a small mainframe with sufficient power to handle critical applications in the short run.

(iv). Reciprocal agreement: Two or more organisations might agree to provide backup facilities to each other in the event of one suffering a disaster. This backup option is relatively cheap, but each participant must maintain sufficient capacity to operate another's critical system. If a third-party site is to be used for backup and recovery purposes, security administrators must ensure that a contract is written to cover issues such as

(1) how soon the site will be made available subsequent to a disaster,
(2) the number of organisations that will be allowed to use the site concurrently in the event of a disaster,
(3) the priority to be given to concurrent users of the site in the event of a common disaster,
(4) the period during which the site can be used,
(5) the conditions under which the site can be used.
(6) the facilities and services the site provider agrees to make available, and
(7) what controls will be in place and working at the off-site facility.

These issues are often poorly specified in reciprocal agreements. Moreover, they can be difficult to enforce under a reciprocal agreement because of the informal nature of the agreement.

8. BACK-UP REDUNDANCY

(1) Multiple Backup Media: For data of high importance it is absolutely unacceptable to have a situation of data loss. Therefore, single point of failure such as failed backup disk that destroys the entire backup history should be eliminated.

(2) Off-Site Backup: Keeping all the eggs in one basket is not a smart strategy. That is why you should keep at least one copy of your redundant backups in an alternative location. In case the size of the backup is considerably big (>10GB), cost of high-speed link, security issues, and backup time will rule out the idea of backing up through high-speed links.

A practical solution would be to take a backup into a removable backup disk, which will be shuttled out of your site into a secure location.

(3) Where to Keep the Backups: If removable-media backups are kept next to the computer, a fire or other disaster will probably destroy both. A secure off-site location is best. At the very least, you should securely store them as far from your computer as possible. Consider keeping one backup disk in the office and the other one or two off-site.

(4) Media - Rotation – Tactics: Once in a while, rotate the active backup media with one of the offsite stored media. This

will update the offsite media with the latest data changes. To reduce data loss in case of a major disaster, it is recommended to daily switch the active backup media with one of the stored.

8.1 Types of Back-up Media: The most common types of backup media available on the market today include:
(i.) *Floppy Diskettes:* Floppy diskettes are available with most desktop computers and they are the cheapest back-up solution. However, these drives have low storage capacity and are slow.

(ii.) *Compact Disks:* Compact Disk read only memory (CD-ROM) drives are standard peripheral in most desktop computers. CD's are low cost storage media and have a higher storage capacity than floppy diskettes.
(iii.) *Tape Drives:* Tape drives are the most common backup media around due to their low cost. The average capacity of a tape drive is 4 to 10 GB. The drawbacks are that they are relatively slow when compared with other media, and can tend to be unreliable. Magnetic tape cartridges are used to store the data, which leaves it susceptible to loss of information over time or through breaking/stretching the tape.
(iv.) *Disk Drives:* Disk drives are expensive but very fast compare to tape drives. The disk drive rotates at a very fast pace and has one or more heads that read and write data. If an organisation is looking for a fast method of backup and recovery then disk drives is the way to go – the difference in speed between a tape drive and a disk drive is hours compared to minutes, respectively.
(v.) *Removable Disks:* Using a removable disk such as a ZIP/JAZ drive is becoming increasingly popular for the backup of single systems. They are quite fast, not that expensive and easy to install and carry around. The downside is that the capacity is usually (at the time of writing this article) not more than 2GB in size.
(vi.) *DAT (Digital Audio Tape) drives:* DAT drives are similar to a standard tape drive but they have a larger capacity. They are fast becoming popular and are slowly replacing the tape drive. The tapes come in DLT (Digital Linear Tape), SDLT (Super Digital Linear Tape), LTO (Linear Tape Open) and AIT (Advanced Intelligent Tape) format, offering up to 260GB of compressed data.
(vii.) *Optical Jukeboxes:* Optical Jukeboxes use magnetic optical disks rather than tapes to offer a high capacity backup solution. They are extremely expensive but offer excellent amounts of secure storage space, ranging from 5 to 20 terabytes. A jukebox is a tower that automatically loads internally stored disks when needed for backup and recovery – you just add a certain amount of CDs or DVDs when you first set it up, so maintenance is relatively low.
(viii.) *Autoloader* Tape Systems: Autoloader tape systems use a magazine of tapes to create extended backup volumes. They have a built-in capability of automatically loading or unloading tapes so you won't have to sit and wait for the "please insert tape 2" prompt! If you use an autoloader you will need a third party application that knows how to handle it. Autoloaders use DAT tapes that come in DLT, LTO and AIT format. By implementing a type library system with multiple drives you can improve the speed of a backup to hundreds of Gigabytes per hour.
(ix.) *USB Flash Drive:* USB flash Drive Plugs into the USB Port on laptop, PC, or Workstation. The USB flash Drive is available in various sizes. This Drive takes advantage of USB Plug and Play capability Saves and backs-up Documents and any File presentations which provides an excellent solution for mobile and storing data as a reliable Data retention media.
(x.) *Zip Drive:* Zip Drive is a small, portable disk drive used primarily for backing up and archiving personal computer files. Zip drives and disks come in various sizes. Zip drive comes with a software utility that provides the facility of copy the entire contents of hard drive to one or more Zip disks. The Zip drive can be purchased in either a Parallel or a Small Computer System Interface (SCSI) version. There are a substantial amount of tools and media available for backing up data. When making your selection, there are five fundamental factors that you should base your decision on.
- Speed – How fast can you backup and restore data using this media?
- Reliability – Can you risk purchasing media that's known to have reduced reliability to save on costs?
- Capacity – Is the media big enough for your backup load?
- Extensibility – If the amount of data grows, will the media support this demand?
- Cost – Does the solution you want fit into your I.T budget?

9. DISASTER RECOVERY PROCEDURAL PLAN :

Disaster: The term disaster can be defined as an incident which jeopardizes business operations and/or human life. It could be due to sabotage (human) or natural. Following is the procedural plans for disaster recovery.

Disaster Recovery Procedural Plan: Normally disaster recovery procedural plan is made when the system is normally working. After visualizing the disaster the action to be taken by different people of the organization are to be documented. This recovery and planning document may include the following areas:

(i) The conditions for activating the plans, which describe the process to be followed before each plan, are activated.

(ii) Emergency procedures, which describe the actions to be taken following an incident which jeopardises business operations and/or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities e.g. police, fire, services and local government.

(iii) Fallback procedures which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time-scale.

(iv) Resumption procedures, which describe the actions to be taken to return to normal business operations.

(v) A maintenance schedule, which specifies how and when the plan will be tested, and the process for maintaining the plan.

(vi) Awareness and education activities, which are designed to create an understanding of the business continuity, process and ensure that the business continues to be effective.

(vii) The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.

(viii) Contingency plan document distribution list.

(ix) Detailed description of the purpose and scope of the plan.

(x) Contingency plan testing and recovery procedure.

(xi) List of vendors doing business with the organisation, their contact numbers and address for emergency purposes.

(xii) Checklist for inventory taking and updating the contingency plan on a regular basis.

(xiii) List of phone numbers of employees in the event of an emergency.

(xiv) Emergency phone list for fire, police, hardware, software, suppliers, customers, back-up location, etc.

(xv) Medical procedure to be followed in case of injury.

(xvi) Back-up location contractual agreement, correspondences.

(xvii) Insurance papers and claim forms.

(xviii) Primary computer centre hardware, software, peripheral equipment and software configuration.

(xix) Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.

(xx) Alternate manual procedures to be followed such as preparation of invoices.

(xxi) Names of employees trained for emergency situation, first aid and life saving techniques.

(xxii) Details of airlines, hotels and transport arrangements.

10. INSURANCE

Policies are contracts that obligate the insurer to indemnify the policyholder or some third party from specific risks in return for the payment of a premium. Adequate insurance coverage is a key consideration when developing a business recovery plan and performing a risk analysis. Policies usually can be obtained to cover the following resources:

- *Equipment:* Covers repair or acquisition of hardware. It varies depending on whether the equipment is purchased or leased.
- *Facilities:* Covers items such as reconstruction of a computer room, raised floors, special furniture.
- *Storage media:* Covers the replacement of the storage media plus their contents – data files, programs, documentation.
- *Business interruption:* Covers loss in business income because an organisation is unable to trade.
- *Extra expenses:* Covers additional costs incurred because an organisation is not operating from its normal facilities.

• *Valuable papers:* Covers source documents, pre-printed reports, and records documentation, and other valuable papers.
• *Accounts receivable:* Covers cash-flow problems that arise because an organization cannot collect its accounts receivable promptly.
• *Media transportation:* Covers damage to media in transit.
• *Malpractice, errors:* Covers claims against an organisation by its customers, and omission e.g., claims and omission made by the clients of an outsourcing vendor or service bureau.

10.1 Kinds of Insurance:

The most common form of first-party insurance is property damage, while the most common from of third-party insurance is liability.

(a) First-party Insurances - Property Damages: Perhaps the oldest insurance in the world is that associated with damage to property. It is designed to protect the insured against the loss or destruction of property. It is offered by the majority of all insurance firms in the world and uses time-tested forms, the industry term for a standard insurance contract accepted industry-wide. This form often defines loss as "physical injury to or destruction of tangible property" or the "loss of use of tangible property which has not been physically injured or destroyed." Such policies are also known as all risks, defined risk, or casualty insurance.

(b) First-party Insurances - Business Interruption: If an insured company fails to perform its contractual duties, it may be liable to its customers for breach of contract. One potential cause for the inability to deliver might be the loss of information system, data or communications. Some in business and the insurance industry have attempted to mitigate this by including information technology in business recovery/disaster plans. As a result, there has emerged a robust industry in hot sites for companies to occupy in case of fire, flood, earthquake or other natural disaster. Disaster recovery has become a necessity in the physical world. While the role of disaster recovery is well understood in business, the insurance industry was slow to accept the indemnity role relative to insuring data in a business interruption liability insurance context. Insurers are generally aggressive in limiting their own liability and have, in a number of instances, argued that a complete cessation of business is necessary to claim damage.

(c) Third-party Insurance – General Liability: Third party insurance is designed to protect the insured from claims of wrongs committed upon others. In is in parts based on the legal theory of torts. Torts are civil wrongs which generally fit into three categories – intentional, negligent and strict liability. Intentional torts are generally excluded from liability insurance policies because they are foreseeable and avoidable by the insured. Strict liability torts, such as product liability issues, are generally covered under specialised liability insurance.

(d) Third-party Insurance - Directors and Officers: Errors and Omissions (E&O) insurance is protection from liability arising from a failure to meet the appropriate standard of care for a given profession. Two common forms of E & O insurance are directors and officers, and professional liability. Directors and officers insurance is designed to protect officers of companies, as individuals, from liability arising from ay wrongful acts committed in the course of their duties as officers. These policies usually are written to compensate the officer's company for any losses payable by the company for the acts of its officer's.

11. TESTING METHODOLOGY AND CHECKLIST

With good planning a great deal of disaster recovery testing can be accomplished with moderate expenditure. There are four types of tests:

(i.) *Hypothetical* - The hypothetical test is an exercise to verify the existence of all necessary procedures and actions specified within the recovery plan and to prove the theory of those procedures. It is a theoretical check and must be conducted regularly. The exercise is generally a brief one designed to look at the worst case for equipment, ensuring the entire plan process is reviewed.

(ii.) *Component* - A component is the smallest set of instructions within the recovery plan which enables specific

processes to be performed. For example the process "System Load/IPL" involves a series of commands to load the system. However, in the recovery situation this may be different from normal operational requirements. Certain functions need to be enabled or disabled to suit the new environment. If this is not fully tested incompatibility problems with other components are likely. Component testing is designed to verify the detail and accuracy of individual procedures within the recovery plan and can be used when no additional system can be made available for extended periods. Examples of component tests include back-up procedures, offsite tape storage recovery, technology and network infrastructure assembly, recovery and restoration procedures and security package start-up procedures.

(iii.) *Module* - A module is a combination of components. The ideal method of testing is that each component be individually tested before being included in a module. The aim of module testing is to verify the validity and functionality of the recovery procedures when multiple components are combined. If one is able to test all modules, even if unable to perform a full test, then one can be confident that the business will survive a major disaster. It is when a series of components are combined without individual tests that difficulties occur. Examples of module testing include alternate site activation, system recovery, network recovery, application recovery, database recovery and run production processing.

(iv.) *Full* - The full test verifies that each component within every module is workable and satisfies the strategy and recovery time objective detailed in the recovery plan. The test also verifies the interdependencies of various modules to ensure that progression from one module to another can be effected without problem or loss of data. The two main objectives associated with full test are:

- To confirm that the total time elapsed meets the recovery time objective.
- To prove the efficiency of the recovery plan to ensure a smooth flow from module to module.

12. AUDIT TOOLS AND TECHNIQUES

The best audit tool and technique is a periodic simulation of a disaster. Other audit techniques would include observations, interviews, checklists, inquiries, meetings, questionnaires and documentation reviews. These tools and methods may be categorised as under:

i. **Automated Tools:** Automated tools make it possible to review large computer systems for a variety of flaws in a short time period. They can be used to find threats and vulnerabilities such as weak access controls, weak passwords, lack of integrity of the system software, etc.

ii. **Internal Control Auditing:** This includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance of laws and regulations.

iii. **Disaster and Security Checklists:** A checklist can be used against which the system can be audited. The checklist should be based upon disaster recovery policies and practices, which form the baseline. Checklists can also be used to verify changes to the system from contingency point of view.

iv. **Penetration Testing:** Penetration testing can be used to locate vulnerabilities.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-08	[6(a)]	6		10	*What do you understand by the term Disaster? What procedural plan do you suggest for disaster recovery?*
Jun-09	[4(a)]	6		10	*As a system auditor, what control measures will you check to minimize threats, risks and exposures in a computerized system?*
Nov-08	[1(b)]	6		5	*Discuss the objectives and goals of Business Continuity planning.*

Nov-08	[6(b)]	6		5	*Describe the methodology of developing a Business Continuity Plan.*
Nov-08	[6(c)]	6		5	*Briefly explain the various types of system's back-up for the system and data together.*
Jun-09	[4(c)]	6		5	*What are the audit tools and techniques used by a system auditor to ensure that disaster recovery plan is in order? Briefly explain them.*

7 - AN OVERVIEW OF ENTERPRISE RESOURCE PLANNING: (ERP)

1.1 General Model of ERP

ERP is a global, tightly integrated closed loop business solution package and is multifaceted. It 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 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. ERP systems are implemented in a three Tier Client Server Architecture; the server stores the data, maintaining its integrity and consistency and processes the requests of the user from the client desktops. The load of data processing and application logic is divided between the server and the client. As companies implementing ERP solutions have multiple locations of operation and control, online data transfer has to be done across locations. To facilitate these transactions, the important enabling technologies for ERP systems are Workflow, Work group, Group Ware, Electronic Data Interchange (EDI), Internet, Intranet, Data warehousing, etc.

