

INFORMATION SYSTEMS CONCEPTS

BASIC CONCEPTS

1. **System:** The term system may be defined as a set of interrelated elements that operate collectively to accomplish some common purpose or goal.
2. **Nature and types of System:** These may be broadly divided in two main categories: Manual and Automated systems.
 - 2.1 **Computer based business system:** Finance and Accounting, Marketing and Sales, Production or manufacturing, Inventory/ Stores management, Human Resource management.
 - 2.2 **Open System and Closed System:** A system which interacts freely with the environment by taking input and returning output is termed as an open system. On the other hand, the system which neither interacts with the environment nor changes with the change in environment is termed as a closed system.
 - 2.3 **Deterministic and Probabilistic System:** A deterministic system operates in a predictable manner. The probabilistic system can be defined in terms of probable behavior, but a certain degree of error is always attached to the prediction of '*what the system will do*'.
3. **Information:** Information is data that have been put into a meaningful and useful context.
 - 3.1 **Attributes of Information:** Availability, Purpose, Mode and Format, Decay, Rate, Frequency, Completeness, Reliability, Cost-benefit Analysis, Validity, Quality, Transparency, and Value of Information.
4. **Information System and its Role in Management**
 - 4.1 **Factors on which information requirements depend:** Operational Function, Types of Decision making, Level of management activity
 - 4.2 **Information Systems at different levels of management**
 - 4.3 **Types of Information:** Internal and external information

5. Types of Information Systems at different levels

5.1 Transaction Processing System (TPS): TPS at the lowest level of management is an information system that manipulates data from business transactions.

5.2 Management Information System (MIS)

5.2.1 Characteristics of an effective MIS: Management oriented, Management Directed, Integrated, Common Data Flows, Heavy Planning element, Sub System Concept, Common Database, and Computerized

5.2.2 Pre-requisites of an effective MIS: Database, Qualified System and management staff, support to top management, Control and Maintenance of MIS, Evaluation of MIS

5.2.3 Effect of using computer for MIS: Speed of processing and retrieval of data increases, Scope of use of information system has expanded, Scope of analysis widened, Complexity of system design and operation increased, Integrates the working of different information sub-system, more comprehensive information, and increases the effectiveness of Information system

5.3 Decision Support System (DSS)

5.3.1 Characteristics: Semi-structured and Unstructured Decisions, Ability to adopt the changing needs, and Ease of learning and use

5.3.2 Components of a DSS: Users, Databases, Planning Languages, Model Base

5.3.3 Tools for DSS: Database Languages, Model based decision support software, Tools for Statistics and Data Manipulation, and Display based decision support software

5.3.4 Examples of DSS in Accounting: Cost Accounting System, Capital Budgeting System, Budget Variance Analysis System, General Decision Support System

5.4 Executive Information System (EIS)

5.4.1 Executive Roles and Decision Making: Strategic Planning, Tactical Planning, Fire Fighting, and Control

5.4.2 Executive Decision Making Environment: Three main sources of information: *Environmental*, *Competitive*, and *Internal*.

5.4.4 Commercially available EIS Products: Commander EIS, Command Center, Executive Edge, and Express EIS.

Question 1

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

Answer

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 following Table:

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: 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.:

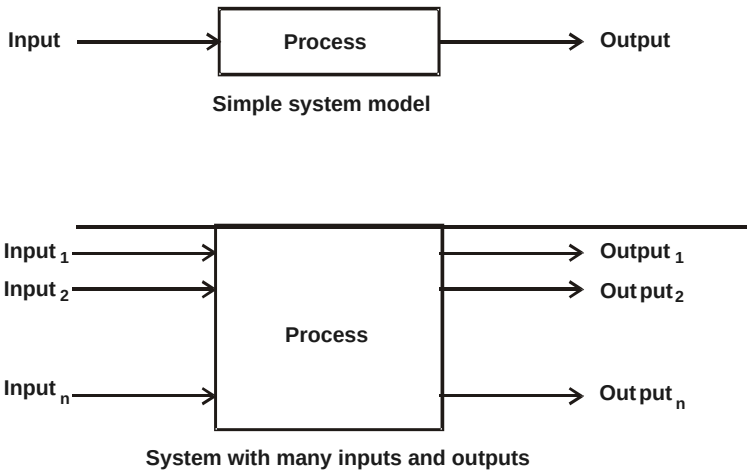


Fig.: Model of a system

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 sub-system being delineated by its boundaries. The interconnections and interactions between the subsystems are termed interfaces. Interfaces occur at the boundary and take the form of inputs and outputs.

