

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

SYSTEM

1. Explain the general model of a system, in brief. Also explain the terms 'Subsystem' and 'Supra-system'.

INFORMATION

2. (a) What is information? Briefly discuss its attributes.
(b) Define an information system. What are the factors on which information requirements depend?

MIS

3. (a) What is MIS? Discuss characteristics of an effective MIS in brief.
(b) Explain the limitations of MIS.

DSS

4. (a) What is DSS? Explain the components of a DSS in brief.
(b) Discuss various examples of DSS in accounting.

SDLC

5. Define the following terms in brief:
(i) Systems Flow Chart (ii) Data Flow Diagram
(iii) CASE Tools (iv) Data Dictionary
(v) Technical Feasibility (vi) Economic Feasibility
6. What is Prototyping? Discuss its advantages and disadvantages in brief.
7. Write short notes on the following:
(i) Audit Trails (ii) Crypto systems
(iii) Preventive Controls (iv) Public Key Infrastructure

CONTROL OBJECTIVES

8. (a) Discuss Audit and Evaluation techniques for Physical access.
(b) Describe various types of firewalls in brief.
9. (a) What is data privacy? Explain the major techniques to address privacy protection for IT systems.
(b) Describe any three ways in which a hacker can hack the system.

10. Define the following terms in brief:

- (i) Static Testing (ii) Dynamic Testing
- (iii) Basic Path Testing (iv) Flow Graphs
- (v) Boundary Value Analysis

TESTING

- 11. Discuss the common factors in deciding 'when to stop testing'.
- 12. (a) What is Unit Testing? Discuss its benefits and limitations.
(b) Discuss the usage and objectives of Error Handling Testing.
- 13. Describe the advantages and disadvantages of Continuous Auditing techniques in brief.

RISK ASSESSMENT METHODOLOGIES

- 14. Define the following terms:
 - (i) Likelihood
 - (ii) Attack
 - (iii) Residual Risk
- 15. (a) Discuss various threats to the computerized environment.
(b) Explain the common risk mitigation techniques.

Business Continuity Planning and Disaster Recovery Planning

- 16. (a) Describe the methodology and phases of developing a business continuity plan?
(b) Explain the significance of a Business Impact Analysis (BIA) phase on developing a business continuity plan.
- 17. Explain briefly the following terms with respect to business continuity and disaster recovery planning.
 - (i) Emergency plan
 - (ii) Single points of failure analysis
 - (iii) First-party insurances
 - (iv) Cold-site, hot-site and warm-site

Enterprise Resource Planning

- 18. Identify the SAP module used to consolidate the financial statements including elimination of inter-company transactions.
- 19. Identify the risks and governance issues an organization faces while migrating to an integrated ERP system.

20. Discuss the various evaluating criteria to assess suitability of an ERP package on implementation.

Information Systems Auditing Standards, Guidelines, Best Practices

21. (a) "The effective way a service organization can communicate information about its controls is through the Service Auditor's Reports". Explain.
(b) State the benefits to a service organization from having a SAS 70 engagement performed.
22. (a) State and explain the standard which covers the aspect of controls for information assurance in general and is said to be a concise superset of COSO.
(b) Define COBIT Framework and briefly state its domains of control objectives.

IS security Policy, IS AUDIT Reporting

23. Describe the role of information systems audit policy in ensuring information security with respect to:
(i) Scope of IS Audit
(ii) Purpose of IS Audit
24. Briefly discuss the issues addressed under the following headings in an information systems (IS) audit Security policy document.
(i) Responsibility Allocation
(ii) Asset and security Classification
(iii) Access Control
(iv) Incident Handling

Information Technology Act, 2000

25. Explain with reference to "Information Technology Act, 2000":
(i) Penal Provisions
(ii) Electronic Governance

SUGGESTED ANSWERS/HINTS

1. General model of a system: The term system may be defined as a set of interrelated elements that operate collectively to accomplish some common purpose or goal. 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 systems 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 organizational processes (such as production, marketing, finance etc.) into goods and services. A computer based information system is also a system which is a collection of people, hardware, software, data and procedures that interact to provide timely information to authorized people who need it.

Systems can be abstract or physical. An abstract system is an 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. A physical system is a set of elements which operate together to accomplish an objective. A physical system may be further defined by examples given in the Table 1.1:

Physical system	Description
Circulatory system	The heart and blood vessels which move blood through the body.
Transportation system	The personnel, machines, and organizations which transport goods.
Weapons system	The equipment, procedures, and personnel which make it possible to use a weapon.
School system	The buildings, teachers, administrators, and textbooks that function together to provide instruction for students.
Computer system	The equipment which functions, together to accomplish computer processing
Accounting system	The records, rules, procedures, equipment, and personnel, which operate to record data, measure income, and prepare reports.

Table 1.1: Physical Systems

The examples illustrate that a system is not a randomly assembled set of elements; it consists of elements, which can be identified as belonging together because of a common purpose, goal, or objective. Physical systems are more than conceptual construct; they display activity or behavior. The parts interact to achieve an objective.