1.2 ERP Characteristics: An ERP system is not only the integration of various organization processes. Any system has to possess few key characteristics to qualify for a true ERP solution. These features are:

(1) Flexibility: An ERP system should be flexible to respond to the changing needs of an enterprise. The client server technology enables ERP to run across various database back ends through Open Database Connectivity (ODBC).

(2) Modular & Open: ERP system has to have open system architecture. This means that any module can be interfaced or detached whenever required without affecting the other modules. It should support multiple hardware platforms for the companies having heterogeneous collection of systems. It must support some third party add-ons also.

(3) Comprehensive: It should be able to support variety of organizational functions and must be suitable for a wide range of business organizations.

(4) Beyond The Company: It should not be confined to the organizational boundaries, rather support the on-line connectivity to the other business entities of the organization.

(5) Best Business Practices: It must have a collection of the best business processes applicable worldwide. An ERP package imposes its own logic on a company's strategy, culture and organisation.

1.3 Features of ERP: Some of the major features of ERP and what ERP can do for the business system are :

• ERP provides multi-platform, multi-facility, multi-mode manufacturing, multi-currency, multi-lingual facilities.

• It supports strategic and business planning activities, operational planning and execution activities, creation of Materials and Resources. All these functions are effectively integrated for flow and update of information immediately upon entry of any information.

• Has end to end Supply Chain Management to optimize the overall Demand and Supply Data.

• ERP facilitates company-wide Integrated Information System covering all functional areas like manufacturing, selling and distribution, payables, receivables, inventory, accounts, human resources, purchases etc.

• ERP performs core activities and increases customer service, thereby augmenting the corporate image.

• ERP bridges the information gap across organisations.

• ERP provides complete integration of systems not only across departments but also across companies under the same management.

• ERP is the solution for better project management.

• ERP allows automatic introduction of the latest technologies like Electronic Fund Transfer (EFT), Electronic Data Interchange (EDI), Internet, Intranet, Video conferencing, E-Commerce etc.

• ERP eliminates most business problems like material shortages, productivity enhancements, customer service, cash management, inventory problems, quality problems, prompt delivery etc.

• ERP provides intelligent business tools like decision support system, Executive information system, Data mining and

easy working systems to enable better decisions.

1.4 Why Companies Undertake ERP

• **Integrate financial information** - As the CEO tries to understand the company's overall performance, he may find many different versions of the truth. Finance has its own set of revenue numbers, sales has another version, and the different business units may each have their own version of how much they contributed to revenue. ERP creates a single version of the truth that cannot be questioned because everyone is using the same system.

• **Integrate customer order information** - ERP systems can become the place where the customer order lives from the time a customer service representative receives it until the loading dock ships the merchandise and finance sends an invoice. By having this information in one software system, rather than scattered among many different systems that can't communicate with one another, companies can keep track of orders more easily, and coordinate manufacturing, inventory and shipping among many different locations simultaneously.

• **Standardise and speed up manufacturing processes** - Manufacturing companies - especially those with an appetite for mergers and acquisitions—often find that multiple business units across the company make the same transaction/ recording/ report using different methods and computer systems. ERP systems come with standard methods for automating some of the steps of a manufacturing process. Standardising those processes and using a single, integrated computer system can save time, increase productivity and reduce headcount.

• **Reduce inventory** - ERP helps the manufacturing process flow more smoothly, and it improves visibility of the order fulfilment process inside the company. That can lead to reduced inventories of the materials used to make products (work-in-progress inventory), and it can help users better plan deliveries to customers, reducing the finished good inventory at the warehouses and shipping docks. To really improve the flow of your supply chain, you need supply chain software, but ERP helps too.

• **Standardise HR information** - Especially in companies with multiple business units, HR may not have a unified, simple method for tracking employees' time and communicating with them about benefits and services. ERP can fix that.

1.5 Benefits of ERP: The benefits accruing to any business enterprise by implementing an ERP package are unlimited. The following are some of the benefits they achieved by implementing the ERP packages:

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

2.1 Business Process Reengineering (BPR):

ERP is a result of a modern Enterprise's concept of how the Information System is to be configured to the challenging environments of new business opportunities. However, merely putting in place an information system is not enough.

Every company that intends to implement ERP has to re-engineer its processes in one form or the other. This process is known as Business Process Reengineering (BPR). BPR is the fundamental rethinking and radical redesign of processes to achieve dramatic improvement in critical, contemporary measure of performance such as cost, quality, service and speed. Radical Redesign means BPR is reinventing and not enhancing or improving. According to BPR philosophy, whatever was being done in past, it was all wrong, so one has to reassemble the new system to redesign it afresh. There is no point in simplifying or automating a business process, which does not add any value to the customer; such business processes should be eliminated altogether. BPR aims at major transformation of the business processes to achieve dramatic improvement. Here, the business objectives of the enterprise such as profits, customer – satisfaction through optimal cost, quality, deliveries etc. are achieved by transformation of the business processes which may, or may not, require the use of IT. The concept of BPR when merges with the concept of IT, the business engineering emerges, which is the rethinking of Business Processes to improve speed, quality and output of materials or services. In other words, business engineering is the method of development of business processes according to changing requirements.

2.2 Business Engineering : Business Engineering has come out of merging of two concepts namely Information Technology and Business Process Reengineering. Business Engineering is the rethinking of Business Processes to improve speed, quality and output of materials or services. The emphasis of business engineering is the concept of Process Oriented Business Solutions enhanced by the Client-Server computing in Information Technology. The main point in business engineering is the efficient redesigning of company's value added chains. Value added chains are a series of connected steps running through a business which when efficiently completed add value to enterprise and customers. Information technology helps to develop business models, which assist in redesigning of business processes. Business Engineering is the method of development of business processes according to changing requirements.

2.3 Business Management: ERP merges very well with common business management issues like Business Process Reengineering, total quality management, mass customisation, service orientation, and virtual corporation etc. The basic objective of implementing an ERP program is to put in place the applications and infrastructure architecture that effectively and completely support the Enterprise's business plan and business processes.

2.4 Business Modelling: The approach of ERP implementation is carried out using MIS planning. First of all, a model consisting of core business processes or activities of the business is to be developed. This is the diagrammatic representation of Business as a large system with interconnection of subsystems or processes that it comprises of.
The Data model consists of two elements.
1. A diagram describing various Business processes and their interactions.
2. An underlying Data Model.

3. 1 ERP IMPLEMENTATION

ERP implementation is a special event in an organisation. It brings together in one platform, different business functions, different personalities, procedures, ideologies and philosophies with an aim to pool knowledge base to effectively integrate and bring worthwhile and beneficial changes throughout the organization. A well managed and implemented ERP package can give a 200 percent return on investment where as a poorly implemented one can yield a return on investment as low as 25 percent.

3.2 ERP Implementation Methodology

Several steps are involved in the implementation of a typical ERP package. These are:
1. Identifying the needs for implementing an ERP package.
2. Evaluating the 'As Is' situation of the business i.e., to understand the strength and weakness prevailing under the existing circumstances.
3. Deciding the 'Would be' situation for the business i.e., the changes expected after the implementation of ERP.
4. Reengineering the Business Process to achieve the desired results in the existing processes.

5. Evaluating the various available ERP packages to assess suitability.
6. Finalising of the most suitable ERP package for implementation.
7. Installing the required hardware and networks for the selected ERP package.
8. Finalising the Implementation consultants who will assist in implementation.
9. Implementing the ERP package.

Let us examine these steps in detail:

1. Identifying the Needs: Some of the basic questions, which are to be answered, are

- Why should an ERP package be implemented?
- Will it improve profitability?
- Can the delivery times of products be reduced?
- How does it improve customer satisfaction in terms of quality, cost, delivery time and service?
- Will it help to reduce cost of products?
- How can it help to increase business turnover and at the same time reduce manpower?
- Will it be possible to reengineer the business processes?

Other requirements to satisfy the information management are:

- Need for quick flow of information between Business partners.
- Effective MIS for quick decision making
- Elimination of manual working.
- High level of integration between various business functions.

2. Evaluating the "AS IS" situation of the business:- To understand the present situation of the business, the various functions should first be listed. The processes used to achieve business transactions should be listed in detail. The details of business process can be obtained by mapping the processes to the functions:

- Total time taken by the business processes.
- Number of decision points existing in the present scenario.
- Number of Departments/Locations of business processes.
- The flow of information and its routing.
- The number of reporting points currently available.

3. Deciding the desired 'Would Be' situation:- The concept of 'Benchmarking' is used to see that processes achieved are the best in industry. Benchmarking is done on various factors like cost, quality, service etc. This concept enables to optimise the processes to gain overall benefits.

4. Reengineering the business process:- Reengineering of business processes is done to

- Reduce the business process cycle time.
- To reduce the number of decision points to a minimum.
- Streamlining the flow of information and eliminating the unwanted flow of information.

5. Evaluation of various ERP packages:- Evaluation of ERP packages are done based on the following criteria:-

(i) **Flexibility**: It should enable organizations to respond quickly by leveraging changes to their advantage, letting them concentrate on strategically expanding to address new products and markets.

(ii) **Comprehensive**: It should be applicable across all sizes, functions and industries. It should have in depth features in accounting and controlling, production and materials management, quality management and plant maintenance, sales and distribution, human resources management and plant maintenance, human resources management and project management. It should also have information and early warning systems for each function and enterprise – wide business intelligence system for informed decision making at all levels.

It should be open and modular. It should embrace an architecture that supports components or modules, which can be used individually, expandable in stages to meet the specific requirements of the business including industry specific functionality. It should be technology independent and mesh smoothly with in house / third party applications, solutions and services including the web.

(iii) **Integrated**: It should overcome the limitations of traditional hierarchical and function oriented structures. Functions like sales and materials planning, production planning, ware house management, financial accounting, and human resources management should be integrated into a work flow of business events and processes across departments and functional areas, enabling knowledge workers to receive the right information and documents at the right time at their desktops across organizational and geographical boundaries.

(iv) **Beyond the Company**: It should support and enable inter-enterprise business processes with customers, suppliers, banks, government and business partners and create complete logistical chains covering the entire route from supply to delivery, across multiple geographic, currencies and country specific business rules.

(v) **Best Business Practices**: The software should enable integration of all business operation in an overall system for planning, controlling and monitoring. It should offer a choice of multiple ready-made business processes including best business practices that reflect the experience and requirements of leading companies across industries. It should intrinsically have a rich wealth of business and organizational knowledge base.

(vi) **New Technologies**: It should incorporate cutting edge and future proof technologies such as object orientation into product development and ensure inter- operability with the Internet and other emerging technologies.

(vii) **Other factors** to be considered are :

- Global presence of the package
- Local presence
- Market targeted by the package
- Price of the package
- Obsolescence of package
- Ease of implementation of package
- Cost of implementation
- Post –implementation support availability.

6. Finalisation of the ERP package:- Finalisation of the ERP package can be done by making a comparison of critical factors through a matrix analysis.

7. Installation of Hardware and Networks:- This work is carried out in a phased manner depending on the schedule of implementation and need of the hardware components.

8. Finalising the Implementation Consultants:- The factors of selection for consultants are:

 Skill set
 Industry specific experience.
 Cost of hiring the consultant.

9. Implementation of ERP package:- The general steps involved in the implementation are

 Formation of team.
 Preparation of plan.
 Mapping of Business Processes to package.
 Gap Analysis i.e., deviation of existing processes from standard processes.
 Customisation.
 Development of user-specific reports and transactions.
 Uploading of Data from existing system.
 Test runs.
 User Training.
 Parallel run.
 Concurrence from user.
 Migration to the new system

 User documentation.
 Post-implementation support.
 System monitoring and fine tuning.

3.3 Implementation Guidelines For ERP : There are certain general guidelines, which are to be followed before starting the implementation of an ERP package.

1. Understanding the corporate needs and culture of the 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.

4. POST- IMPLEMENTATION

Most of the post-implementation problems of ERP can be traced to wrong expectations and fears. Sometimes it is also due to the ERP vendors and their pre-implementation sales hype. Popular expectations are:

- An improvement in processes,
- Increased productivity on all fronts,
- Total automation and disbanding of all manual processes,
- Improvement of all key performance indicators,
- Elimination of all manual record keeping,
- Real time information system available to concerned people on a need basis,
- Total integration of all operations.

Some of the fears on ERP implementations are:

- Job redundancy.
- Loss of importance as information is no longer an individual prerogative.
- Change in job profile:
- An organizational fear of loss of proper control and authorization.
- Increased stress caused by greater transparency.
- Individual fear of loss of authority.

Balancing the expectations and fears is a very necessary part of the implementation process. The ground realities are:

- Changing the organization involves three levers-strategies, business process and change, and consequential organization change.
- In most companies in India, many process related key performance indicators have not been measured till now, either because the company did not feel it necessary or lacked the tools to do so. Measuring such indicators brings in new culture.
- The genetic nature of the ERP packages is such that there would be processes peculiar to some sectors and organizations, which may have to be kept out of the process.
- Some of the processes are better done manually.

5. RISK AND GOVERNANCE ISSUES IN AN ERP

Organizations face several new business risks when they migrate to real-time, integrated ERP systems. Those risks include:

• *Single point of failure* - Since all the organization's data and transaction processing is within one application system and transaction processing is within one application system.

• *Structural changes* - Significant personnel and organizational structures changes associates with reengineering or redesigning business processes.

• *Job role changes* - Transition of traditional user's roles to empowered-based roles with much greater access to enterprise information in real time and the point of control shifting from the back-end financial processes to the front-end point of creation.

• *Online, real-time* - An online, real-time system environment requires a continuous business environment capable of utilizing the new capabilities of the ERP application and responding quickly to any problem requiring of re-entry of information (e.g., if field personnel are unable to transmit orders from handheld terminals, customer service staff may need the skills to enter orders into the ERP system correctly so the production and distribution operations will not be adversely impacted).

• *Change management* - It is challenging to embrace a tightly integrated environment when different business processes have existed among business units for so long. The level of user acceptance of the system has a significant influence on its success. Users must understand that their actions or inaction have a direct impact upon other users and, therefore, must learn to be more diligent and efficient in the performance of their day-today duties. Considerable training is therefore required for what is typically a large number of users.

• *Distributed computing experience* - Inexperience with implementing and managing distributed computing technology may pose significant challenges.

• *Broad system access* - Increased remote access by users and outsiders and high integration among application functions allow increased access to application and data.

• *Dependency on external assistance* - Organization accustomed to in-house legacy systems may find they have to rely on external help. Unless such external assistance is properly managed, it could introduce an element of security and resource management risk that may expose the organizations to greater risk.

• *Program interfaces and data conversions* - Extensive interfaces and data conversions from legacy systems and other commercial software are often necessary. The exposures of data integrity, security and capacity requirements for ERP are therefore often much higher.

• *Audit expertise* - Specialist expertise is required to effectively audit and control an ERP environment. The relative complexity of ERP systems has created specialisation such that each specialist may know only a relatively small fraction of the entire ERP's functionality in a particular core module, e.g. FI auditors, who are required to audit the entire organisation's business processes, have to maintain a good grasp of all the core modules to function effectively.