A supra-system refers to the entity formed by a system and other equivalent systems with which it interacts. 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.

Question 2

Define the following terms briefly:

- (a) Open system
- (b) Closed system
- (c) Deterministic System
- (d) Probabilistic system
- (e) Transaction Processing System (TPS)
- (f) Decision Support System (DSS)
- (g) Executive Information System (EIS)

Answer

- (a) **Open System:** A system that interacts freely with its environment by taking input and returning output is termed as an open system.
- (b) **Closed System:** A system that does not interact with the environment or does not change with the changes in environment is termed as a closed system.
- (c) **Deterministic System:** A deterministic system operates in a predictable manner. The interaction among the parts is known with certainty. If one has a description of the systems at a given point in time plus a description of its operation, the next state of the system may be given exactly, without error.
- (d) **Probabilistic System:** It can be described in terms of probable behaviour, but a certain degree of error is always attached to the prediction of what the system will do.
- (e) **Transaction Processing System (TPS):** It manipulates data from business transactions. Any business activity such as sales, purchase, production, delivery, payments or receipts involves transaction and these transactions are to be organized and manipulated to generate various information products for external use.
- (f) **Decision Support System (DSS):** It is a system that provides tools to managers to assist them in solving semi-structured and unstructured problems in their own, somewhat personalized way. That is, a DSS supports the human decision-making process, rather than providing a means to replace it.
- (g) **Executive Information Systems (EIS):** It is a tool that provides direct on-line access to relevant information in a useful and navigable format. Relevant information

Information Systems Control and Audit

is timely, accurate and actionable information about the aspects of a business that are of particular interest to the senior manager.

Question 3

Identify and justify the type of each one of the following systems based on how they perform within an environment and/or certainty/ uncertainty:

- (i) Marketing system
- (ii) Communication system
- (iii) Manufacturing system
- (iv) Pricing system
- (v) Hardware-Software system.

Answer

System	System Type	Justification
(i) Marketing system	<i>Open System</i>	The marketing system plays a pivotal role in the running of a business in the competitive environment. The objective of the system is to maximize customer satisfaction by providing a free interactive environment. The system takes input/feedbacks and facilitates the outcomes as products of the company and to create new customers.
(ii) Communication System	<i>Open System</i>	The communication system in an organization is a point of contact to balance the external influence and render its services to the customers. The system interacts freely with its environment by taking input and returning output.
(iii) Manufacturing System	<i>Closed System</i>	This system is in place to meet a particular objective. It neither interacts with the environment nor changes with the change in the environment. A manufacturing unit is completely isolated from its environment for its operation.
(iv) Pricing System	<i>Probabilistic and Open System</i>	The system has a probable behavior and interacts freely with its environment by taking inputs and returning outputs. The pricing system is a dynamic one which

		influences the form of profit and goodwill of an organization.
(v) Hardware-Software System	<i>Closed Deterministic System</i>	The interaction among the various parts of the system is known with certainty and it does not interact with the environment and does not change with the change in the environment. Here the requirements of the hardware and software inventory are known with certainty. The operational state of these systems is predictable.

Question 4

Explain the limitations of MIS.

Answer

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.

Information Systems Control and Audit

Question 5

Differentiate between open and closed systems.

Answer

A Closed System is self-contained and does not interact or make exchange across its boundaries with its environment. Closed systems do not get the feedback they need from the external environment and tend to deteriorate. A Closed Systems one that has only controlled and well defined input and output. Participant in a closed system become closed to external feed back without fully being aware of it. Some of the examples of closed systems are manufacturing systems, computer programs etc.

Open System actively interact with other systems and establish exchange relationship. They exchange information, material or energy with the environment including random and undefined inputs. Open systems tend to have form and structure to allow them to adapt to changes in their external environment for survival and growth. Organizations are considered to be relatively open systems.

Question 6

What are the characteristics of a business system?

Answer

Characteristics of a business system: A business system is an organized grouping of interdependent functioning units or components, linked together according to a plan, to achieve a specific objective. All systems have some common characteristics. These are as follows:

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

Question 7

Explain, in brief, the human resource management system.

Answer

Human resource management system: Human resources are the most valuable asset for an organization. Utilization of these resources in most effective and efficient way is an important function for any enterprise. Human resource management system aims to achieve this goal. Skill database maintained in HRM system, with details of qualifications, training, experience, interests etc., helps management for allocating manpower to right activity at the time of need or starting a new project. This system also keeps track of employees' output or efficiency. Administrative functions like keeping track of leave records or handling other related functions are also included in HRM system. An HRM system may have the following modules.