A general model of a physical system may be given in terms of input, process and output. This is, of course, very simplified because a system may have several inputs and outputs as shown below in the Fig. 1.1:

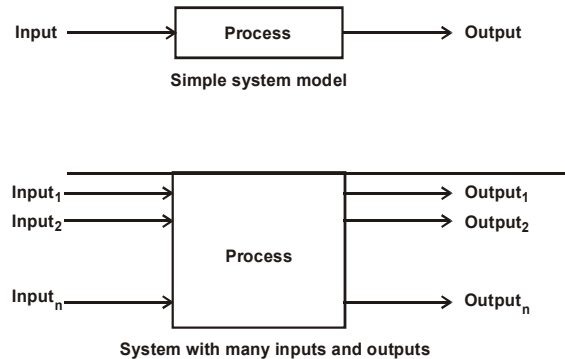


Fig. 1.1: Model of a system

Subsystem and Supra-system: 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. The interconnections and interactions between the subsystems are termed interfaces. Interfaces occur at the boundary and take the form of inputs and outputs.

A supra-system refers to the entity formed by a system and other equivalent systems with which it interacts. For example, an organization may be subdivided into numerous functional areas such as marketing, finance, manufacturing, research and development, and so on. Each of these functional areas can be viewed as a subsystem of a larger organizational system because each could be considered to be a system in and of itself. 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 organization are elements in the same supra-system within the organization.

2. (a) **Information:** Information is data that have been put into a meaningful and useful context. It has been defined by Davis and Olson as-"information is data that has been processed into a form that is meaningful to the recipient and is of real or perceived value in current or progressive decision". 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.

Attributes of Information: The important attributes of useful and effective information are as follows:

- **Availability:** This is a very important property of information. If information is not available at the time of need, it is useless. Data is organized in the form of facts and figures in databases and files from where various information is derived for useful purpose.
- **Purpose:** Information must have purposes at the time it is transmitted to a person or machine, otherwise it is simple data. Information communicated to people has a variety of purposes because of the variety of activities performed by them in business organizations. The basic purpose of information is to inform, evaluate, persuade, and organize.
- **Mode and format:** The modes of communicating information to humans are sensory (through sight, hear, taste, touch and smell) but in business they are either visual, verbal or in written form.

Format of information should be so designed that it assists in decision making, solving problems, initiating planning, controlling and searching. Therefore, all the statistical rules of compiling statistical tables and presenting information by means of diagram, graphs, curves, etc., should be considered and appropriate one followed. The reports should preferably be supplied on an exception basis to save the manager from an overload of information. Also, the data should only be classified into those categories, which have relevance to the problem at hand.

- **Decay:** Value of information usually decays with time and usage and so it should be refreshed from time to time. For example, we access the running score sheet of a cricket match through Internet sites and this score sheet is continually refreshed at a fixed interval or based on status of the state. Similarly, in highly fluctuating share market a broker is always interested about the latest information of a particular stock/s.
- **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 measure by the number of numeric characters transmitted per minute, such as sales reports from a district office. For machines the rate may be based on the number of bits of information per character (sign) per unit of time.
- **Frequency:** The frequency with which information is transmitted or received affects its value. Financial reports prepared weekly may show so little changes

that they have small value, whereas monthly reports may indicate changes big enough to show problems or trends.

Frequency has some relationship with the level of management also it should be related to an operational need. For example, at the level of foreman it should be on a daily or weekly basis but, at the management control level, it is usually on monthly basis.

- **Completeness:** The information should be as complete as possible. The classical ROI or Net Present Value (NPV) models just provide a point estimate and do not give any indication of the range within which these estimates may vary. Hartz's model for investment decisions provides information on mean, standard deviation and the shape of the distribution of ROI and NPV. With this complete information, the manager is in a much better position to decide whether or not to undertake the venture.
- **Reliability:** It is just not authenticity or correctness of information; rather technically it is a measure of failure or success of using information for decision-making. If information leads to correct decision on many occasions, we say the information is reliable.
- **Cost benefit analysis:** The benefits that are derived from the information must justify the cost incurred in procuring information. The cost factor is not difficult to establish. Using costing techniques, we shall have to find out the total as well as the marginal cost of each managerial statement but benefits are hard to quantify, i.e., they are usually intangibles. In fact, the assessment of such benefits is very subjective and its conversion into objective units of measurement is almost impossible. However, to resolve this problem, we can classify all the managerial statements into many categories with reference to the degree of importance attached, say, (a) absolutely essential statements, (b) necessary statement, (c) normal statements, (d) extra statements. The statements falling in the first category cannot be discontinued whatever be the cost of preparing them. The second category statements may have a high cost but may be discontinued only in very stringent circumstances. The normal statements may include those, which can be discontinued or replaced if their costs are too high. In the last category we may list those statements which may be prepared only if the benefits arising out of them are substantially higher than the costs involved.
- **Validity:** It measures the closeness of the information to the purpose which it purports to serve. For example, some productivity measure may not measure, for the given situation, what they are supposed to do e.g., the real rise or fall in productivity. The measure suiting the organization may have to be carefully selected or evolved.

- **Quality:** A study conducted by Adams a management expert, about management attitude towards information system, reveals that 75% of managers treated quantity investments as nearly identical in terms of job performance; yet given a choice, 90% of them preferred an improvement in quality of information over an increase in quantity. Quality refers to the correctness of information. Information is likely to be spoiled by personal bias. For example, an over-optimistic salesman may give rather too high estimates of the sales. This problem, however, can be circumvented by maintaining records of salesman's estimates and actual sales and deflating or inflating the estimates in the light of this. Errors may be the result of:
 - Incorrect data measurement and calculation methods.
 - Failure to follow processing procedure, and,
 - Loss or non-processing of data, etc.,

To get rid of the errors, internal controls should be developed and procedure for measurements prescribed. Information should, of course, be accurate otherwise it will not be useful; but accuracy should not be made a fetish, for example, the sales forecast for groups of products can well be rounded off to thousands of rupees.