More recently, some of the additional risks and good governance issues introduced by the enabled ERP environments concern:

• *Single sign on* - It reduces the security administration effort associated with administrating web-based access to multiple systems, but simultaneously introduces additional risk in that an incorrect assignment of access may result in inappropriate access to multiple systems.

• *Data content quality* - As enterprise applications are opened to external suppliers and customers, the need for integrity in enterprise data becomes paramount.

• *Privacy and confidentiality* - Regularity and governance issues surrounding the increased capture and visibility of

personal information, i.e. spending habits.

7.5.1 Why do ERP projects fail so often?

At its simplest level, ERP is a set of best practices for performing the various duties in the departments of your company, including in finance, manufacturing and the warehouse. To get the most from the software, you have to get people inside your company to adopt the work methods outlined in the software. If the people in the different departments that will use ERP don't agree that the work methods embedded in the software are better than the ones they currently use, they will resist using the software or will want IT to change the software to match the ways they currently do things. This is where ERP projects break down. Political fights erupt over how or even whether the software will be installed. IT gets bogged down in long, expensive customisation efforts to modify the ERP software to fit with powerful business barons' wishes. Customisations make the software more unstable and harder to maintain when it finally does come to life. Because ERP covers so much of what a business does, a failure in the software can bring a company to a halt, literally. The mistake companies make is assuming that changing people's habits will be easier than customising the software. It's not. Getting people inside your company to use the software to improve the ways they do their jobs is by far the harder challenge. If people are resistant to change, then the ERP project is more likely to fail.

8. ERP SOFTWARE PACKAGE (SAP)

SAP AG has developed an ERP package called SAP. It will be worthwhile to look into this package in detail because SAP looked at the entire business as a single entity when developing this software. Therefore, it is a unique system that supports nearly all areas of business on a global scale. SAP has a number of Application Modules in the package. Some of these modules are given below:

1. Financials.
2. Controlling
3. Investment Management
4. Treasury
5. Integrated Enterprise Management
6. Sales and Distribution.
7. Production Planning and Control.
8. Materials Management
9. Human Resources Management.
10. Internet and Intranet.

Enterprise Controlling

Enterprise can be managed by using an Integrated Enterprise Management. This consists of getting accounting data prepared by subsidiaries for corporate reporting which will be automatically prepared simultaneously within the local books of each subsidiary. This data is transferred to a module called Enterprise Controlling (EC). It is easy to transfer the data to the EC module to automatically set up consolidated financial statements including elimination of inter-company transactions, currency translation etc.

Enterprise Controlling consists of 3 modules.

1. EC-CS.
2. EC-PCA
3. EC-EIS.

1. EC-CS:- This component is used for financial statutory and management consolidation which also allows fully automated consolidation of investments-even for many companies and complex investment structures.

2. EC-PCA:- Allows to work with internal transfer prices and at the same time to have the right values from company, profit centre, and enterprise perspectives in parallel. Any transaction that touches an object such as customer order, plant or cost centre allocated to a profit centre will be automatically posted to EC-PCA. It is also possible to take data

directly from EC-PCA to EC-CS consolidation to prepare complete financial statutory statements and management reports in parallel. This provides the management with a consistent view of external and internal financial management reports.

3. EC-EIS (Executive Information System):- Executive Information System allows to take financial data from EC-PCA ,EC-CS or any other application and combine with any external data such as market data, industry benchmarks and /or data from non-SAP applications to build a company specific comprehensive enterprise information system .

Enterprise Controlling:- It allows to control the whole enterprise from a corporate and a business unit perspective within one common infrastructure . It helps to speed up provision of business control information by fully automated corporate reporting from operative accounting via financial consolidation to management reporting. From EC-EIS top-level reports, end users can drill down to more detailed information within EC or any other R/3 application. EC can work with data from SAP and non-SAP sources.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-02	[4(a)]	12		10	What is an ERP system? Bring out the major challenges involved in its implementation
May-03	[4(b)]	12		10	Explain the process of evaluation of various ERP packages.
Nov-03	[5(b)]	12		8	Write down the general guidelines which are to be followed before starting the implementation of an ERP package.
Nov-03	[5(a)]	12		2	What is an ERP (Enterprise Resource Planning) system?
Nov-04	[5(a)]	12		10	Write a detailed note on the expectations, fears and the ground realities that a corporate management faces during the post-implementation phase of ERP.
Nov-04	[7(b)]	12		5	Write short note : Business Process Re-engineering
May-05	[6(a)]	12		5	What are the characteristics and features of an ERP?
May-05	[6(b)]	12		5	List any five ERP Vendors and briefly describe the ERP packages offered by them
Nov-05	[4(b)]	12		10	What are the benefits achieved by implementing the ERP packages?
Nov-05	[7(c)]	12		5	Business Engineering
May-06	[5(b)]	12		5	Explain the various criteria used for evaluation of the ERP packages.
Nov-06	[7(a)]	12		5	Enterprise Controlling
May-07	[2(b)]	12		10	How will you establish and implement Critical Success Factors (CSFs) and key Performance Indicators (KPIs) un an organisation for achieving the benefits of implementations of ERP?
Nov-07	[6(a)]	12		10	What is Enterprise Resources Planning? Briefly describe its benefits.
May-08	[4(a)]	12		5	Briefly explain the characteristics and features of an Enterprise Resource Planning.
Nov-08	[1(a)]	7		10	Briefly explain Enterprise Resource Planning(ERP) and

					describe five of its Characteristics.
Jun-09	[1(a)]	7		5	Practice Problem
Jun-09	[1(b)]	7		5	Practice Problem
Jun-09	[1(c)]	7		5	Practice Problem
Jun-09	[1(d)]	7		5	Suggest how to go about the implementation of ERP package.

8 - INFORMATION SYSTEM AUDITING STANDARDS GUIDELINES, BEST PRACTICES

INTRODUCTION: This chapter delves into some of the recommended and popular standards. Some have impacted domestic industry directly while some like HIPAA has primarily affected in India, Business Process Outsourced (BPOs) companies processing Health Information and other companies in India having interest in health industry and relations with entities of the same industry in USA.

1. IS AUDIT STANDARDS

Every profession has a unique repository of knowledge, which lends credence to its specialisation. The knowledge often forms the basis to define commonly accepted practices. Very often the technical competencies and skills of professionals are assessed against these practices. So the first step towards becoming a specialised professional is to gain a thorough understanding of this repository of knowledge. IS audit standards provide audit professionals a clear idea of the minimum level of acceptable performance essential to discharge their responsibilities effectively. Some of the standards discussed in this chapter by their year of birth are as follows:

Year – Standards: 1994 - COSO, CoCo; 1996 – HIPAA; 1998 - BS 7799; 2000 - COBIT

Discussion on these is presented in the order of their current trend of popularity and not year of birth perhaps in recognition of marketing power that all persons and products posses!

2. AAS 29 – AUDITING AND ASSURANCE STANDARD ON AUDITING IN A COMPUTER INFORMATION SYSTEMS ENVIRONMENT:

AAS 29 issued by the ICAI established standards on procedures to be followed when an audit relating to accounting information is conducted in a computer information systems environment. The pronouncement outlines the procedures that an auditor entrusted with financial, operational and other conventional audit objective relating to accounting information should carry out while auditing in a computerised environment.

AAS29 requires the auditor to consider the effect of a CIS environment on his audit and discuss the risks and caution that an auditor should exercise while carrying out traditional audit objectives in a computer information system environment and elaborates on the following:

 The auditor's responsibility in gaining sufficient understanding and assurance on the adequacy of accounting and internal controls that protect against the inherent and control risks in a CIS and the resulting considerations to be taken while designing audit procedures.

 The potential impact of auditing in a CIS on the assessment of control and audit risks.

 The auditor is required to determine the following factors to determine the effect of CIS environment on the audit arising from

 The extent to which the CIS is used for recording, compiling and analysing accounting information.

 The system of internal controls relating to the authorised, complete, accurate and valid processing and reporting procedures.

 The impact of CIS accounting system on the audit trail.

 The standard also requires the auditor to have sufficient knowledge of the CIS and possess appropriate specialised skills to enable him to plan, direct, supervise, control and review the work performed.

3. BS 7799

BS 7799 is an International Standard setting out the requirements for an Information Security Management System. It helps identify, manage and minimize the range of threats to which information is regularly subjected.

Specification for information security management systems" constitutes what is known as BS 7799 from the British

Standards Institute. The "Security Code of Conduct" from the British Government's Department of Trade and Industry was a originator from which grew BS 7799, which has, in turn, subsequently grown into ISO 17799. The Australian/New Zealand standard, AS/NZS 4444 is a very close adaptation of BS 7799.

BS 7799 Part 1 became an international standard (ISO/IEC 17799) in December 2000. It has been revised in line with ISO procedures. BS 7799 Part 2, although still a UK standard, it has been published as a national standard in many countries and is now itself at an advanced stage of international status.

From the outset, BS7799 focused on protecting the ***availabilit***y, ***confidentiality*** and ***integrity*** of organizational information and this remains, today, the driving objective of the standard. Though, it doesn't talk about protection from every single possible threat, but only from those that the organization considers relevant and only to the extent that is justified financially and commercially through a risk assessment. BS7799 was originally just a single standard, and had the status of a Code of Practice. In other words, it provided guidance for organizations, but hadn't been written as specification that could form the basis of an external third party verification and certification scheme.

3.1 Benefits of Using BS 7799

The benefits of using BS7799 are straightforward. Using it well will result in:

♦ Reduced operational risk
♦ Increased business efficiency
♦ Assurance that information security is being rationally applied

This is achieved by ensuring that:

♦ Security controls are justified.
♦ Policies and procedures are appropriate.
♦ Security awareness is good amongst staff and managers.
♦ All security relevant information processing and supporting activities are auditable and are being audited.
♦ Internal audit, incident reporting / management mechanisms are being treated appropriately.
♦ Management actively focus on information security and its effectiveness.

3.2 Components of BS 7799: The standard is composed of two parts: BS 7799 (ISO 17799) Part 1 - Code of Practice on Information Security Management and BS 7799 Part 2 – Specification for Information Security Management Systems. The Code of Practice on Information Security provides a comprehensive set of security controls comprising the best information security practices in current use. It is strongly business-orientated, focusing on being a good management tool rather than being concerned with technical details.

ISO 27001 – (BS7799: Part II) – Information Security Management Standard

It deals with the Information Security Management Standard (ISMS). In general, organizations shall establish and maintain documented ISMS addressing assets to be protected, organization approach to risk management, control objectives and control, and degree of assurance required.

(i) *Establishing Management Framework*: This would include the following activities:

 Define information security policy;
 Define scope of ISMS including functional, asset, technical, and locational boundaries;
 Make appropriate risk assessment;
 Identify areas of risk to be managed and degree of assurance required;
 Select appropriate controls;
 Prepare Statement of Applicability.

(ii) *Implementation*: Effectiveness of procedures to implement controls to be verified while reviewing security policy and technical compliance.

(iii) *Documentation*: The documentation shall consist of evidence of action undertaken under establishment of the following:
 Management control
 Management framework summary, security policy, control objective, and implemented control given in prepare Statement of Applicability
 Procedure adopted to implement control under Implementation clause
 ISMS management procedure
 Document Control: The issues focused under this clause would be
o Ready availability
o Periodic review
o Maintain version control;
o Withdrawal when obsolete
o Preservation for legal purpose
 Records: The issues involved in record maintenance are as follows:
o Maintain to evidence compliance to Part 2 of BS7799.;
o Procedure for identifying, maintaining, retaining, and disposing of such evidence;
o Records to be legible, identifiable and traceable to activity involved.
o Storage to augment retrieval, and protection against damage.

3.3 Areas of focus of ISMS: There are ten areas of focus of ISMS. These are described in the following paragraphs:
(i) Security Policy: This activity involves a thorough understanding of the organization business goals and its dependence on information security. This entire exercise begins with creation of the IT Security Policy. This is an extremely important task and should convey total commitment of top management-. The policy cannot be a theoretical exercise. It should reflect the needs of the actual users. It should be implementable, easy to understand and must balance the level of protection with productivity. The policy should cover
• a definition of information security
• a statement of management intention supporting the goals and principles of information security
• allocation of responsibilities for every aspect of implementation
• an explanation of specific applicable proprietary and general, principles, standards and compliance requirements.
• an explanation of the process for reporting of suspected security incidents
• a defined review process for maintaining the policy document
• means for assessing the effectiveness of the policy embracing cost and technological changes
• nomination of the policy owner

The detailed **control and objectives** are as follows:
• *Information Security Policy*: To provide management direction and support for information security
• *Information System Infrastructure*: To manage information security within the organisation
• *Security of third party access*: To maintain the security of organisational information processing facilities and information assets accessed by third parties
• *Outsourcing:* To maintain the security of information when the responsibility for information processing has been outsourced to another organization
ii) **Organisational Security :** A management framework needs to be established to initiate, implement and control information security within the organization. This needs proper procedures for approval of the information security policy, assigning of the security roles and coordination of security across the organization.
The detailed **control and objectives** are as follows:
• *Information System Infrastructure*: To manage information security within the organisation

• *Security of third party access*: To maintain the security of organisational information processing facilities and information assets accessed by third parties
• *Outsourcing:* To maintain the security of information when the responsibility for information processing has been outsourced to another organisation

(iii) Asset Classification and Control

One of the most laborious but essential task is to manage inventory of all the IT assets, which could be information assets, software assets, physical assets or other similar services. These information assets need to be classified to indicate the degree of protection. The classification should result into appropriate information labeling to indicate whether it is sensitive or critical and what procedure, is appropriate to copy, store, transmit or destruction of the information asset. An Information Asset Register (IAR) should be created detailing each of the following information asset within the organization:

- Databases
- Personnel records
- Scale models
- Prototypes
- Test samples
- Contracts
- Software licenses
- Publicity material

The Information Asset Register (IAR) should also describe who is responsible for each information asset and whether there is any special requirement for confidentiality, integrity or availability. For administrative convenience, separate register may be maintained under the subject head of IAR e.g. 'Media Register' will detail the stock of software and its licenses. One major advantage of following this practice is that, it provides a good back-up for example, in case the carton/label containing password is accidentally misplaced, media register will provide the necessary information. Similarly, 'Contracts Register' will contain the contracts signed and thus other details. The impact that is an addendum to mere maintenance of a register is control and thus protection of valuable assets of the corporation. The value of each asset can then be determined to ensure that appropriate security is in place.

The detailed **control and objectives** thereof are as follows:

- *Accountability for assets*: to maintain appropriate protection of organizational assets,
- *Information Classification*: to ensure that information assets receive an appropriate level of protection.

(iv) Personnel Security: Human errors, negligence and greed are responsible for most thefts, frauds or misuse of facilities. Various proactive measures that should be taken are, to make personnel screening policies, confidentiality agreements, terms and conditions of employment, and information security education and training. Alert and well-trained employees who are aware of what to look for can prevent future security breaches.