- Personal administration
- Recruitment management
- Travel management
- Benefit administration
- Salary administration
- Promotion management.

An ideal HR development emphasizes on optimal utilization of human resources by introducing a consistent and coherent policy aiming at promoting commitment to the enterprise. The HRM system assists to achieve this goal.

Question 8

What is information? Briefly discuss its attributes.

Answer

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

Information Systems Control and Audit

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

Information Systems Control and Audit

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.

Question 9

Define an information system. What are the factors on which information requirements depend?

Answer

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

Information Systems Control and Audit

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 highlighted 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.

Question 10

Explain different levels of management activities in management planning and control hierarchy.

Answer

Different Levels of Management activities: Management at different levels take decisions matching to their position or hierarchy in the organization and different types of information systems are designed and developed for them, i.e. an information system for a departmental manager will be characteristically different from one designed for a corporate manager.

Information Systems Control and Audit

If we consider an organization having a pyramidal management structure with the corporate level managers at the top and operational managers at the bottom we will observe that typical categories of data are manipulated at different levels.

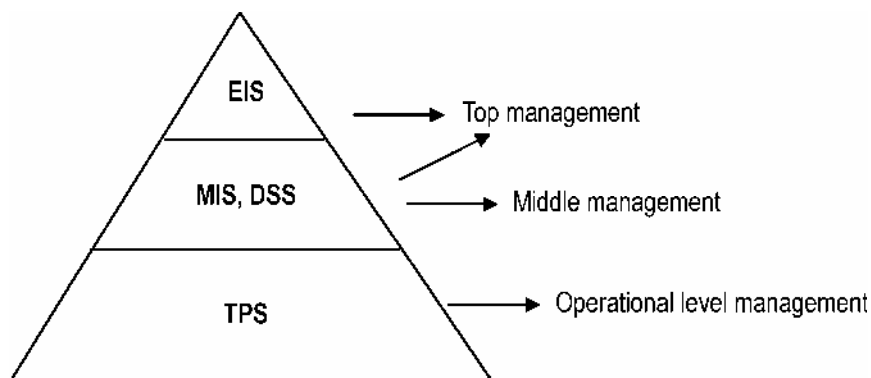


Fig.: Different Levels of Management

The above figure exhibits data available at different functional areas of an organization for management. At the lowest level that is managed by operational level managers (like supervisor, section in-charge), all types of inputs available from various sources are collected. The routine office work, like maintaining inward register and public interaction are mostly done at this level. However, no decision-making process is carried out at this level.

At the middle level of management the decision making – process starts. Inputs from different internal and external information sources are collected (normally passé from operational level managers) and processed for strategic decisions. Middle level managers who are expected to contribute significantly towards development of the organization are the key personnel to carry out the processing activities of the strategic data. They use various tools of analysis and typical software products to report to the higher level with options and possible effects. This job is very critical and important as well because tactical decisions by the top management are dependent on the information passed from middle management.

Question 11

System analysts develop various categories of information systems to meet a variety of business needs. Discuss any three such systems briefly.

Answer

Systems analysts develop the following types of information systems to meet a variety of business needs:

- (i) Transaction processing systems

- (ii) Management information systems
- (iii) Decision support systems
- (iv) Executive information systems
- (v) Expert systems.

Three of the above categories are discussed largely below:

- (i) **Transaction Processing Systems:** These systems are aimed at expediting and improving the routine business activities that all organizations engage. Standard operating procedures, which facilitate handling of transactions, are often embedded in computer programs that control the entry of data, processing of details, search and presentation of data and information. Transaction processing systems if properly computerized, provide speed and accuracy and can be programmed to follow routines without any variance.
- (ii) **Management Information Systems (MIS):** Transaction processing systems are operations oriented. In contrast, MIS assist managers in decision making and problem solving. They use results produced by the transaction processing systems, but they may also use other information. In any organization, decisions must be made on many issues that recur regularly and require a certain amount of information. Because the decision making process is well understood, the manager can identify the information that will be needed for the purpose. In turn, the information systems can be developed so that reports are prepared regularly to support these recurring decisions.
- (iii) **Decision Support Systems:** Not all decisions are of a recurring nature. Some occur only once or recur infrequently. Decision support systems (DSS) are aimed at assisting managers who are faced with unique (non-recurring) decision problems. In well structured situations, it is possible to identify information needs in advance, but in an unstructured environment, it becomes difficult to do so. As information is acquired, the manager may realize that additional information is required. In such cases, it is impossible to pre-design system report formats and contents. A DSS must, therefore, have greater flexibility than other information systems. Finally, we can say that DSS is of much more use when business are of an unstructured or semi-structured in nature. A decision support system is an integrated piece of software incorporating data base, model base and user interface. While the decision-support system can be of use at the tactical level, it is the strategic level that could make best use of it.