- **Transparency:** If information does not reveal directly what we want to know for decision-making, it is not transparent. For example, total amount of advance does not give true picture of utilization of fund for decision about future course of action; rather deposit-advance ratio is perhaps more transparent information in this matter.
 - **Value of information:** It is defined as difference between the value of the change in decision behavior caused by the information and the cost of the information. In other words, given a set of possible decisions, a decision-maker may select one on basis of the information at hand. If new information causes a different decision to be made, the value of the new information is the difference in value between the outcome of the old decision and that of the new decision, less the cost of obtaining the information.
- (b) **Information System:** 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. Hence onwards we will focus our discussions only to computer-based information system. In modern business perspective the information system has far reaching effects for smooth and efficient operations.

Factors on which information requirements depend: The factors on which information requirements of executives depend are:

- **Operational function:** The grouping or clustering of several functional units on the basis of related activities into 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. Operational functions differ in respect of content and characteristics of information required by them.

Information requirement depends upon operational function. The information requirement of different operational functions varies not only in content but also in characteristics. 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 behavior, new product impact in the market etc.

The characteristics which must be possessed by 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.

- **Type of decision making:** Organizational decisions can be categorized follows:

- (i) **Programmed decisions:** Programmed decisions or structured decisions refer to decisions made on problems and situations by reference to a predetermined set of precedents, procedures, techniques and rules. These are well-structured in advance and are time-tested for their validity. As a problem or issue for decision-making emerges, the relevant pre-decided rule or procedure is applied to arrive at the decision. For example, in many organizations, there is a set procedure for receipt of materials, payment of bills, employment of clerical personnel, release of budgeted funds, and so on.

Programmed decisions are made with respect to familiar, routine, recurring problems which are amenable for structured solution by application of known and well-defined operating procedures and processes. Not much judgment and discretion is needed in finding solutions to such problems. It is a matter of identifying the problem and applying the rule. Decision making is thus simplified.

Organizations evolve a repertory of procedures, rules, processes and

techniques for handling routine and recurring situations and problems, on which managers have previous experience and familiarity. One characteristic of programmed decisions is that they tend to be consistent over situations and time. Also managers do not have to lose much sleep in brooding over them. However, programmed decisions do not always mean solutions to simple problems. Decision-making could be programmed even to complex problems-such as resource allocation problems for example-by means of sophisticated mathematical/statistical techniques.

- (ii) Non-programmed decisions or unstructured decisions: These 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, judgment and vision to tackling problems and situations, which arise infrequently and about which not much is known. There is no simple or single best way of making decisions on unstructured problems, which change their character from time to time, which is surrounded by uncertainty and enigma and which defy quick understanding. Solutions and decisions on them tend to be unique or unusual-for example, problems such as a sudden major change in government policy badly affecting a particular industry, the departure of a top level key executive, drastic decline in demand for a particular high profile product, competitive rivalry from a previously little known manufacturer etc. do not have ready-made solutions.

It is true that several decisions are neither completely programmed nor completely non-programmed but share the features of both.

- Level of management activity: Different levels of management activities in management planning and control hierarchy are as follows:
 - (i) Strategic Level or Top level: Strategic level management is concerned with developing of organizational mission, objectives and strategies. Decisions made at this level of organization to handle problems critical to the survival and successes of the organization are called strategic decisions. They have a vital impact on the direction and functioning of the organization-as for example decisions on plant location, introduction of new products, making major new fund-raising and investment operations, adoption of new technology, acquisition of outside enterprises and so on. Much analysis and judgment go into making strategic decisions.

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

- (ii) Tactical Level or middle level: Tactical level lies in middle of managerial hierarchy. At this level, managers plan, organize, 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. The other features of tactical decisions are: they are more specific and functional; they are made in a relatively closed setting; information for tactical decisions is more easily available and digestible; they are less surrounded by uncertainty and complexity; decision variables can be forecast and quantified without much difficulty and their impact is relatively localized and short-range. Tactical decisions are made with a strategic focus.

The distinction between strategic and operational decisions could be high-lighted by means of an example. Decisions on mobilization of military resources and efforts and on overall deployment of troops to win a war are strategic decisions. Decisions on winning a battle are tactical decisions.

As in the case of programmed and non-programmed decisions, the dividing line between strategic and tactical decision is thin. For example, product pricing is tactical decision in relation to the strategic decision of design and introduction of a new product in the market. But product pricing appears to be a strategic decision to down-line tactical decisions on dealer discounts.

- (iii) 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.
- 3. (a) 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'.

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

- **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. Such a system is not necessarily for top management only; it may also meet the information requirements of middle level or operating levels of management as well.
- **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. In brief, management should be responsible for setting system specifications and it must play a key role in the subsequent trade off decisions that occur in system development.
- **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.
- **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 utilize a minimum of data processing procedures and sub-systems to process the data and strive to minimize the number of output documents and reports produced by the system. This eliminates duplication in data collections and documents and procedures. It avoids duplication, also simplifies operations and produces an efficient information system. However, some duplication is necessary in order to insure effective information system.
- **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. It means that MIS designer should keep in view future objectives and requirements of firm's information in mind. The designer must avoid the possibility of system obsolescence before the system gets into operation.
- **Sub system concept:** Even though the information system is viewed as a single entity, it must be broken down into digestible sub-systems which can be implemented one at a time by developing a phasing plan. The breaking down of MIS into meaningful sub-systems sets the stage for this phasing plan.