Appropriate personnel security ensures that:

• Employment contracts and staff handbooks have agreed, clear wording
• Ancillary workers, temporary staff, contractors and third parties are covered
• Anyone else with legitimate access to business information or systems is covered

The detailed control and objectives thereof are as follows:

• *Security in Job definition and Resourcing:* To reduce the risks of human error, theft, fraud, or misuse of facilities
• *User Training*: To ensure that users are aware of information security threats and concerns, and are equipped to support organisational security policy in course of their normal work
• *Responding to security incidents and malfunctions:* To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents

(v) Physical and Environmental Security: Designing a secure physical environment to prevent unauthorized access, damage and interference to business premises and information is usually the beginning point of any security plan. This involves physical security perimeter, physical entry control, creating secure offices, rooms, facilities, providing physical access controls, providing protection devices to minimize risks ranging from fire to electromagnetic radiation, providing adequate protection to power supplies and data cables are some of the activities. Cost effective design and constant

monitoring are two key aspects to maintain adequate physical security control.
The detailed **control and objectives** thereof are as follows:
• *Secure areas:* To prevent unauthorized access, damage and interference to business premises and information
• *Equipment Security:* To prevent loss, damage or compromise of assets and interruption to business activities
• *General Controls*: To prevent compromise or theft of information and information processing facilities
(vi)Communications and Operations Management: Properly documented procedures for the management and operation of all information processing facilities should be established. This includes detailed operating instructions and incident response procedures. Network management requires a range of controls to achieve and maintain security in computer networks. This also includes establishing procedures for remote equipment including equipment in user areas. Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks. Exchange of information and software between external organizations should be controlled, and should be compliant with any relevant legislation. Electronic commerce involves electronic data interchange, electronic mail and online transactions across public networks such as Internet.

The detailed **control and objectives** thereof are as follows:
• *Operational procedures and responsibilities:* To ensure correct and secure operation of information processing facility
• *System planning and acceptance:* To minimise risks of system failure
• *Protection against malicious software:* To protect the integrity of software and info
• *Housekeeping:* To maintain the integrity and availability of information processing and communication services
• *Network Management*: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure
• *Media handling and security:* Prevent damage to assets and interruptions to business activity
• *Exchanges of information and software:* To prevent loss, modification or misuse of information exchanged between organisations
(vii) Access Control: Access to information and business processes should be controlled on the business and security requirements. This will include defining access control policy and rules, user access management, user registration, privilege management, user password use and management, review of user access rights, network access controls, enforcing path from user terminal to computer, user authentication, node authentication, segregation of networks, network connection control, network routing control, operating system access control, user identification and authentication, use of system utilities, application access control, monitoring system access and use and ensuring information security when using mobile computing and tele-working facilities.
The detailed **control and objectives** thereof are as follows:
• *Business requirement for access control:* To control access to information
• *User access management:* To prevent unauthorised access to info systems
• *User responsibilities:* To prevent unauthorised user access
• *Network access control:* Protection of networked services
• *Operating system access control:* To prevent unauthorised computer access
• *Application Access Control:* To prevent unauthorised access to information held in information systems
• *Monitoring System Access and use:* To detect unauthorised activities
• *Mobile Computing and teleworking:* To ensure information security when using mobile computing & teleworking facilities
(viii) Systems Development and Maintenance: Security should ideally be built at the time of inception of a system. Hence security requirements should be identified and agreed prior to the development of information systems. This begins with security requirements analysis and specification and providing controls at every stage i.e. data input, data processing, data storage and retrieval and data output. It may be necessary to build applications with cryptographic controls. There should be a defined policy on the use of such controls, which may involve encryption, digital signature, use of digital certificates, protection of cryptographic keys and standards to be used for cryptography.
The detailed **control and objectives** thereof are as follows:
• *Security requirements of system:* To ensure that security is built into information systems

• *Security in application systems:* To prevent loss, modification or misuse of user data in application system
• *Cryptographic Controls:* To protect the confidentiality, authenticity or integrity of information
• *Security of system files:* To ensure that IT projects and support activities are conducted in a secure manner
• *Security in development and support process:* To maintain the security of application system software and information

(ix) Business Continuity Management: : A business continuity management process should be designed, implemented and periodically tested to reduce the disruption caused by disasters and security failures. This begins by identifying all events that could cause interruptions to business processes and depending on the risk assessment, preparation of a strategy plan. The plan needs to be periodically tested, maintained and re-assessed based on changing circumstances There is one control which is described herein below along with its objectives:

• *Aspects of business continuity management:* To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters

(x) Compliance: It is essential that strict adherence is observed to the provision of national and international IT laws, pertaining to Intellectual Property Rights (IPR), software copyrights, safeguarding of organizational records, data protection and privacy of personal information, prevention of misuse of information processing facilities, regulation of cryptographic controls and collection of evidence.

The detailed **control and objectives** thereof are as follows:

♦ *Compliance with legal requirements*: To avoid breaches of any criminal and civil law, and statutory, regulatory, or contractual obligations, and of any security requirements

♦ *Review of security policy and technical compliance:* To ensure compliance of systems with organisational security policies and standards

♦ *System Audit Consideration:* To maximise the effectiveness, and to minimise interference to/from the system audit process

4. CMM - CAPABILITY MATURITY MODEL

The CMM presents sets of recommended practices in a number of key process areas that have been shown to enhance software process capability. The CMM is based on knowledge acquired from software process assessments and extensive feedback from both industry and government. The Capability Maturity Model for Software provides software organizations with guidance on how to gain control of their processes for developing and maintaining software and how to evolve toward a culture of software engineering and management excellence. The CMM was designed to guide software organizations in selecting process improvement strategies by determining current process maturity and identifying the few issues most critical to software quality and process improvement.

A software process is a set of activities, methods, practices, and transformations that are used to develop and maintain software and the associated products such as project plans, design documents, code, test cases, and user manuals. Software process maturity is the extent to which a specific process is explicitly defined, managed, measured, controlled, and effective. Maturity implies a potential for growth in capability and indicates both the richness of an organization's software process and the consistency with which it is applied in projects throughout the organization. As a software organization gains in software process maturity, it institutionalization in software process building takes place.

The Five Levels of Software Process Maturity

Continuous process improvement is based on many small, evolutionary steps rather than revolutionary innovations. The CMM provides a framework for organizing these evolutionary steps into five maturity levels that lay successive foundations for continuous process improvement. These five maturity levels are discussed below

(i) *Level 1 - The Initial Level*: At the Initial Level, the organization typically does not provide a stable environment for developing and maintaining software. At this Level, capability is a characteristic of the individuals, not of the organization. During a crisis of software success depends entirely on having an exceptional manager and a seasoned and effective software team. But if someone leaves the project, it is difficult to handle the crises and a challenging task.

(ii) *Level 2 - The Repeatable Level*: At this Level, policies for managing a software project and procedures to implement

those policies are established. Planning and managing new projects is based on experience with similar projects. An effective process can be characterized as one which is practiced, documented, enforced, trained, measured, and able to improve. This Level makes the organizations to install basic software management controls. Software project standards are defined. The project's process is under the effective control of a project management system, following realistic plans based on the performance of previous projects.
(iii) *Level 3 - The Defined Level*: At this Level, documentation for development and maintenance is prepared. This standard process is referred to throughout the CMM as the organization's standard software process, to help the software managers and technical staff perform more effectively. A group of experts standardize the process. An organization-wide training program is implemented to ensure that the staff and managers have the knowledge and skills required to fulfill their assigned roles. This process capability is based on a common, organization wide understanding of the activities, roles, and responsibilities in a defined software process.
(iv) *Level 4 - The Managed Level*: At the Managed Level, the organization sets quantitative quality goals for both software products and processes. Productivity and quality are measured for important software process activities across all projects as part of an organizational measurement program. An organization-wide software process database is used to collect and analyze the data available from the projects' defined software processes. This level of capability allows an organization to product trende in process and product quality within qualitative limits. Because of the stability and measured data when some exceptional circumstance occurs, the special cause of variation can be identified and addressed. The software products are of predictably high quality.
(v) *Level 5 - The Optimizing Level*: The entire organization is focused on continuous process improvement. The organization has the means to identify weaknesses and strengthen the process proactively, with the goal of preventing the occurrence of defects. Data on the effectiveness of the software process is used to perform cost benefit analyses of new technologies and proposed changes to the organization's software process. In short, the cost of development is cut, best engineering practices are developed and used. Continuous improvement is done. Technology and process improvements are planned and managed as ordinary business activities.

5. Control Objectives for Information Related Technology (COBIT): The Information Systems Audit and Control Foundation (ISACF) developed the Control Objectives for Information and Related Technology (COBIT). COBIT is a trademark of generally applicable information systems security and control practices for IT controls. The framework allows:
(i) management to benchmark the security and control, practices *of* IT environments;
(ii) users of IT services to be assured that adequate security and control exist, and
(iii) auditors to substantiate their opinions on internal control and to advice on IT security and control matters.

The framework addresses the issue of control from three vantage points, or dimensions:
(1) Business Objectives. To satisfy business objectives, information must conform t*o* certain criteria the COBIT refers to as business requirements for information. The criteria are divided into seven distinct yet overlapping categories that map into the COSO objectives: effectiveness (relevant, pertinent, and timely), efficiency, confidentiality, integrity, availability, compliance with legal requirements and reliability.
(2) IT resources, while include people, application systems, technology, facilities, and data.
(3) IT processes, which are broken into four domains: planning and organization, acquisition and implementation, delivery and support, and monitoring.

COBIT, which consolidates standards from 36 different sources into a single framework, is having a big impact on the information systems profession. It is helping managers to learn how *to* balance risk and control investment in an information system environment. It provides users with greater assurance that the security and IT controls provided by internal and third parties are adequate. It guides auditors as they substantiate their opinions and as they provide advice to management on internal controls.

5. COBIT – IT Governance Model

COBIT is positioned to be comprehensive for management and to operate at a higher level than technology standards for information systems management. The underpinning concept of the COBIT Framework is that control in IT is approached by looking at information that is needed to support the business objectives or requirements, and by looking at information as being the result of the combined application of IT-related resources that need to be managed by IT processes. To satisfy business objectives, information needs to conform to certain criteria, which COBIT refers to as business requirements for information. In establishing the list of requirements, COBIT combines the principles embedded in existing and known reference models:

♦ *Quality Requirements:* Quality , Cost, Delivery

♦ *Fiduciary requirements* - Effectiveness and Efficiency of operations, Reliability of Information, Compliance with laws and regulations

♦ Security Requirements – Confidentiality, Integrity, Availability

5.1 COBIT's working definitions : Starting the analysis from the broader Quality, Fiduciary and Security requirements, seven distinct, certainly overlapping, categories were extracted. COBIT's working definitions are as follows:

♦ *Effectiveness* - deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.

♦ *Efficiency* - concerns the provision of information through the optimal (most productive and economical) use of resources.

♦ *Confidentiality* - concerns the protection of sensitive information from unauthorized disclosure.

♦ I*ntegrity* - relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.

♦ *Availability* - relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

♦ *Compliance* - deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria.

♦ *Reliability of Information* - relates to the provision of appropriate information for management to operate the entity and for management to exercise its financial and compliance reporting responsibilities.

5.2 IT resources : The IT resources identified in COBIT can be explained/defined as follows:

♦ *Data* - are objects in their widest sense (i.e. external and internal), structured and nonstructured, graphics, sound, etc.

♦ *Application systems* - are understood to be the sum of manual and programmed procedures.

♦ *Technology* - covers hardware, operating systems, database management systems, networking, multimedia, etc.

♦ *Facilities* - are all the resources to house and support information systems.

♦ *People* - include staff skills, awareness and productivity to plan, organize, acquire, deliver, support and monitor information systems and services.

5.3 The COBIT Framework: The COBIT Framework consists of high-level control objectives and an overall structure for their classification. The underlying theory for the classification is that there are, in essence, three levels of IT efforts when considering the management of IT resources. Starting at the bottom, there are the activities and tasks needed to achieve a measurable result. At the highest level, processes are naturally grouped together into domains. Their natural grouping is often confirmed as responsibility domains in an organisational structure and is in line with the management cycle or life cycle applicable to IT processes.

Domain of COBIT : With the preceding as the framework, the domains are identified using wording that management would use in the day-to-day activities of the organisation—not auditor jargon. Thus, four broad domains are identified: planning and organisation, acquisition and implementation, delivery and support, and monitoring. Definitions for the four domains identified for the high-level classification are:

♦ *Planning and Organisation* - This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. Furthermore, the realization of the strategic vision needs to be planned, communicated and managed for different perspectives. Finally, a proper organisation as well as technological infrastructure must be put in place. The following table lists the high level control objectives for the Planning and Organization domain.

Plan and Organize
PO1 Define a Strategic IT Plan and direction
PO2 Define the Information Architecture
PO3 Determine Technological Direction
PO4 Define the IT Processes, Organisation and Relationships
PO5 Manage the IT Investment
PO6 Communicate Management Aims and Direction
PO7 Manage IT Human Resources
PO8 Manage Quality
PO9 Assess and Manage IT Risks
PO10 Manage Projects
PO11 Manager Quality

♦ *Acquisition and Implementation* - To realize the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure that the life cycle is continued for these systems. The following table lists the high level control objectives for the Acquisition and Implementation domain.

Acquire and Implement
AI1 Identify Automated Solutions
AI2 Acquire and Maintain Application Software
AI3 Acquire and Maintain Technology Infrastructure
AI4 Enable Operation and Use
AI5 Procure IT Resources
AI6 Manage Changes
AI7 Install and Accredit Solutions and Changes

♦ *Delivery and Support* - This domain is concerned with the actual delivery of required services, which range from traditional operations over security and continuity aspects to training. In order to deliver services, the necessary support processes must be set up. This domain includes the actual processing of data by application systems, often classified under application controls. The following table lists the high level control objectives for the Delivery and Support domain.

Deliver and Support
DS1 Define and Manage Service Levels
DS2 Manage Third-party Services
DS3 Manage Performance and Capacity
DS4 Ensure Continuous Service
DS5 Ensure Systems Security
DS6 Identify and Allocate Costs
DS7 Educate and Train Users
DS8 Manage Service Desk and Incidents
DS9 Manage the Configuration
DS10 Manage Problems
DS11 Manage Data

DS12 Manage the Physical Environment
DS13 Manage Operations

♦ *Monitoring* - All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses management's oversight of the organization's control process and independent assurance provided by internal and external audit or obtained from alternative sources. The following table lists the high level control objectives for the Monitoring domain.

Monitor and Evaluate
ME1 Monitor and Evaluate IT Processes
ME2 Monitor and Evaluate Internal Control
ME3 Ensure Regulatory Compliance
ME4 Provide IT Governance

5.4 COBIT and Other Standards
1) COBIT and ISO/IEC 17799:2005: The two international standards used today are COBIT and ISO/IEC 17799:2005. COBIT (Control Objectives for Information and related Technology) was released and used primarily by the IT community. In 1998, Management Guidelines were added, and COBIT became the internationally accepted framework for IT governance and control. ISO/IEC 17799:2005 (The Code of Practice for Information Security Management) is also an international standard and is best practice for implementing security management. The two standards do not compete with each other and actually complement one another. COBIT typically covers a broader area while ISO/IEC 17799 is deeply focused in the area of security.