Question 12

What is MIS? Discuss characteristics of an effective MIS in brief.

Information Systems Control and Audit

Answer

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 inter locking 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.

Question 13

Explain the concept of decomposition with the help of an example.

Answer

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

Information Systems Control and Audit

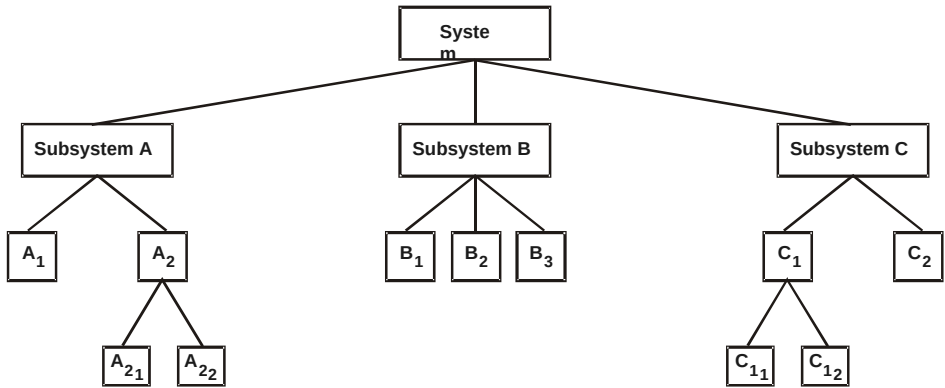


Fig.: Hierarchical relations of subsystems

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

1. Information system divided into sub system such as:

Sales and order entry

Inventory

Production

Personnel and payroll

Purchasing

Accounting and control

Planning

Environmental intelligence

2. Each sub system is divided further into sub systems. For example, the personnel and payroll sub system might be divided into the following smaller sub systems:

Creation and update of personnel pay roll records.

Personnel reports

Payroll data entry and validation

Hourly payroll processing

Salaried payroll processing

Payroll reports for management

Payroll reports for Government

3. If the task is to design and program a new system, the sub systems (major applications) defined above might be further sub divided into smaller sub systems or modules. For example, the hourly payroll processing sub system might be factored into modules for the calculation of deductions and net pay, payroll register and audit controls preparation, cheque printing and register and controls output as shown below:

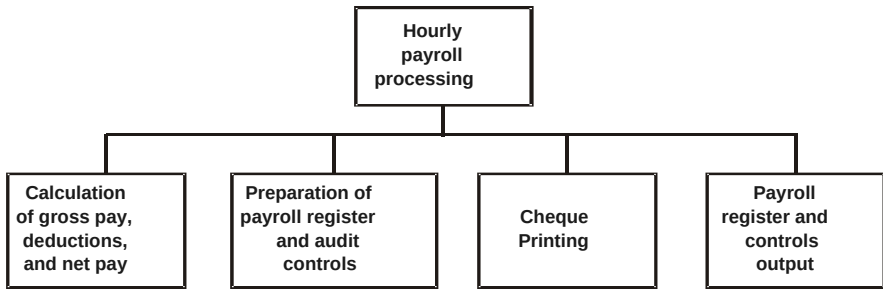


Fig.: Payroll Processing

Decomposition into sub systems is used to analyze an existing system and to design and implement a new system. In both the cases, the designer must decide how to factor i.e. where to draw the boundaries.

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

Question 14

Explain the concept of MIS in terms of its three elements.

Answer

MIS comprises of three elements viz., **management, information and system**. These are given as follows:

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

- (i) Determination of organizational objectives and developing plans to achieve them.
- (ii) Securing and organizing human beings and physical resources so as to achieve the laid down objectives.
- (iii) Exercising adequate controls over the functions performed at the lower level.

Information Systems Control and Audit

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

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

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

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

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

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

Question 15

Discuss the potential impact of computers and MIS on different levels of management.