- 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 organization 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.
- Computerized: 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.

(b) Limitations of MIS: The main limitations of MIS are as follows:

- The quality of the outputs of MIS is basically governed by the quantity of input and processes.
- MIS is not a substitute for effective management. It means that it cannot replace managerial judgment in making decisions in different functional areas. It is merely an important tool in the hands of executives for decision making and problem solving.
- MIS may not have requisite flexibility to quickly update itself with the changing needs of time, especially in fast changing and complex environment.
- MIS cannot provide tailor-made information packages suitable for the purpose of every type of decision made by executives.
- MIS takes into account mainly quantitative factors, thus it ignores the non-quantitative factors like morale and attitude of members of the organization, which have an important bearing on the decision making process of executives.
- MIS is less useful for making non-programmed decisions. Such types of decisions are not of the routine type and thus require information, which may not be available from existing MIS to executives.
- The effectiveness of MIS is reduced in organizations, where the culture of hoarding information and not sharing with other holds.
- MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.

4. (a) DSS: A decision support system (DSS) can be defined as a system that provides tools to managers to assist them in solving semi structured 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.

Components of a DSS: A decision support system has four basic components: the user, one or more databases, a planning language, and the model base, as given in Fig. 4.1:

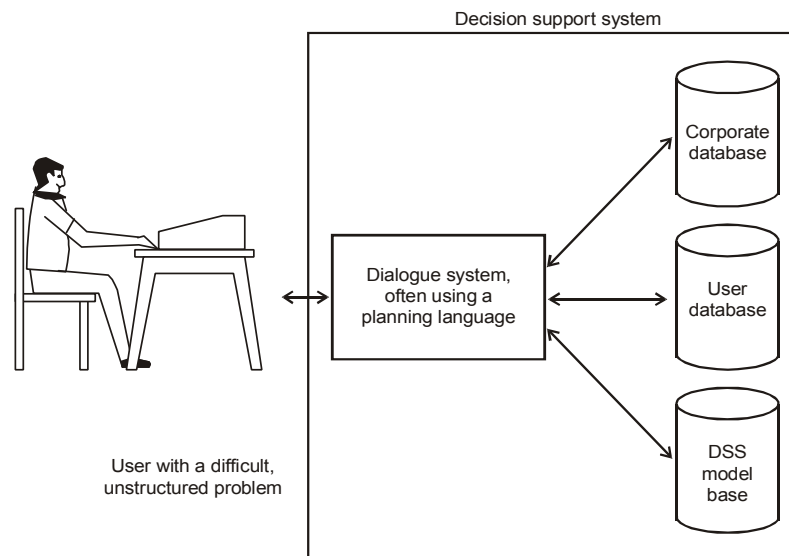


Fig. 4.1: The Components of a decision support system

- (i) The users: The user of a decision support system is usually a manager with an unstructured or semi-structured problem to solve. The manager may be at any level of authority in the organization (e.g., either top management or operating management). Typically, 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. Often, the planning language is nonprocedural, meaning that the user can concentrate on

what should be accomplished rather than on how the computer should perform each step.

- (ii) **Databases:** Decision support systems include one or more databases. These databases contain both routine and non-routine data from both internal and external sources. The data from external sources include data about the operating environment surrounding an organization – for example, data about economic conditions, market demand for the organization's goods or services, and industry competition.

Decision support system users may construct additional databases themselves. Some of the data may come from internal sources. An organization often generates this type of data in the normal course of operations – for example, data from the financial and managerial accounting systems such as account, transaction, and planning data. The database may also capture data from other subsystems such as marketing, production, and personnel. External data include assumptions about such variables as interest rates, vacancy rates, market prices, and levels of competition.

- (iii) **Planning Languages:** Two types of planning languages that are commonly used in decision support systems are: general –purpose planning languages and special-purpose planning languages. General-purpose planning languages allow users to perform many routine tasks – for example, retrieving various data from a database or performing statistical analyses. The languages in most electronic spreadsheets are good examples of general-purpose planning languages. These languages enable user to tackle a broad range of budgeting, forecasting, and other worksheet-oriented problems. Special-purpose planning languages are more limited in what they can do, but they usually do certain jobs better than the general-purpose planning languages. Some statistical languages, such as SAS, SPSS, and Minitab, are examples of special purpose planning languages.

- (iv) **Model base:** The planning language in a decision support system allows the user to maintain a dialogue with the model base. The model base is the 'brain' of the decision support system because it performs data manipulations and computations with the data provided to it by the user and the database. There are many types of model bases, but most of them are custom-developed models that do some types of mathematical functions-for example, cross tabulation, regression analysis, time series analysis, linear programming and financial computations. The analysis provided by the routines in the model base is the key to supporting the user's decision. The model base may dictate the type of data included in the database and the type of data provided by the user. Even where the quantitative analysis is simple, a system that requires users to concentrate on certain kinds of data can improve the effectiveness of decision making.

(b) Examples of Decision Support Systems in accounting: Decision support systems are widely used as part of an organization's AIS. The complexity and nature of decision support systems vary. Many are developed in-house using either a general type of decision support program or a spreadsheet program to solve specific problems. Below are several illustrations of these systems.