2) COBIT and Sarbanes Oxley : Public companies that are subject to the U.S. Sarbanes Oxley Act of 2002 are encouraged to adopt the following control frameworks: the Committee of Sponsoring Organizations of the Treadway Commission – COSO Internal Control Integrated Framework and the IT Governance Institute's Control Objectives for Information and Related Technology –COBIT. In choosing which of the control frameworks to implement in order to comply with Sarbanes-Oxley, the U.S. Securities and Exchange Commission suggests that companies follow the COSO framework.

3) **COSO** COBIT approaches IT control by looking at information not just financial information that is needed to support business requirements and the associated Information Technology (IT) resources and processes. COSO control objectives focus on effectiveness, efficiency of operations, reliable financial reporting, and compliance with laws and regulations.

6. COCO
The "Guidance on Control" report, known colloquially as CoCo, was produced in 1999 by the Criteria of Control Board of The Canadian Institute of Chartered Accountants. CoCo does not cover any aspect of information assurance per se. It is concerned with control in general. CoCo is "guidance," meaning that it is not intended as "prescriptive minimum requirements" but rather as "useful in making judgments" about "designing, assessing and reporting on the control systems of organizations." As such, CoCo can be seen as a model of controls for information assurance, rather than a set of controls. CoCo's generality is one of its strengths: if information assurance is just another organizational activity, then the criteria that apply to controls in other areas should apply to this one as well. CoCo "builds on the concepts in the COSO document." CoCo can be said to be a concise superset of COSO. It uses the same three categories of objectives:
•effectiveness and efficiency of operations
•reliability of financial reporting
•compliance with applicable laws and regulations
Four important concepts about "control" are as follows:
1 Control is affected by people throughout the organization, including the board of directors (or its equivalent), management and all other staff.
2 People who are accountable, as individuals or teams, for achieving objectives should also be accountable for the

effectiveness of control that supports achievement of those objectives.
3 Organizations are constantly interacting and adapting.
4 Control can be expected to provide only reasonable assurance, not absolute assurance.

7. ITIL (IT INFRASTRUCTURE LIBRARY)

The IT Infrastructure Library (ITIL) is so named as it originated as a collection of books (standards) each covering a specific 'practice' within IT management. After the initial published works, the number of publications quickly grew (within ITIL v1) to over 30 books. In order to make ITIL more accessible (and affordable) to those wishing to explore it, one of the aims of the ITIL v2 project was to consolidate the works into a number of logical 'sets' that aimed to group related sets of process guidelines for different aspects of the management of Information Technology systems, applications and services together

The eight ITIL books and their disciplines are:
The **IT Service Management** sets relating to
1. Service Delivery
2. Service Support

Other operational guidance relating to

3. ICT Infrastructure Management
4. Security Management
5. The Business Perspective
6. Application Management
7. Software Asset Management

To assist with the implementation of ITIL practices a further book was published providing guidance on implementation (mainly of Service Management)
8. Planning to Implement Service Management

8. SYSTRUST AND WEBTRUST

SysTrust and WebTrust are two specific services developed by the AICPA that are based on the Trust Services Principles and Criteria. SysTrust engagements are designed for the provision or advisory services or assurance on the reliability of a system. WebTrust engagements relate to assurance or advisory services on an organization's system related to e-commerce. Only certified public accountants (CPAs) may provide the assurance services of Trust Services that result in the expression of a Trust Services, WebTrust, or SysTrust opinion, and in order to issue SysTrust or WebTrust reports, CPA firms must be licensed by the AICPA.
The following principles and related criteria have been developed by the AICPA/CICA for use by practitioners in the performance of Trust Services engagements such as SysTrust and WebTrust.
♦ *Security.* The system is protected against unauthorized access (both physical and logical).
♦ *Availability.* The system is available for operation and use as committed or agreed.
♦ *Processing integrity.* System processing is complete, accurate, timely, and authorized.
♦ *Online privacy.* Personal information obtained as a result of e-commerce is collected, used, disclosed, and retained as committed or agreed.
♦ *Confidentiality.* Information designated as confidential is protected as committed or agreed.
Each of these Principles and Criteria are organized and presented in four broad areas:
♦ *Policies*. The entity has defined and documented its policies relevant to the particular principle.
♦ *Communications.* The entity has communicated its defined policies to authorized users.
♦ *Procedures.* The entity uses procedures to achieve its objectives in accordance with its defined policies.
♦ *Monitoring.* The entity monitors the system and takes action to maintain compliance with its defined policies.

At the completion of a SysTrust engagement, the practitioner renders an opinion on the management's assertion that effective controls have been maintained. The practitioner can report on all the SysTrust principles together or on each

separately.

9. HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) were enacted by the U.S. Congress in 1996.

♦ Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.

♦ Title II of HIPAA, the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The AS provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the US health care system. What is of interest here is the Security Rule issued under the Act

9.1 The Security Rule: the security lays out three types of security safeguards required for compliance :

1) administrative,
2) physical, and
3) technical.

For each of these types, the Rule identifies various security standards, and for each standard, it names both required and addressable implementation specifications. The standards and specifications are as follows:

(a). Administrative Safeguards - policies and procedures designed to clearly show how the entity will comply with the act

♦ Covered entities (entities that must comply with HIPAA requirements) must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures.

♦ The policies and procedures must reference management oversight and organizational buy-in to compliance with the documented security controls.

♦ Procedures should clearly identify employees or classes of employees who will have access to protected health information (PHI). Access to PHI in all forms must be restricted to only those employees who have a need for it to complete their job function.

♦ The procedures must address access authorization, establishment, modification, and termination.

♦ Entities must show that an appropriate ongoing training program regarding the handling PHI is provided to employees performing health plan administrative functions.

♦ Covered entities that out-source some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements. Companies typically gain this assurance through clauses in the contracts stating that the vendor will meet the same data protection requirements that apply to the covered entity. Care must be taken to determine if the vendor further out-sources any data handling functions to other vendors and monitor whether appropriate contracts and controls are in place.

♦ A contingency plan should be in place for responding to emergencies. Covered entities are responsible for backing up their data and having disaster recovery procedures in place. The plan should document data priority and failure analysis, testing activities, and change control procedures.

♦ Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying potential security violations. Policies and procedures should specifically document the scope, frequency, and procedures of audits. Audits should be both routine and event-based.

♦ Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or the normal course of operations.

(b) Physical Safeguards - controlling physical access to protect against inappropriate access to protected data

♦ Controls must govern the introduction and removal of hardware and software from the network. (When equipment is retired it must be disposed of properly to ensure that PHI is not compromised.)

♦ Access to equipment containing health information should be carefully controlled and monitored.

♦ Access to hardware and software must be limited to properly authorized individuals.

♦ Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts.
♦ Policies are required to address proper workstation use. Workstations should be removed from high traffic areas and monitor screens should not be in direct view of the public.
♦ If the covered entities utilize contractors or agents, they too must be fully trained on their physical access responsibilities.

(c) Technical Safeguards - controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient
♦ Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized. If closed systems/networks are utilized, existing access controls are considered sufficient and encryption is optional.
♦ Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner.
♦ Data corroboration, including the use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity.
♦ Covered entities must also authenticate entities it communicates with. Authentication consists of corroborating that an entity is who it claims to be. Examples of corroboration include: password systems, two or three-way handshakes, telephone call-back, and token systems.
♦ Covered entities must make documentation of their HIPAA practices available to the government to determine compliance.
♦ In addition to policies and procedures and access records, information technology documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing.
♦ Documented risk analysis and risk management programs are required.

10. SAS 70 – STATEMENT OF AUDITING STANDARDS FOR SERVICE ORGANISATIONS

Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A SAS 70 audit or service auditor's examination is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes. In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers.

SAS No. 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. A formal report including the auditor's opinion ("Service Auditor's Report") is issued to the service organization at the conclusion of a SAS 70 examination.

SAS 70 provides guidance to enable an independent auditor ("service auditor") to issue an opinion on a service organization's description of controls through a Service Auditor's Report. SAS 70 is not a pre-determined set of control objectives or control activities that service organizations must achieve. Service auditors are required to follow the AICPA's standards for fieldwork, quality control, and reporting. A SAS 70 examination is not a "checklist" audit.

SAS No. 70 is generally applicable when an auditor ("user auditor") is auditing the financial statements of an entity ("user organization") that obtains services from another organization ("service organization"). Service organizations that provide such services could be application service providers, bank trust departments, claims processing centres, Internet

data centres, or other data processing service bureaus.

10.1 Service Auditor's Reports: One of the most effective ways a service organization can communicate information about its controls is through a Service Auditor's Report. There are two types of Service Auditor's Reports: Type I and Type II.

A Type I report describes the service organization's description of controls at a specific point in time (e.g. June 30, 2003).

A Type II report not only includes the service organization's description of controls, but also includes detailed testing of the service organization's controls over a minimum six month period (e.g. January 1, 2003 to June 30, 2003). The contents of each type of report is described in the following table:

Report Contents	**Type I Report**	**Type II Report**
1. Independent service auditor's report (i.e. opinion).	Included	Included
2. Service organization's description of controls.	Included	Included
3. Information provided by the independent service auditor; includes a description of the service auditor's tests of operating effectiveness and the results of those tests.	Optional	Included
4. Other information provided by the service organization (e.g. glossary of terms).	Optional	Optional

In a Type I report, the service auditor will express an opinion on (1) whether the service organization's description of its controls presents fairly, in all material respects, the relevant aspects of the service organization's controls that had been placed in operation as of a specific date, and (2) whether the controls were suitably designed to achieve specified control objectives.

In a Type II report, the service auditor will express an opinion on the same items noted above in a Type I report, and (3) whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.

10.2 Benefits to the Service Organization: Service organizations receive significant value from having a SAS 70 engagement performed. A Service Auditor's Report with an unqualified opinion that is issued by an Independent Accounting Firm differentiates the service organization from its peers by demonstrating the establishment of effectively designed control objectives and control activities. A Service Auditor's Report also helps a service organization build trust with its user organizations (i.e. customers).

10.3 Benefits to the User Organization: User organizations that obtain a Service Auditor's Report from their service organization(s) receive valuable information regarding the service organization's controls and the effectiveness of those controls.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-08	[4(a)]	8		10	*What do you understand by Software Process Maturity? Discuss five levels of Software Process Maturity of Capability Maturity Model(CMM).*

Jun-09	[5(a)]	8		10	*When an organization is audited for the effective implementation of ISO 27001-(BS 7799: part II) - information Security management System, what are to be verified under.* *(i) Establishing Management Framework* *(ii) Implementation* *(iii) Documentation.*
Jun-09	[5(c)]	8		5	*Briefly explain Asset classification and Control under Information Security management Systems.*
Jun-09	[7(b)]	8		5	*Control Objectives for Information related Technology (COBIT)*

9 - DRAFTING OF IS SECURITY POLICY, AUDIT POLICY, IS AUDIT REPORTING – A PRACICAL PERSPECTIVE

1. WHAT IS INFORMATION SYSTEM SECURITY?

Security relates to the protection of valuable assets against loss, disclosure, or damage. Securing valuable assets from threats, sabotage, or natural disaster with physical safeguards such as locks, perimeter fences, and insurance is commonly understood and implemented by most organizations. However, security must be expanded to include logical and other technical safeguards such as user identifiers, passwords, firewalls, etc. which are not understood nearly as well by organizations as physical safeguards. In organizations where a security breach has been experienced, the effectiveness of security policies and procedures has had to be reassessed.

This concept of security applies to all information. In this context, the valuable assets are the data or information recorded, processed, stored, shared, transmitted, or retrieved from an electronic medium. The data or information is protected against harm from threats that will lead to its loss, inaccessibility, alteration, or wrongful disclosure. The protection is achieved through a layered series of technological and non-technological safeguards such as physical security measures, user identifiers, passwords, smart cards, biometrics, firewalls, etc.

Security Objective : The objective of information system security is "the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity". For any organization, the security objective is met when:

• **Confidentiality**: Data and information are disclosed only to those who have a right to know it

• **Integrity**: Data and information are protected against unauthorised modification

• **Availability**: Information systems are available and usable when required

The relative priority and significance of confidentiality, integrity and availability vary according to the data within the information system and the business context in which it is used.

1.1 What information is sensitive?: The following examples highlight a few of the many factors necessary for a company to succeed. The common thread in each case is the critical information that each generates.

• **Strategic Plans:** Most organizations readily acknowledge that strategic plans are crucial to the success of a company. But do most companies really make an effort to protect these plans?

• **Business Operations:** Business operations consist of an organization's process and procedures, most of which are deemed to be proprietary. As such, they may provide a market advantage to the organization. This is the case when one company can provide a service profitably at a lower price than the competition. A company's client lists and the prices charged for various products and services can also be damaging in the hands of a competitor.

• **Finances:** Financial information, such as salaries and wages, are very sensitive and should not be made public. While general salary ranges are known within industry sectors, precise salary information can provide a competitive edge. As salaries and wage-related charges normally comprise the majority of fixed costs, lower costs in this area contribute directly to an organization's profitability. When a competitor knows specific information about a company's wages, the competitor may be able to price its products accordingly. When competitors' costs are lower, they can either under-price the market or increase profits. In either case, the damage to an organization may be significant.

1.2 Establishing better information protection: The examples above highlight only three of the various types of sensitive information every business holds. Protecting this information is crucial to the overall success or failure of a company. Businesses hold such a vast array of data, what steps do they need to take to keep all of their critical information protected? These points may be considered:

• **Not all data has the same value.** And, as such, the information may be handled and protected differently. Organizations must determine the value of the different types of information in their environment before they can plan for the appropriate levels of protection.

• **Know where the critical data resides.** In today's business environment, this is normally the company's information systems infrastructure. Because each piece of information may require different levels of protection, identifying where each is located enables an organization to establish an integrated security solution.

• **Develop an access control methodology. Information does not have to be removed to** cause damage or to have financial impact. Information that is inadvertently damaged disclosed or copied without the knowledge of the owner may render the data useless. To guard against this, organizations must establish some type of access control methodology.

• **Protect information stored on media. Employees can cause considerable damage by** walking out the door with information on 3 ½-inch floppy disks or CD-ROMS. In addition, companies should control magnetic media to reduce the loss of software (both application and operating system). And finally, when migrating from one platform to another, the status of all hard drives, and the associated data, should be controlled.

• **Review hardcopy output.** The hardcopy output of employees' daily work should also be reviewed. Although strategic plans in their final forms may be adequately protected, what measures are used to safeguard all drafts and working papers? What information is regularly placed in the recycle or trash containers without thought to its value?

2. PROTECTING COMPUTER-HELD INFORMATION SYSTEMS

Prior to discussing the details of how to protect the information systems, we need to define a few basic ground rules that must be addressed sequentially:

• **Rule #1:** We need to know what the information systems are and where these are located.

• **Rule #2:** We need know the value of the information held and how difficult it would be to recreate if it were damaged or lost.

• **Rule #3:** We need to know who is authorized to access the information and what they are permitted to do with the information.

• **Rule #4:** We need to know how quickly information needs to be made available should it become unavailable for whatever reason (loss, unauthorized modification, etc.)

These four rules are deceptively simple. For most organizations, providing answers to permit the design and implementation of any information system protection is very taxing.

There are two basic types of protection that an organization can use: Preventative and Restorative.

1) Preventative Information Protection : This type of protection is based on use of security controls. Information system security controls are generally grouped into three types of control: Physical, Logical, and Administrative. Organizations require all three types of controls. The organization's Information Security Policy through the associated Information Security Standards documentation mandates use of these controls. Here are some examples of each type of control:

• **Physical:** Doors, Locks, Guards, Floppy Disk Access Locks, Cables locking systems to desks/walls, CCTV, Paper Shredders, Fire Suppression Systems

• **Logical (Technical):** Passwords, File Permissions, Access Control Lists, Account Privileges, Power Protection Systems

• **Administrative:** Security Awareness, User Account Revocation, Policy

2) Restorative Information Protection: Security events that damage information sytems will happen. If an organization cannot recover or recreate critical information systems n an acceptable time period, the organization will suffer and possibly have to go out of business. Planning and operating an effective and timely information system backup and recovery program is vital to an operation. Information system backup does not simply involve backing up "just the valuable information," but it frequently also means backing up the system as well, since the information may need services that the system provides to make the information usable. The key requirement of any restorative information system protection plan is that the information systems can be recovered. This is frequently an issue that many

organizations fail to properly address. There is a common belief that if the backup program claimed it wrote the information system to the backup media, it can be recovered from the backup media. However, there are many variables that can prove that belief wrong.
Here are a few questions any restorative information system protection program must address:
• Has the recovery process been tested recently?
• How long did it take?
• How much productivity was lost?
• Did everything go according to plan?
• How much extra time was needed to input the data changes since the last backup?

3) Holistic Protection: Protecting corporate information systems from harm or loss is not an easy task. Protection must be done holistically and give the organization the appropriate level of security at a cost that is acceptable to the business.

3. INFORMATION SECURITY POLICY
A Policy is a plan or course of action, designed to influence and determine decisions, actions and other matters. The security policy is a set of laws, rules, and practices that regulates how assets including sensitive information are managed, protected, and distributed within the user organisation.
An information Security policy addresses many issues such as disclosure, integrity and availability concerns, who may access what information and in what manner, basis on which access decision is made, maximised sharing versus least privilege, separation of duties, who controls and who owns the information, and authority issues.

3.1 Issues to address: This policy does not need to be extremely extensive, but clearly state senior management's commitment to information security, be under change and version control and be signed by the appropriate senior manager. The policy should at least address the following issues:
• a definition of information security,
• reasons why information security is important to the organisation, and its goals and principles,
• a brief explanation of the security policies, principles, standards and compliance requirements,
• definition of all relevant information security responsibilities
• reference to supporting documentation.

3.2 Members of Security Policy: Security has to encompass managerial, technological and legal aspects. Security policy broadly comprises the following three groups of management:
• Management members who have budget and policy authority
• Technical group who know what can and cannot be supported
• Legal experts who know the legal ramifications of various policy charges

4. TYPES OF INFORMATION SECURITY POLICIES AND THEIR HIERARCHY
Various types of information security policies are:
1. *Information Security Policy* - This policy provides a definition of Information Security, its overall objective and the importance that applies to all users.
2. *User Security Policy* – This policy sets out the responsibilities and requirements for all IT system users. It provides security terms of reference for Users, Line Managers and System Owners.
3. *Acceptable Usage Policy* – This sets out the policy for acceptable use of email and Internet services.
4. *Organisational Information Security Policy* – This policy sets out the Group policy for the security of its information assets and the Information Technology (IT) systems processing this information. Though it is positioned at the bottom of the hierarchy, it is the main IT security policy document.
5. *Network & System Security Policy* – This policy sets out detailed policy for system and network security and applies to

IT department users
6. *Information Classification Policy* - This policy sets out the policy for the classification of information
7. *Conditions of Connection* – This policy sets out the Group policy for connecting to their network. It applies to all organizations connecting to the Group, and relates to the conditions that apply to different suppliers' systems.

4.1 Components of the Security Policy: A good security policy should clearly state the following:
• Purpose and Scope of the Document and the intended audience
• The Security Infrastructure
• Security policy document maintenance and compliance requirements
• Incident response mechanism and incident reporting
• Security rganization Structure
• Inventory and Classification of assets
• Description of technologies and computing structure
• Physical and Environmental Security
• Identity Management and access control
• IT Operations management
• IT Communications
• System Development and Maintenance Controls
• Business Continuity Planning
• Legal Compliances
• Monitoring and Auditing Requirements
• Underlying Technical Policy

4.2 Purpose and Scope: It defines what the uthorizedd is trying to accomplish through the policy. The primary objective of the policy would be to ensure confidentiality, integrity and availability of information and related systems. The security policy is designed to:
(a). Deny uthorizedd access to any IT resources, and Restrict access to data and resources or IT processes.
(b). Within the operational constraints, the security controls will allow the required services to be available to authorized users only.
(c). The scope defines how far the policy would be applicable, to whom it would be applicable and the period for which the policy would be applicable.

4.3 Security Organisation Structure: The security responsibility and the line of reporting in the organisation should be defined in the policy as stated below:
• **Information Security Forum (ISF):** This forum is chaired by the GSO and includes senior representatives from each of the divisions within the Group, together with the AGSO. The AGSO provides the reporting conduit from the ISMG. It is the role of this forum to ensure that there is clear direction and visible management support of security initiatives within the organisation.
• **Information Security Management Group (ISMG):** This cross functional group is chaired by the AGSO and comprises of a Divisional System Security Officer (DSSO) from each of the divisions within the Group, together with the IT Security Officer (ITSO), and the Personnel and Facilities Management Security Officers. Its role is to co-ordinate the implementation and management of information security controls across all of the divisions and sites.
• **Group Security Officer (GSO):** The GSO will have overall responsibility for security within the Group. This includes the security of all information assets, the network accreditation scheme and for non-IT security including physical and personnel matters.
• **Assistant Group Security Officer (AGSO):** The AGSO reports to the GSO and the Information Security Forum and is responsible for the co-ordination of information security implementation and management across the Group. The AGSO chairs the ISMG.

• **IT Management:** IT Management have overall responsibility for security of the IT infrastructure. This is discharged mainly through Installation Security Officers (ISOs) and the IT Security Officer (ITSO) who will report directly to the IS Service Manager.

• **IT Security Officer (ITSO)**: The IT Security Officer reports to the ISMG on IT security matters. The ITSO is responsible for managing IT security programmes and IT security incidents. The ITSO will chair regular meetings of the ISO's.

• **Installation Security Officer (ISO):** An ISO will be appointed for each IT environment (including Network and Desktop) from the IT Team Leaders. ISOs will be responsible for all security matters related to their system/installation and/or network and will meet regularly with the IT Security Officer.

• **Personnel Security Officer (PSO):** The Personnel Security Officer (PSO) will report directly to Personnel Management and the ISMG on all security matters relating to personnel. The role involves ensuring the controls set out are implemented, adhered to and reviewed as necessary.

• **Facilities Management Security Officer (FMSO)**: The Facilities Management Security Officer (FMSO) will report directly to Facilities Management on all security matters relating to personnel. The role involves ensuring the controls are implemented, adhered to and reviewed as necessary.

• **Divisional System Security Officer (DSSO):** A System Security Officer (SSO) from each division will be appointed as a DSSO. The DSSO carries the same responsibilities as a SSO and in addition is responsible for representing the SSOs in their division at the ISMG and for communicating requirements and issues to/from this group.

• **System Security Officer (SSO):** A senior user will be appointed to fulfil the role of System Security Officer (SSO) for each major application system or group of systems. SSO responsibilities focus on business aspects of security thus ensuring that the information security of the system meets all relevant business control objectives.

• **System Owners**: System Owners carry the overall responsibility for the information security of their own systems. Much of the day to day operational aspects of live systems may be delegated across a range of user defined roles and technical roles including their systems accreditation process. System Owners are responsible for allocation of protective markings to their systems and data according to the Information classification policy, and all staff for treating protectively marked material accordingly.

• **Line Managers:** All Line Managers with any responsibility for live or developing IT systems must take appropriate steps to ensure compliance with the aims and objectives of this policy. As part of this process they will ensure that all required security measures are understood and in force.

Users: All users of live IT systems are required to comply with the security procedures for their system and any applicable general IT security guidance.

4.4 Responsibility allocation: The responsibilities for the management of Information Security should be set out in this policy.

• An owner would be appointed for each information asset.

• All staff should be aware of the need for Information Security and should be aware of their responsibilities.

• been completed successfully and the System Owner is satisfied.

• All new network communications links must be approved.

• A contact list of organisations that may be required in the event of a security incident to be maintained.

• Risk assessments for all third party access to the information assets and the IT Network must be carried out.

• Access by third parties to all material related to the IT Network and infrastructure must be strictly limited and controlled. There should be a Conditions of Connection agreement in place for all third party connections.

• All outsourcing contracts must detail all major changes to software and hardware including major updates and new versions must be approved. It is not permissible to make the changes to a live system until tests have security responsibilities

4.5. Asset Classification and Security Classification:

• An inventory of assets must be maintained. This must include physical, software and information assets.

• A formal, documented classification scheme (as set out in the Information Classification Policy) should be in place and all staff must comply with it.

• The originator or 'owner' of an item of information (e.g. a document, file, diskette, printed report, screen display, e-mail, etc.) should provide a security classification, where appropriate.
• The handling of information, which is protectively marked CONFIDENTIAL or above must be specifically approved (i.e. above RESTRICTED).
• Exchanges of data and software between organisations must be controlled. Organisations to whom information is to be sent must be informed of the protective marking associated with that information, in order to establish that it will be handled by personnel with a suitable clearance corresponding to the protective marking.
• Appropriate procedures for information labelling and handling must be agreed and put into practice.
• Classified waste must be disposed of appropriately and securely.

4.6 Access Control
• Access controls must be in place to prevent unauthorised access to information systems and computer applications
• Access must only be granted in response to a business requirement. Formal processes must be in place to provide individuals with access. The requirement for access must be reviewed regularly.
• System Owners are responsible for approving access to systems and they must maintain records of who has access to a particular system and at what level. The actual access controls in place must be audited against this record on a regular basis.
• Users should be granted access to systems only up to the level required to perform their normal business functions.
• The registration and de-registration of users must be formally managed.
• Access rights must be deleted for individuals who leave or change jobs.
• Each individual user of an information system or computer application will be provided with a unique user identifier (user id)
• It should not be permitted for an individual to use another person's user id or to log-on, to allow another individual to gain access to an information system or computer application.
• PCs and terminals should never be left unattended whilst they are connected to applications or the network. Someone may use the equipment to access confidential information or make unauthorised changes.
• Passwords Policy should be defined and the structure of passwords and the duration of the passwords should be specified. Passwords must be kept confidential and never disclosed to others.
• Mobile computing - When using mobile computing facilities, such as laptops, notebooks, etc., special care should be taken to ensure that business information is not compromised, particularly when the equipment is used in public places.

4.7 Incident Handling:
• Security incident reporting times and approach must be consistent at all times. Specific procedures must be introduced to ensure that incidents are recorded and any recurrence is analysed to identify weaknesses or trends.
• Procedures for the collection of evidence relating to security incidents should be standardised. All staff must be made aware of the process. Adequate records must be maintained and inspections facilitated to enable the investigation of security breaches or concerted attempts by third parties to identify security weaknesses.

4.8 Physical and Environmental Security
• Physical security should be maintained and checks must be performed to identify all vulnerable areas within each site.
• The IT infrastructure must be physically protected.
• Access to secure areas must remain limited to authorised staff only.
• Confidential and sensitive information and valuable assets must always be securely locked away when not in use.
• Computers must never be left unattended whilst displaying confidential or sensitive information or whilst logged on to systems.
• Supplies and equipment must be delivered and loaded in an isolated area to prevent any unauthorised access to key facilities
• Equipment, information or software must not be taken off-site without proper authorisation.

• Wherever practical, premises housing computer equipment and data should be located away from, and protected against threats of deliberate or accidental damage such as fire and natural disaster.
• The location of the equipment room(s) must not be obvious. It will also where practical be located away from, and protected against threats of, unauthorised access and deliberate or accidental damage, such as system infiltration and environmental failures

4.9 Business Continuity Management
• A Business Continuity Plan (BCP) must be maintained, tested and updated if necessary. All staff must be made aware of it.
• A Business Continuity and Impact Assessment must be conducted annually.
• Suppliers of network services must be contractually obliged to provide a predetermined minimum service level.

4.10 System Development and Maintenance Controls
• System development or enhancements must have appropriate security controls included to safeguard their availability and ensure the integrity and confidentiality of the information they process.
• All security requirements and controls must be identified and agreed prior to the development of information systems.

5. AUDIT POLICY
5.1 Purpose of the audit policy : Purpose of this audit policy is to provide the guidelines to the audit team to conduct an audit on IT based infrastructure system. The Audit is done to protect entire system from the most common security threats which includes the following:
• Access to confidential data
• Unauthorized access of the department computers.
• Password disclosure compromise
• Virus infections.
• Denial of service attacks
• Open ports, which may be accessed from outsiders
• Unrestricted modems unnecessarily open ports
Audits may be conducted to ensure integrity, confidentiality and availability of information and resources.

objective and the scope of the IS Audit policy
The IS Audit Policy should lay out the objective and the scope of the Policy. An IS audit is conducted to
• Safeguarding of Information System Assets/Resources
• Maintenance of Data Integrity
• Maintenance of System Effectiveness
• Ensuring System Efficiency
• Compliance with Information System related policies, guidelines, circulars, and any other instructions requiring compliance in whatever name called.

5.2 Scope of IS Audit : The scope of information system auditing should encompass the examination and evaluation of the adequacy and effectiveness of the system of internal control and the quality of performance by the information system. Information System Audit will examine and evaluate the planning, organising, and directing processes to determine whether reasonable assurance exists that objectives and goals will be achieved. Such evaluations, in the aggregate, provide information to appraise the overall system of internal control. The scope of the audit will also include the internal control system(s) for the use and protection of information and the information system, as under:
• Data
• Application systems
• Technology
• Facilities

• People

The Information System auditor will consider whether the information obtained from the above reviews indicates coverage of the appropriate areas. The information system auditor will examine, among others, the following:

• Information system mission statement and agreed goals and objectives for information system activities.
• Assessment of the risks associated with the use of the information systems and approach to managing those risks.
• Information system strategy plans to implement the strategy and monitoring of progress against those plans.
• Information system budgets and monitoring of variances.
• High level policies for information system use and the protection and monitoring of compliance with these policies.
• Major contract approval and monitoring of performance of the supplier.
• Monitoring of performance against service level agreements.
• Acquisition of major systems and decisions on implementation.
• Impact of external influences on information system such as internet, merger of suppliers or liquidation etc.
• Control of self-assessment reports, internal and external audit reports, quality assurance reports or other reports on Information System.
• Business Continuity Planning, Testing thereof and Test results.
• Compliance with legal and regulatory requirements.
• Appointment, performance monitoring and succession planning for senior information system staff including internal information system audit management and business process owners.