- **Cost Accounting system:** The health care industry is well known for its cost complexity. Managing costs in this industry requires controlling costs of supplies, expensive machinery, technology, and a variety of personnel. Cost accounting applications help health care organizations calculate product costs for individual procedures or services. Decision support systems can accumulate these product costs to calculate total costs per patient. Health care managers many combine cost accounting decision support systems with other applications, such as productivity systems. Combining these applications allows managers to measure the effectiveness of specific operating processes. One health care organization, for example, combines a variety of decision support system applications in productivity, cost accounting, case mix, and nursing staff scheduling 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, such as net present value and internal rate of return, with decision support tools that consider some benefits of new technology not captured in strict financial analysis. One decision support system designed to support decisions about investments in automated manufacturing technology is AutoMan, which allows decision makers to consider financial, nonfinancial, 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. One institution uses a computerized decision support system to generate monthly variance reports for division comptrollers. The system allows these comptrollers to graph, view, analyze, 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:** As mentioned earlier, some planning languages used in decision support systems are general purpose and therefore have the ability to analyze many different types of problems. In a

sense, these types of decision support systems are a decision-maker's tools. The user needs to input 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 then asks the user to compare decision variables with each other. For instance, the system might ask the user how important cash inflows are versus initial investment amount to a capital budgeting decision. The decision maker also makes judgments about which investment is best with respect to these cash flows and which requires the smallest initial investment. Expert Choice analyzes these judgments and presents the decision maker with the best alternative.

5. (i) **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 emphasize 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.
- (ii) **Data Flow Diagram:** A Data Flow Diagram (DFD) graphically describes the flow of data within an organization. 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. Each is represented on a DFD by one of the symbols.
- (iii) **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. CASE products are still relatively new and evolving. However numerous organizations have already reported great success with them.

- (iv) **Data Dictionary:** A data dictionary is a computer file that contains descriptive information about the data items in the files of a business information system. Thus, a data dictionary is a computer file about data. Each computer record of a data dictionary contains information about a single data item used in a business information system. This information may include:
- Codes describing the data item's length (in characters), data type (alphabetic, numeric, alphanumeric, etc.), and range (e.g., values from 1 to 99 for a department code)
 - The identity of the source document(s) used to create the data item.
 - The names of the computer files that store the data item.
 - The names of the computer programs that modify the data item.
 - The identity of the computer programs or individuals permitted to access the data item for the purpose of file maintenance, upkeep, or inquiry.
 - The identity of the computer programs or individuals not permitted to access the data item.
- (v) **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:
- Does the necessary technology exist to do what is suggested (and can it be acquired)?
 - Does the proposed equipment have the technical capacity to hold the data required to use the new system?
 - Will the proposed system provide adequate responses to inquiries, regardless of the number or location of users?
 - Can the system be expanded if developed?
 - Are there technical guarantees of accuracy, reliability, ease of access, and data security?
- (vi) **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:
- The cost of conducting a full systems investigation.
 - The cost of hardware and software for the class of applications being considered.

- The benefits in the form of reduced costs or fewer costly errors.
 - The cost if nothing changes (i.e., the proposed system is not developed)
 - The procedure employed is the traditional cost-benefit study.
6. Prototyping: The traditional approach sometimes may take years to analyze, design and implement a system. In order to avoid such delays, organizations 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. Decision supports semi-structured or unstructured management decision environment, are ideal for the experimentation and trial-and-error development associated with prototyping. Expert systems are other ideal candidates for prototyping approach because expert knowledge usually requires continual refinements. Prototyping can also be used in the development of transaction processing system. It is most commonly used during the system design stage, for instance, to develop the mock screen for input etc.

Advantages of Prototyping: The major advantages of this approach are as follows:

- 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.
- 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.

- 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: The major disadvantages of this approach are as follows:

- 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.
- 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.
- 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.

In spite of above listed limitations, to some extent, systems analysis and development has been greatly improved by the introduction of prototyping. Prototyping enables the user to take an active part in the systems design, with the analyst acting in an advisory role. Prototyping makes use of the expertise of both the user and the analyst, thus ensuring better analysis and design, and prototyping is a crucial tool in that process.

7. (i) **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 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.
- (ii) **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.

(iii) 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:

- A clear-cut understanding about the vulnerabilities of the asset
- Understanding probable threats
- 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. Some examples of preventive controls are as under:

- 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

(iv) 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 key. 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.

8. (a) 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. Information processing facility (Computer room, programmers area, tape library, printer stations and management offices) and any off-site storage facilities should also be included in this tour. Much of the testing of physical safeguards can be achieved by visually observation of the safeguards tested previously. Documents to assist with this effort include emergency evacuation procedures, inspection tags, fire suppression system test results and key lock logs. Testing should extend beyond the information processing. 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.

- (b) **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).

The four primary firewall types are given as follows:

- (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.
- (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.

Additionally, proxy servers provide another layer of access control by segregating the flow of Internet traffic to support additional authentication and logging capability, as well as content filtering. Web and e-mail proxy servers,

for example, are capable of filtering for potential malicious code and application-specific commands (see "Malicious Code"). They may implement anti-virus and anti-spam filtering, disallow connections to potentially malicious servers, and disallow the downloading of files in accordance with the institution's security policy.

- (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.

- 9. (a) **Data Privacy:** This 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.

Protecting data privacy in information systems : Increasingly, as heterogeneous information systems with different privacy rules are interconnected, technical control and logging mechanisms (policy appliances) will be required to reconcile, enforce and monitor privacy policy rules (and laws) as information is shared across systems and to ensure accountability for information use. There are several technologies to address privacy protection in enterprise IT systems. These falls into two categories: communication and enforcement.

- (i). **Policy Communication**

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

(ii). 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.

(b) The three ways in which a hacker can hack, are given as follows:

- 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.
- 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.
- 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, and Blade Runner. Simply we can turn the computer into an FTP server, without any authentication.

10. (i) 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 organization. These standards can be for

Coding, Integrating and Deployment. Reviews, Inspection's and Walkthrough's are static testing methodologies.

- (ii) **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.
 - (iii) **Basic 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.
 - (iv) **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.
 - (v) **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:
 - 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.
 - 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.
 - Apply guidelines 1 and 2 to the output.
 - If internal data structures have prescribed boundaries, a test case should be designed to exercise the data structure at its boundary.
11. **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.
- Practically, the decision of stopping testing is based on the level of the risk acceptable to the management. As testing is a never ending process we can never assume that 100 % testing has been done. The risk can be measured by Risk analysis but for small duration / low budget / low resources project, risk can be deduced by simply: -
 - ◆ Measuring Test Coverage.
 - ◆ Number of test cycles.
 - ◆ Number of high priority bugs.

12. (a) 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.

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.

Limitations: It is important to realize 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.

(b) Usage of Error Handling Testing: The main usages of this Testing technique are:

- 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 of Error Handling Testing: The objective of error handling testing is to determine that:

- Application system recognizes 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.

13. Continuous Auditing Technique: Continuous auditing enables auditors to shift their focus from the traditional 'transaction' audit to the 'system and operations' audit.

Advantages: 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.

Disadvantages: The following are some of the disadvantages and limitations 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.
14. (i) Likelihood: Likelihood of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event. The presence, tenacity and strengths of threats, as well as the effectiveness of safeguards must be considered while assessing the likelihood of the threat occurring.
- (ii) Attack: 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.
- (iii) Residual Risk: Any risk still remaining after the counter measures are analyzed and implemented is called Residual Risk. An organization'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 minimized, but it can seldom be eliminated. Residual risk must be kept at a minimal, acceptable level. As long as it is kept at an acceptable level, (i.e. the likelihood of the event occurring or the severity of the consequence is sufficiently reduced) the risk has been managed.
15. (a) Threats to the Computerized Environments: A few common threats to the computerized environment can be:
- Power Loss: Power failure can cause disruption of entire computing equipments since computing equipments depends on power supply.
 - Communication Failure: Failure of communication lines result in inability to transfer data which primarily travel over communication lines. Where the organization depends on public communication lines e.g. for e-banking communication failure present a significant threat that will have a direct impact on operations.

- **Disgruntled Employees:** A disgruntled employee presents a threat since, with access to sensitive information of the organization, he may cause intentional harm to the information processing facilities or sabotage operations.
 - **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 organization network being compromised with virus attacks.
 - **Malicious Code:** Malicious code such as viruses and worms which freely access the unprotected networks may affect organizational and business networks that use these unprotected networks.
 - **Abuse of access privileges by employees:** The security policy of the company authorizes employees based on their job responsibilities to access and execute select functions in critical applications.
 - **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.
 - **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 organization.
 - **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.
 - **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.
- (b) **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:
- **Insurance:** An organization 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. Under the Advanced Management Approach under Basel II norms, a bank will be allowed to recognize the risk mitigating

impact of insurance in the measures of operational risk used for regulatory minimum capital requirements. The recognition of insurance mitigation is limited to 20% of the total operational risk capital charge calculated under the AMA.

- Outsourcing: The organization 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. For example, outsourcing of telecommunication line viz. subscribing to a leased line does not transfer the risk. The organization remains liable for failure to provide service because of a failed telecommunication line. Consider the same example where the organization has outsourced supply and maintenance of a dedicated leased line communication channel with an agreement that states the minimum service level performance and a compensation clause in the event failure to provide the minimum service level results in to a loss. In this case, the organization has successfully mitigated the risk.
- 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 organization for any loss suffered by the customer and user consequent to the technological failure. Thus a bank may state that services at ATM are subject to availability of service there and customers need to recognize that such availability cannot be presumed before claiming the service. The delivery of service is conditional upon the system functionality. Whereas the service is guaranteed if the customer visits the bank premises within the banking hours.

It must be recognized that the organization 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.

16. (a) Methodology and phases of 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 organization. The methodology emphasizes on the following:
- Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
 - Obtaining commitment from appropriate management to support and participate in the effort;

- Defining recovery requirements from the perspective of business functions;
- Documenting the impact of an extended loss to operations and key business functions;
- Focusing appropriately on disaster prevention and impact minimisation, as well as orderly recovery;
- Selecting business continuity teams that ensure the proper balance required for plan development;
- Developing a business continuity plan that is understandable, easy to use and maintain; and
- 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.

The eight phases are:

- (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
- (b) Significance of a Business Impact Analysis (BIA) phase on developing a business continuity plan: The first step in a sensible business continuity process is to consider the potential impact of each type of problem. 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.

The tasks to be undertaken in this phase are enumerated as under:

- 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.
- Identify critical business processes.
- Identify and quantify threats/ risks to critical business processes both in terms of outage and financial impact.
- Identify dependencies and interdependencies of critical business processes and the order in which they must be restored.
- Determine the maximum allowable downtime for each business process.
- Identify the type and the quantity of resources required for recovery e.g. tables chairs, faxes, photocopies, safes, desktops, printers, etc.
- 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.