5.3 IS Audit Reports :-

According to the recommendations, IS Audit reports broadly include the following sections: title page, table of contents, summary including the recommendations, introduction, findings and appendices. These components of an audit report are discussed below:

(i) *Cover and Title Page*: Audit reports should use a standard cover, with a window showing the title: "Information System Audit" or "Data Audit", the department's name and the report's date of issue (month and year). These items are repeated at the bottom of each page. The title page may also indicate the names of the audit team members.

(ii) *Table of Contents* : The table lists the sections and sub-sections with page numbers including summary and recommendations, introduction, findings (by audit field) and appendices (as required).

(iii) *Summary / Executive Summary* : The summary gives a quick overview of the salient features at the time of the audit in light of the main issues covered by the report. It should not normally exceed three pages, including the recommendations.

(iv) *Introduction* : Since readers will read the summary, the introduction should not repeat details. It should include the following elements:

 Context: This sub-section briefly describes conditions in the audit entity during the period under review, for instance, the entity's role, size and organisation especially with regard to information system management, significant pressures on information system management during the period under review, events that need to be noted, organisational changes, IT disruptions, changes in roles and programs, results of internal audits or follow-up to our previous audits, if applicable.

 Purpose: This sub-section is a short description of what functions and special programs were audited and the clients' authorities.

 Scope: The scope lists the period under review, the issues covered in each function and program, the locations visited and the on-site dates.

 Methodology: This section briefly describes sampling, data collection techniques and the basis for auditors' opinions. It also identifies any weaknesses in the methodology to allow the client and auditee to make informed decisions as a result of the report.

(v) *Findings*: Findings constitute the main part of an audit report. They result from the examination of each audit issue in the context of established objectives.

(vi) *Opinion*: If the audit assignment requires the auditor to express an audit opinion, the auditor shall do so in

consonance to the requirement.

(vii) *Appendices*: Appendices can be used when they are essential for understanding the report. They usually include comprehensive statistics, quotes from publications, documents, and references.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Jun-09	[6(a)]	9		10	*What purpose the information system audit policy will serve? Briefly describe the scope of information system audit.*
Nov-08	[4(b)]	9		5	*Discuss various types of Information Security polices and their hierarchy.*
Nov-08	[4(c)]	9		5	*State and briefly explain the contents of a Standard information System Audit Report.*
Jun-09	[5(b)]	9		5	*The Information Security Policy of an organization has been defined and documented as given below: "Our organization is committed to ensure Information Security through established goals and principles. Responsibilities for implementing every aspect of specific applicable proprietary and general principles, standards and compliance requirements have been defined. This is reviewed at least once a year for continued suitability with regard to cost and technological changes." Identify the salient components that have not been covered in the above policy.*

10 - INFORMATION TECHNOLOGY ACT, 2000

I. Brief History

The Government of India realized the need for introducing a new law and for making suitable amendments to the existing laws to facilitate **e-commerce and give legal recognition to electronic records and digital signatures.**

II. Objectives of the Act

1. To grant legal recognition to transactions carried out by means of EDI and other means of electronic communication commonly referred to as e-commerce in place of paper based methods of communication.
2. To grant legal recognition to Digital signature for authentication of any info. or matter which requires authentication under any law for time being in force.
3. To facilitate electronic filing of documents with Government Departments
4. To facilitate electronic storage of data.
5. Facilitate and give legal recognition to fund transfer between banks and financial institutions.
6. Legal recognition for keeping books of account by Bankers in electronic form.
7. To amend Indian penal code, Indian evidence Act, Banker's Book Evidence Act and RBI Act.

III. Scope of the Act and Definitions

It extends to the whole of India and unless otherwise provided in the Act, it applies to any offence or contravention there under committed outside India by any person.

The Act shall not apply to following:

1. A negotiable instrument (other than cheque) as defined in negotiable instrument Act, 1881.
2. Power of Attorney as defined in P-O-A Act, 1882.
3. A trust as defined in Indian Trusts Act, 1882.
4. A will as defined in Indian Succession Act, 1925 including any other testamentary disposition by whatever name called.
5. Any contract for sale or conveyance of immovable property or any interest in such property.
6. Any such class of documents or transactions as may be notified by Central Government in official Gazette.

Important Definitions

(i) Addressee
(ii) Afixing digital signature
(iii) A symmetric Crypto System
(iv) Digital signature
(v) Electronic form
(vi) Information
(vii) Intermediary
(viii) Key pair
(ix) Originator
(x) Prescribed
(xi) Private key
(xii) Public Key

IV Authentication of Electronic Records using Digital Signatures

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 electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tampering with the content of the electronic record will immediately invalidate the digital signature.

Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the public key corresponding to such private key.

This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature.

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

Refer Annexure 1

V Electronic Governance

It specifies the procedures to be followed for sending and receiving of electronic records.

S.	Title	Content
4	Legal recognition of electronic records	Where any law requires that any information or matter should be in the typewritten or printed form then such requirement shall be deemed to be satisfied if it is in an electronic form.
5	Legal recognition of Digital Signatures	Where any law requires that any information or matter should be authenticated by affixing the signature of any person, then such requirement shall be satisfied by means of Digital Signature affixed in such manner as may be specified by Central Government.
6	Foundation of Electronic Governance	It provides that filling of any form, application or other documents, creation, retention or preservation of records, issues or grant of any license or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form. The appropriate Government has the power to prescribe the manner and format of the electronic records and the method of payment of fee in that connection.
7	Documents to be retained in electronic form	It provides that the documents, records or information which has to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form provided the follow provided the following conditions are satisfied: (i) the information therein remains accessible so as to be usable subsequently. (ii) The electronic record is retained in its original format or in a format which accurately represents the information contained. (iii) The details which will facilitate the identification of origin, destination, dates and time of dispatch or

		receipt of such electronic record are available therein.
8	Publication of rules, regulations and notifications in the Electronic Gazette.	It provides that where any law requires publication of any rule, regulation, order, by-law, notification or any other matter in the official gazettethen the requirement shall be deemed to be satisfied if the same is published in an electronic form.
9	CG/SG can't insist doc. to be in electronic form.	It provides that the conditions stipulated in S. 6,7 & 8 shall not confer any right to insist that the document should be accepted in electronic format by CG/SG

Power of Central Government to make Rules (Sec 10)

CG, in respect of Digital Signature may prescribe by rules the following: -

(a) The type of digital signature.
(b) Manner and format in which it has to be a fixed
(c) Manner of procedure which facilities identification of person Afixing digital signatures.
(d) Control processes/procedures, to ensure adequate integrity, security and confidentiality.
(e) Any other matter.

VI Attribution receipts and dispatch of electronic records

11 – How Electronic Record attributed to person who originated it.
12 – Acknowledgement of Receipt.
13 – Time and Place of Dispatch and Receipt.

VII Secure Electronic records and secure digital signatures (Sec 14-16)

Security procedures need to be applied to digital signature for being treated as secure digital signature and CG is empowered to prescribe security procedures after taking into account factors like nature of transaction, level of sophistication availability and cost of alternative procedures etc.

VIII Regulation of Certifying Authorities

A Flat **F**rown **R**ed **L**ady **A**rrived **R**ear **R**oad **R**iver (17-25)

Section	Code	Contents
17	A	Appointment of Controller and other officers to regulate certifying authorities.
18	F	Functions of controller i.r.o. Certi. Authorities
19	F	Foreign Certifying Authorities (recognition of)
20	R	Controller acting as Repository of all Digital Signature Certificates. He maintains a computerized database of all public keys in such a manner that they are available to general public
21	L	Power of Controller to issue license to the Certifying Authority to issue Digital Signature Certificates.
22	A	Application for license.
23	R	Renewal of license
24	R	Rejection or Grant of license by controller on certain grounds

25	R	Revocation of license/suspension
27		Controller's power to delegate
30		Duties of Certifying Authorities Certain procedures to be followed i.r.o. Digital Signatures. (URSO) (a) make use of hardware, software, and procedures that are secure from intrusion and misuse; (b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions. (c) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured and (d) observe such other standards as may be specified by regulations. Every person employed by him complies with provisions of Act, Rules, Regulations, etc. Display of license at conspicuous place. Immediate surrender in case of suspension/revocation of license Disclose Digital Signature Certificate which contains public key corresponding. to Pvt. key used by certifying authority.

IX Digital Signature Certification

- Procedure for application
- Procedure for suspension
- Procedure for revocation

Certifying authority must be satisfied that applicant

1. Holds private key corresponding to public key
2. Private key is capable of creating digital signature
3. Public key can be used to verify digital signature affixed.

X Duties of subscribers (40-42)

1. On acceptance of Dig. Signature certificate, the subscriber shall generate key pair using secure system.
   Deemed to have accepted DSC when
   i. Publishes or authorises publication to one or more persons.
   ii. Otherwise demonstrates his approval to DSC
   By so accepting subscriber certifies to the public that –
   i. Holds private key corresponding to public key.
   ii. Info contained in certificate as well as material relevant to them are true.
2. Exercise reasonable care to retain control of his private key corresponding to public key. If it is compromised (endangered or exposed), immediately communicate the fact to certifying Authority, else subscriber shall be liable till he has informed.

XI Penalties and Adjudication

Sec 43 deals with penalty for damage to computer system, etc by any of different methods.

Sec 46 confers the power to adjudicate contravention under the Act to an officer not below the rank of Director to Government of India or equivalent officer of state. Such application shall be made by CG. Person so appointed shall have adequate exp. in field of Info. Technology and such legal and judicial experience as may be prescribed by CG.

Sec 47 provides that while deciding upon the quantum of compensation the adjudicating officer shall have due regards to (i) amt. of gain of unfair advantage. (ii) amt. of loss caused to any person (iii) nature of default.

XII Cyber Regulations Appellate Tribunal

It has appellate powers in respect of orders passed by adjudicating officer.

1. Establishment and composition (no, qualification, period of holding office)
2. Salaries and Allowances
3. Filling of Vacancy
4. Resignation and removal of presiding officer
5. Appeal to Cyber Regulations Appellate Tribunal
6. Powers and procedures of Appellate Tribunal
7. Appeal to High Court.
8. Compounding of Contravention
9. Recovery of Penalty

XIII Offences, Powers and Penalties (65-78)

The **H**ead **O**ffice **D**epartment **I**nternal **P**roblems **M**ade **C**hairman **F**ace **F**ar **I**ntensive **C**ircumstances **I**n **P**ublic.

Section	Code	Contents	Imprisonment Upto	Fine Upto
65	T	Tampering with computer source documents	3 years	Rs. 200,000
66	H	Hacking with computer system publishing of Info. which is 1st time subsequent	3 years	Rs. 200,000
67	O	Obscene in elec. Form	10 years	Rs. 200,000
68	D	Controller's directions to certifying Authorities or any employees failure to comply	3 years	Rs. 200,000
69	I	Intercept any info transmitted through any computer system/network		
70	P	Protected system. Any unauthorised access to such system	10 years	Not Defined
71	M	Penalty for Misrepresentation or suppressing any material fact	2 years	Rs. 100,000
72	C	Penalty for breach of confidentiality and privacy of el. records, books, info., etc without consent of person to whom they belong.	2 years	Rs. 100,000
73	F	Penalty for publishing False Digital Signature Certificate	2 years	Rs. 100,000
74	F	Fraudulent Publication	2 years	Rs. 100,000
75	I	Act also to apply for offences or contravention committed outside India if the act or conduct constituting the offence involves a computer, computer system or computer network located in India		
76	C	Confiscation of any computer, computer		

		system, floppies, CDs, tape drives or other accessories related thereto in contravention of any provisions of the Act, Rules, Regulations or Orders made.		
77	I	Penalty and Confiscation shall not interfere with other punishments provided under any law.		
78	P	Power to investigate offences by police officer not below rank of Dy. Superintendent of Police.		

XIV Network Service Providers Not Liable in Certain Cases.

Shall not be liable for any third party info or data made available by him, if he proves that the offence was committed without his knowledge/consent.

XV Miscellaneous

1. Power of Central Government to make Rules [Sec. 87]
2. Power of State Government to make Rules
3. Cyber Regulations Advisory Committee.
4. Power of the Controller to make Regulations.
   F – Foreign Certifying Authority
   L – Terms and Conditions under which Licence may be granted.
   O – Other Standards to be observed by certifying Authority
   D – Database
   S – Particulars to be submitted for issue for Digital Signature Certificate
   D – Disclosure by Certifying Authority U/s. 34
   C – Communicate compromise of pvt. key to the certifying Authority.
5. Power of Police officer/ other officers to enter, search, arrest etc.
6. Liability of companies [Sec. 85]

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
				10	What is a Digital Signature? How is it used? What are the duties of certifying authorities in regard to its usage?
				10	Explain briefly the scope of the Information Technology act, 2000 along with the relevant definitions that are used.
				4	Write Short Note : Digital Signature Certificate
				10	What are the powers of the Central Government to make rules, as given in Section 87, Chapter XIII of Information Technology act, 2000?
				2	Define: (i) Affixing digital signature
				2	Define: (ii) Asymmetric crypto system
				2	Define: (iii) Computer network
				2	Define: (iv) Private and Public keys
				2	Define: (v) Secure system

				5	State the objectives and scope of IT Act, 2000
				5	What are the duties of certifying authorities with respect to digital signature ?
				5	Describe the composition and powers of cyber regulatory appellate tribunal.
				10	Describe some of the powers of the cyber Apllelate Tribunal.
				5	Describe some of the powers of controller under section 89 to make regulations consistent with Information Technology Act, 2000.
				5	What are the duties of certifying authorities with respect to digital signature ?
				5	Objectives of Information Technology Act, 2000
				5	Discuss briefly the powers of Central Government under Section 87 to make rules in respect of Information Technology Act, 2000.
Nov-08	[1(c)]	10		5	State the liabilities of companies under section 85 of Information Technology Act, 2000.
Nov-08	[7(c)]	10		5	Powers of Cyber Appellate tribunal
Jun-09	[6(b)]	10		5	State the duties of the subscriber of a digital signature as specified in Section 40 to 42 of Chapter VIII of Information Technology Act, 2000.
Jun-09	[6(c)]	10		5	What are the conditions subject to which electronic record may be authenticated by means of affixing digital signature?

APPENDIX

What is a Digital Signature?

An introduction to Digital Signatures, by David Youd

Bob

(Bob's public key)

(Bob's private key)

Bob has been given two keys. One of Bob's keys is called a Public Key, the other is called a Private Key.

Bob's Co-workers:

Pat Doug Susan

Anyone can get Bob's Public Key, but Bob keeps his Private Key to himself

Bob's Public key is available to anyone who needs it, but he keeps his Private Key to himself. Keys are used to encrypt information. Encrypting information means "scrambling it up", so that only a person with the appropriate key can make it readable again. Either one of Bob's two keys can encrypt data, and the other key can decrypt that data.