17. (i) Emergency plan: The Plan Development phase of the business continuity planning methodology 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)

Recovery plan components are defined and plans are documented as Emergency plan, Backup-Plan and Recovery Plan. The organization's recovery strategy needs

to be developed for the recovery of the core business processes. In the event of a disaster, it is survival and not business as usual.

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. If an organization undertakes a comprehensive security review program, the threat identification and exposure analysis phases involve identifying those situations that require the emergency plan to be invoked.

When the situation that evokes the plan has been identified the four aspects of the emergency plan must be articulated. First, the plan must show who is to be notified immediately when the disaster occurs - management, police, fire department, medicos, and so on. Second, the plan must show actions to be undertaken, such as shutdown of equipment, removal of files, and termination of power. Third, any evacuation procedures required must be specified. Fourth, 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.

- (ii) Single points of failure analysis: The objective is to identify any single point of failure within the organization'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 organization'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. Organizations 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 organization that may lead to disaster being declared. To ensure single point failures are identified within the organizations 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

- (iii) First-party insurances: The purpose of insurance is to spread the economic cost and the risk of loss from an individual or business to a large number of people. This is accomplished through the use of an insurance policy. Insurance is generally divided into two general classes based upon whether the insured is the injured party. Lawyers call these two divisions first-party and third-party insurance. First-party insurance identifies claims by the policyholder against their own insurance. The most common form of first-party insurance is property damage.

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.

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.

- (iv) Cold-site, hot-site and warm-site: A key element in minimising the threat of a disaster occurring in an organisation is "hardening" the organisation's infrastructure from potential sources of risk one of it is alternate processing facility arrangements. A security administrator should consider the following backup options:
- 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.
 - 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.

- 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 warm site might contain selected peripheral equipment plus a small mainframe with sufficient power to handle critical applications in the short run.
18. An 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 allows controlling 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. 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.
- 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.
- 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.
- 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 .
19. Risks and governance issues an organization faces while migrating to an integrated ERP system: 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-to-day 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.

The governance issues in an ERP environment are:

- **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.
20. **Evaluation of various ERP packages:** ERP implementation in an organization 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. Implementation of ERP is a risky effort since it involves considerable amount of time, efforts and valuable resources. Even with all these, the success of an implementation is not guaranteed.

The ability of the ERP package to manage and support dynamically changing business processes is a critical requirement for the organization and therefore the package should be expandable and adaptable to meet these changes. The ERP implementation methodology involves several steps of which one is evaluating the various available ERP packages to assess suitability.

Evaluation of ERP packages are done based on the following criteria:

- **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.
- **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, sales and distribution, 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.

- **Integrated:** It should overcome the limitations of traditional hierarchical and function oriented structures. Functions like sales and materials planning, production planning, warehouse management, financial accounting, and human resources management should be integrated into a workflow 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.
- **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 geographies, currencies and country specific business rules.
- **Best business practices:** The software should enable integration of all business operation in an overall system for planning, controlling and monitoring and offer a choice of multiple ready-made business processes including best business practices that reflect the experiences, suggestions and requirements of leading companies across industries. In other words, it should intrinsically have a rich wealth of business and organizational knowledge base.
- **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.

Other factors to be considered are:

- Global presence of 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.

21. (a) **Service Auditor's Reports:** 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.

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 are 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.

- (b) **Benefits to a service organization from having a SAS 70 engagements performed:** 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.

In an audit of a user organization's financial statements, the user auditor obtains an understanding of the entity's internal control sufficient to plan the audit. Identifying and evaluating relevant controls is generally an important step in the user auditor's overall approach. If a service organization provides transaction processing or other data processing services to the user organization, the user auditor may be required to gain an understanding of the controls at 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).

Without a current Service Auditor's Report, a service organization may have to entertain multiple audit requests from its customers and their respective auditors. Multiple visits from user auditors can place a strain on the service organization's resources. A Service Auditor's Report ensures that all user organizations and their auditors have access to the same information and in many cases this will satisfy the user auditor's requirements.

SAS 70 engagements are generally performed by control oriented professionals who have experience in accounting, auditing, and information security. A SAS 70 engagement allows a service organization to have its control policies and procedures evaluated and tested (in the case of a Type II engagement) by an independent party. Very often this process results in the identification of opportunities for improvements in many operational areas.

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. The user organization receives a detailed description of the service organization's controls and an independent assessment of whether the controls were placed in operation, suitably designed, and operating effectively (in the case of a Type II report).

22. (a) COSO Internal Control Integrated Framework states that internal control is a process established by an entity's board of directors, management, and other personnel designed to provide reasonable assurance regarding the achievement of stated objectives. Its control objectives focus on effectiveness, efficiency of operations, reliable financial reporting, and compliance with laws and regulations.

CoCo is built on the concepts in the COSO document and is said to be a concise superset of COSO.

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. It is concerned with control in general as “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.” 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. It uses three categories of objectives: •effectiveness and efficiency of operations •reliability of financial reporting •compliance with applicable laws and regulations CoCo states that the “essence of control is purpose, capability, commitment, and monitoring and learning,” These form a cycle that continues endlessly if an organization is to continue to improve. Four important concepts about “control” are as follows:

- Control is affected by people throughout the organization, including the board of directors (or its equivalent), management and all other staff.
- 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.
- Organizations are constantly interacting and adapting.
- Control can be expected to provide only reasonable assurance, not absolute assurance.

- (b) COBIT Framework: 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

The COBIT Framework consists of high-level control objectives and an overall structure for their classification. There are the activities and tasks needed to achieve a measurable result. Activities have a life-cycle concept while tasks are more discrete. The life-cycle concept has typical control requirements different from discrete activities. Processes are then defined one layer up as a series of joined activities or tasks with natural (control) breaks. At the highest level, processes are naturally grouped together into domains. Their natural grouping is often confirmed as responsibility domains in an organizational structure and is in line with the management cycle or life cycle applicable to IT processes. The four broad domains are identified: planning and organization, acquisition and implementation, delivery and support, and monitoring.

The high level control objectives for the Planning and Organization domain.

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

Table 22.1: Plan and Organize

The high level control objectives for the Acquisition and Implementation domain.

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 Accredited Solutions and Changes

Table 22.2: Acquire and Implement

The high level control objectives for the Delivery and Support domain.

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

Table 22.3: Deliver and Support

The high level control objectives for the Monitoring domain.

ME1	Monitor and Evaluate IT Processes
ME2	Monitor and Evaluate Internal Control
ME3	Ensure Regulatory Compliance
ME4	Provide IT Governance

Table 22.4: Monitor and Evaluate

23. (i) Scope of IS Audit: The IS audit policy is to provide the guidelines to the audit team to conduct an audit on IT based infrastructure system in ensuring information security are:

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, organizing, 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 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.

- (ii) Purpose of IS Audit: 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.

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.

24. 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 organization.

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, maximized sharing versus least privilege, separation of duties, who controls and who owns the information, and authority issues.

- (i) 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.

- All new network communications links must be approved.
- A contact list of organizations 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

(ii) Asset 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 organizations must be controlled. Organizations 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 labeling and handling must be agreed and put into practice.
- Classified waste must be disposed of appropriately and securely.

(iii) Access Control

- Access controls must be in place to prevent unauthorized 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 unauthorized 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.

(iv) 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 analyzed to identify weaknesses or trends.
- Procedures for the collection of evidence relating to security incidents should be standardized. 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

25. (i) Penal Provisions: Chapter IX contains sections 43 to 47. It provides for awarding compensation or damages for certain types of computer frauds. It also provides for the appointment of Adjudication Officer for holding an inquiry in relation to certain computer crimes and for awarding compensation. Sections 43 to 45 deal with different nature of penalties.

Penalty for damage to computer, computer system or network: Section 43 deals with penalty for damage to computer, computer system, etc by any of the following methods:

- (a) securing access to the computer, computer system or computer network;
- (b) downloading or extracting any data, computer database or information from such computer system or those stored in any removable storage medium;
- (c) introducing any computer contaminant or computer virus into any computer, computer system or network;
- (d) damaging any computer, computer system or network or any computer data, database or programme;
- (e) disrupting any computer, computer system or network;
- (f) denying access to any person authorized to access any computer, computer system or network;
- (g) providing assistance to any person to access any computer, computer system or network in contravention of any provisions of this Act or its Rules;
- (h) charging the services availed of by one person to the account of another person by tampering with or manipulation any computer, computer system or network.

Explanation.- For the purposes of this section,-

- (i) "computer contaminant" means any set of computer instructions that are designed:
 - (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
 - (b) by any means to disrupt the normal operation of the computer, computer system, or computer network;
- (ii) "computer database" means a representation or information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

- (iii) “computer virus” means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;
- (iv) “damage” means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

Section 44 states that if any person who is required under this Act or any rules or regulations made there under to:

- (a) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;
- (b) file any return or furnish any information, books or other documents within the time specified in the regulations fails to file, return or furnish the same within the time specified in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;
- (c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

Section 45 provides for residuary penalty. Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

Section 46 confers the power to adjudicate contravention under the Act to an officer not below than the rank of a Director to the Government of India or an equivalent officer of a State Government. Such appointment shall be made by the Central Government. In order to be eligible for appointment as an adjudicating officer, a person must possess adequate experience in the field of Information Technology and such legal or judicial experience as may be prescribed by the Central Government. The adjudicating officer so appointed shall be responsible for holding an inquiry in the prescribed manner after giving reasonable opportunity of being heard and thereafter, imposing penalty where required.

Section 47 provides that while deciding upon the quantum of compensation, the adjudicating officer shall have due regard to the amount of gain of unfair advantage and the amount of loss caused to any person as well as the respective nature of the default.

- (ii) Electronic Governance: It specifies the procedures to be followed for sending and receiving of electronic records and the time and the place of the dispatch and receipt.

Section 4 provides for “legal recognition of electronic records”. It provides that 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.

Section 5 provides for 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 if it is authenticated by means of Digital Signatures affixed in such manner as may be prescribed by the Central Government.

For the purposes of this section, “signed”, with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression “signature” shall be construed accordingly.

Section 6 lays down the foundation of Electronic Governance. It provides that the filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any licence or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form. The appropriate Government office has the power to prescribe the manner and format of the electronic records and the method of payment of fee in that connection.

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

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

This section does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

Moreover, this section does not apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

Section 8 provides for the publication of rules, regulations and notifications in the Electronic Gazette. It provides that where any law requires the publication of any rule, regulation, order, bye-law, notification or any other matter in the Official Gazette, then such requirement shall be deemed to be satisfied if the same is published in an electronic form. It also provides where the Official Gazette is published both in the printed as well as in the electronic form, the date of publication shall be the date of publication of the Official Gazette which was first published in any form.