Susan (shown below) can encrypt a message using Bob's Public Key. Bob uses his Private Key to decrypt the message. Any of Bob's coworkers might have access to the message Susan encrypted, but without Bob's Private Key, the data is worthless.

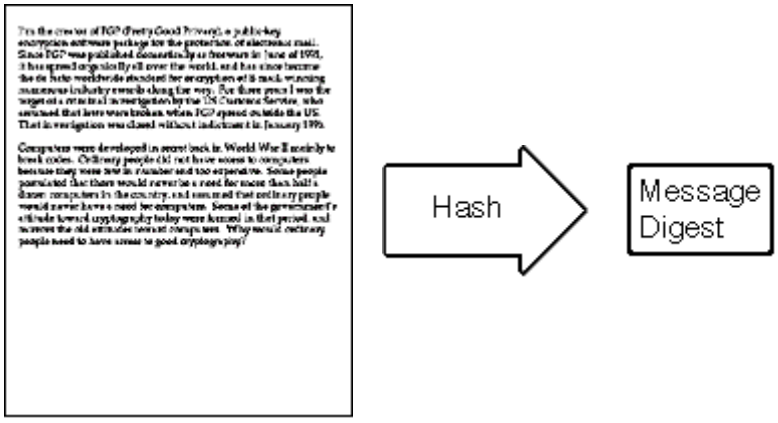
"Hey Bob, how about lunch at Taco Bell. I hear they have free refills!"

HNFmsEm6Un
BejhhyCGKOK
JUxhiygSBCEiC
0QYIh/Hn3xgiK
BcyLK1UcYiY
lxx2lCFHDC/A

HNFmsEm6Un
BejhhyCGKOK
JUxhiygSBCEiC
0QYIh/Hn3xgiK
BcyLK1UcYiY
lxx2lCFHDC/A

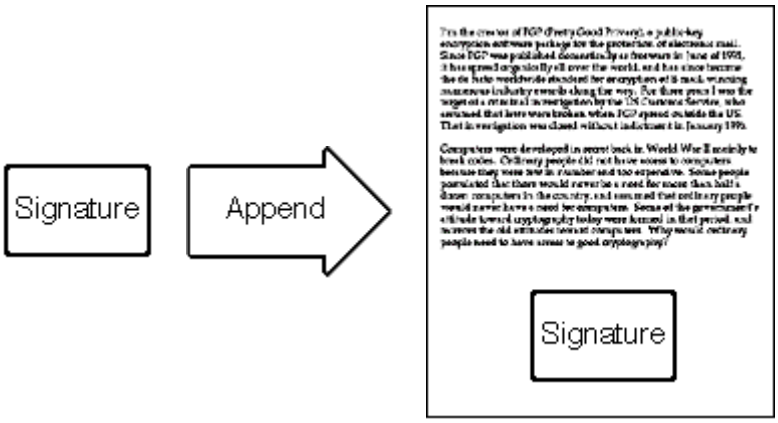
"Hey Bob, how about lunch at Taco Bell. I hear they have free refills!"

With his private key and the right software, Bob can put digital signatures on documents and other data. A digital signature is a "stamp" Bob places on the data which is unique to Bob, and is very difficult to forge. In addition, the signature assures that any changes made to the data that has been signed can not go undetected.

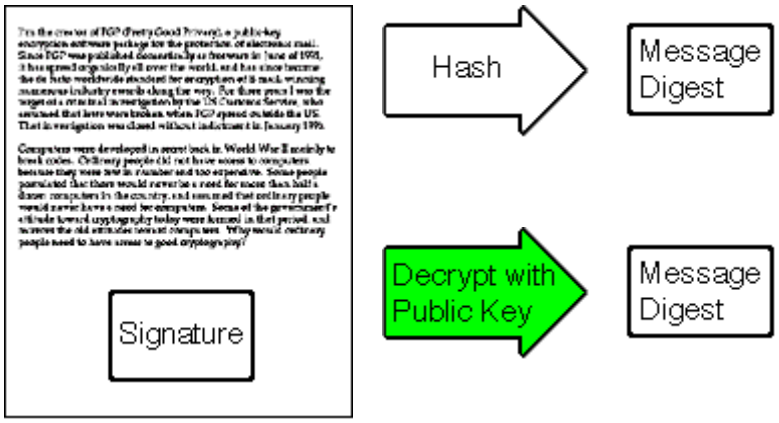


To sign a document, Bob's software will crunch down the data into just a few lines by a process called "hashing". These few lines are called a message digest. (It is not possible to change a message digest back into the original data from which it was created.)

Bob's software then encrypts the message digest with his private key. The result is the digital signature.



Finally, Bob's software appends the digital signature to document. All of the data that was hashed has been signed.



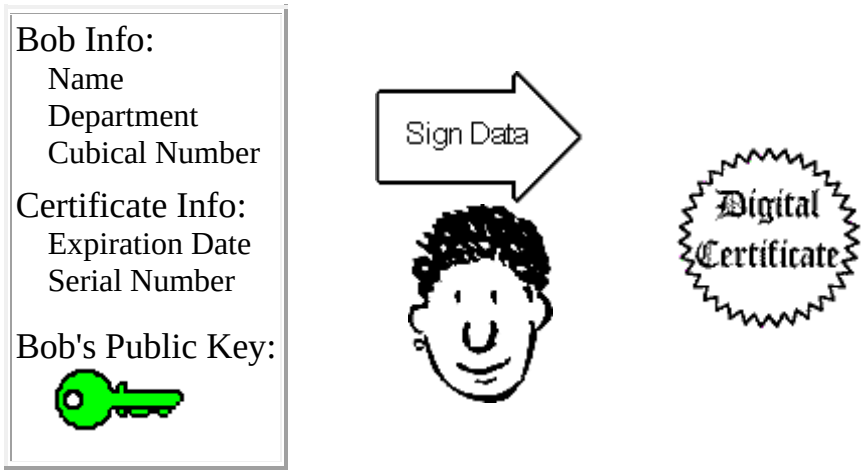
Bob now passes the document on to Pat.

First, Pat's software decrypts the signature (using Bob's public key) changing it back into a message digest. If this worked, then it proves that Bob signed the document, because only Bob has his private key. Pat's software then hashes the document data into a message digest. If the message digest is the same as the message digest created when the signature was decrypted, then Pat knows that the signed data has not been changed.

Plot complication...

Doug (our disgruntled employee) wishes to deceive Pat. Doug makes sure that Pat receives a signed message and a public key that appears to belong to Bob. Unbeknownst to Pat, Doug deceitfully sent a key pair he created using Bob's name. Short of receiving Bob's public key from him in person, how can Pat be sure that Bob's public key is authentic?

It just so happens that Susan works at the company's certificate authority center. Susan can create a digital certificate for Bob simply by signing Bob's public key as well as some information about Bob.

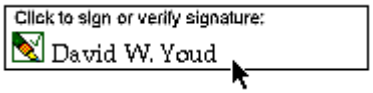


Now Bob's co-workers can check Bob's trusted certificate to make sure that his public key truly belongs to him. In fact, no one at Bob's company accepts a signature for which there does not exist

a certificate generated by Susan. This gives Susan the power to revoke signatures if private keys are compromised, or no longer needed. There are even more widely accepted certificate authorities that certify Susan.

Let's say that Bob sends a signed document to Pat. To verify the signature on the document, Pat's software first uses Susan's (the certificate authority's) public key to check the signature on Bob's certificate. Successful de-encryption of the certificate proves that Susan created it. After the certificate is de-encrypted, Pat's software can check if Bob is in good standing with the certificate authority and that all of the certificate information concerning Bob's identity has not been altered.

Pat's software then takes Bob's public key from the certificate and uses it to check Bob's signature. If Bob's public key de-encrypts the signature successfully, then Pat is assured that the signature was created using Bob's private key, for Susan has certified the matching public key. And of course, if the signature is valid, then we know that Doug didn't try to change the signed content.



Although these steps may sound complicated, they are all handled behind the scenes by Pat's user-friendly software. To verify a signature, Pat need only click on it.

Questions asked in Previous Examination - Chapterwise

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Module Ans Page No.	Marks	Question
Nov-08	[2(b)]	1		1.29 – 1.32	5	*What is Decision Support System?. Briefly explain three characteristics of Decision Support System.*
Nov-08	[2(c)]	1		1.42 – 1.43	5	*Explain Executive Information System(EIS). What purpose does it serve?*
Nov-08	[2(a)]	2		2.2 – 2.4	10	*State and briefly explain the six stages of System Development Life Cycle (SDLC).*
Jun-09	[2(a)]	2		2.11 – 2.13	10	*The top management of company has decided to develop a computer information system for its operations. Is it essential to conduct the feasibility study of system before implementing it? If answer is yes, state the reasons. Also discuss three different angles through which the feasibility study of the system is to be conducted.*
Nov-08	[7(a)]	2		2.52	5	*Advantages of Application Packages*
Nov-08	[7(d)]	2		2.81 – 2.82	5	*Information System Maintenance.*
Jun-09	[7(a)]	2		2.46	5	*System Manual*
Nov-08	[3(a)]	3		3.26 -3.28	10	*What do you understand by classification of information? Explain different classifications of information.*
Jun-09	[3(a)]	3		3.7 & 3.9	10	*A company is engaged in the stores taking data activities. Whenever, input data error occurs, the entire stock data is to be reprocessed at a cost of Rs. 50,000. The management has decided to introduce a data validation step that would reduce errors from 12% to 0.5% at a cost of Rs. 2,000 per stock taking period. The time taken for validation causes an additional cost of Rs. 200. (i) Evaluate the percentage of costbenefit effectiveness of the decision taken by the management and (ii) suggest preventive control measures to avoid errors for improvement.*
Nov-08	[3(c)]	3		3.22 – 3.23	5	*Briefly explain the formal change management policies, and procedures*

						to have control over system and program changes.
Nov-08	[7(b)]	3		3.14 – 3.15	5	*Key elements in System Development and Acquisition Control*
Jun-09	[2(b)]	3		3.8	5	"While reviewing a client's control system, an information system auditor will identify three components of internal control." State and briefly explain these three Components.
Jun-09	[3(b)]	3		3.21 – 3.22	5	*What are the issues that should be considered by a system auditor at post implementation review stage before preparing the audit report?*
Jun-09	[7(c)]	3		3.53	5	*Firewalls*
Nov-08	[3(b)]	4		4.1	5	*Explain software testing and state its objectives.*
Jun-09	[2(c)]	4		4.7 – 4.14	5	While testing a software, how will you involve the people working in the system Areas?
Jun-09	[7(d)]	4		4.8 – 4.9	5	*White Box Testing.*
Nov-08	[5(a)]	5		5.1 -5.2	10	*Explain the following terms with reference to Information Systems:* *(i) Risk* *(ii) Threat* *(iii) Vulnerability* *(iv) Exposure* *(v) Attack*
Nov-08	[5(b)]	5		5.3 – 5.4	5	*"There always exist some Common threats to the computerized environment." Explain these threats.*
Nov-08	[5(c)]	5		5.5 – 5.6	5	*What do you understand by "Risk Assessment"? Discuss the various areas that are to be explored to determine the risk.*
Jun-09	[3(c)]	5		5.4	5	*"Always, there exist some threats due to Cyber Crimes." Explain these threats.*
Jun-09	[4(b)]	5		5.10	5	*State and explain four commonly used techniques to assess and evaluate risks.*
Nov-08	[6(a)]	6		6.17 – 6.18	10	*What do you understand by the term Disaster? What procedural plan do you suggest for disaster recovery?*
Jun-09	[4(a)]	6		6.9 – 6.10	10	*As a system auditor, what control measures will you check to minimize threats, risks and exposures in a computerized system?*
Nov-08	[1(b)]	6		6.2	5	*Discuss the objectives and goals of Business Continuity planning.*

Nov-08	[6(b)]	6		6.3	5	*Describe the methodology of developing a Business Continuity Plan.*
Nov-08	[6(c)]	6		6.12	5	*Briefly explain the various types of system's back-up for the system and data together.*
Jun-09	[4(c)]	6		6.24	5	*What are the audit tools and techniques used by a system auditor to ensure that disaster recovery plan is in order? Briefly explain them.*
Nov-08	[1(a)]	7		7.2 – 7.5	10	*Briefly explain Enterprise Resource Planning(ERP) and describe five of its Characteristics.*
Jun-09	[1(a)]	7			5	Practice Problem
Jun-09	[1(b)]	7			5	Practice Problem
Jun-09	[1(c)]	7			5	Practice Problem
Jun-09	[1(d)]	7		7.14	5	*Suggest how to go about the implementation of ERP package.*
Nov-08	[4(a)]	8		8.13 -8.17	10	*What do you understand by Software Process Maturity? Discuss five levels of Software Process Maturity of Capability Maturity Model(CMM).*
Jun-09	[5(a)]	8		8.5	10	*When an organization is audited for the effective implementation of ISO 27001-(BS 7799: part II) - information Security management System, what are to be verified under.* *(i) Establishing Management Framework* *(ii) Implementation* *(iii) Documentation.*
Jun-09	[5(c)]	8		8.7	5	*Briefly explain Asset classification and Control under Information Security management Systems.*
Jun-09	[7(b)]	8			5	*Control Objectives for Information related Technology (COBIT)*
Jun-09	[6(a)]	9		9.16 – 9.17	10	*What purpose the information system audit policy will serve? Briefly describe the scope of information system audit.*
Nov-08	[4(b)]	9		9.8 -9.9	5	*Discuss various types of Information Security polices and their hierarchy.*
Nov-08	[4(c)]	9		9.22 – 9.23	5	*State and briefly explain the contents of a Standard information System Audit Report.*
Jun-09	[5(b)]	9		9.7 – 9.8	5	*The Information Security Policy of an organization has been defined and documented as given below:* *"Our organization is committed to ensure Information Security through*

						established goals and principles. Responsibilities for implementing every aspect of specific applicable proprietary and general principles, standards and compliance requirements have been defined. This is reviewed at least once a year for continued suitability with regard to cost and technological changes." Identify the salient components that have not been covered in the above policy.
Nov-08	[1(c)]	10		10.21	5	*State the liabilities of companies under section 85 of Information Technology Act, 2000.*
Nov-08	[7(c)]	10		10.15 – 10.16	5	*Powers of Cyber Appellate tibunal*
Jun-09	[6(b)]	10		10.12	5	*State the duties of the subscriber of a digital signature as specified in Section 40 to 42 of Chapter VIII of Information Technology Act, 2000.*
Jun-09	[6(c)]	10		10.6	5	*What are the conditions subject to which electronic record may be authenticated by means of affixing digital signature?*

Marks Allocation to Chapters

Sum of Marks	Year of Exam		
Chapter No.	Nov-08	Jun-09	Grand Total
1	10		10
2	20	15	35
3	20	25	45
4	5	10	15
5	20	10	30
6	25	15	40
7	10	20	30
8	10	20	30
9	10	15	25
10	10	10	20
Grand Total	140	140	280