Answer**Potential impact of computers and MIS on different levels of management**

The potential impact of computers on top level management may be quite significant. An important factor which may account for this change is the fast development in the area of computer science. It is believed that in future computers would be able to provide simulation models to assist top management in planning their work activities. For example, with the help of a computer it may be possible in future to develop a financial model by using simulation technique, which will facilitate executives to test the impact of ideas and strategies formulated on future profitability and in determining the needs for funds and physical resources. By carrying sensitivity analysis with the support of computers, it may be possible to study and measure the effect of variation of individual factors to determine final results. Also, the availability of a new class of experts will facilitate effective communication with computers. Such experts may also play a useful role in the development and processing of models. In brief, potential impact of computers would be more in the area of planning and decision making.

Futurists believe that top management will realize the significance of techniques like simulation, sensitivity analysis and management science. The application of these techniques to business problems with the help of computers would generate accurate, reliable, timely and comprehensive information to top management. Such information will be quite useful for the purpose of managerial planning and decision making. Computerized MIS will also influence in the development, evaluation and implementation of a solution to a problem under decision making process.

Potential impact of Computers and MIS on middle management level will also be significant. It will bring a marked change in the process of their decision making. At this level, most of the decisions will be programmed and thus will be made by the computer, thereby drastically reducing the requirement of middle level managers. For example, in the case of inventory control system; computer will carry records of all items in respect of their purchase, issue and balance. The reorder level, reorder quantity etc. for each item of material will also be stored in computer after its predetermination. Under such a system, as soon as the consumption level of a particular item of material will touch reorder level, computer will inform for its purchase immediately. The futurists also foresee the computer and the erosion of middle management as the vehicles for a major shift to recentralization. The new information technology will enable management to view an operation as a single entity whose effectiveness can only be optimized by making decisions that take into account the entity and not the individual parts.

The impact of Computers and MIS today at supervisory management level is maximum. At this level managers are responsible for routine, day-to-day decisions and activities of the organization which do not require much judgement and discretion. In a way, supervisory manager's job is directed more towards control functions, which are highly receptive to

Information Systems Control and Audit

computerization. For control, such managers are provided with accurate, timely, comprehensive and suitable reports. A higher percentage of information requirements of executives is met out at this level.

Potential impact of Computers and MIS on supervisory level will completely revolutionize the working at this level. Most of the controls in future will be operated with the help of computers. Even the need of supervisory managers for controlling the operations will be substantially reduced. Most of the operations/activities now performed manually will be either fully or partially automated.

Question 16

Describe the main pre-requisites of a Management Information System, which makes it an effective tool.

Answer

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

- (i) **Database:** It is a superfile which consolidates data records formerly stored in many data files. The data in database is organized in such a way that access to the data is improved and redundancy is reduced. Normally, the database is subdivided into major information sub-sets needed to run. The database should be user-oriented, capable of being used as a common data source, available to authorized persons only and should be controlled by a separate authority such as DBMS. Such a database is capable of meeting information requirements of its executives, which is necessary for planning, organizing and controlling the operations of the business.
- (ii) **Qualified System and Management Staff:** MIS should be manned by qualified officers. These officers who are experts in the field should understand clearly the views of their fellow officers. The organizational management base should comprise of two categories of officers (i) System and Computer experts and (ii) Management experts. Management experts should clearly understand the concepts and operations of a computer. Their whole hearted support and cooperation will help in making MIS an effective one.
- (iii) **Support of Top Management:** An MIS becomes effective only if it receives the full support of top management. To gain the support of top management, the officer should place before them all the supporting facts and state clearly the benefits which will accrue from it to the concern. This step will certainly enlighten the management and will change their attitude towards MIS.
- (iv) **Control and Maintenance of MIS:** Control of the MIS means the operation of the system as it was designed to operate. Sometimes users develop their own procedures or shortcut methods to use the system, which reduces its effectiveness.

To check such habits of users, the management at each level in the organization should device checks for the information system control.

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

- (v) **Evaluation of MIS:** An effective MIS should be capable of meeting the information requirements of its executives in future as well. The capability can be maintained by evaluating the MIS and taking appropriate timely action. The evaluation of MIS should take into account the following points:
- Examining the flexibility to cope with future requirements;
 - Ascertaining the view of the users and designers about the capabilities and deficiencies of the system ; and
 - Guiding the appropriate authority about the steps to be taken to maintain effectiveness of MIS.

Question 17

Describe the main prerequisites of a MIS which makes it an effective tool. Explain the major constraints in operating it.

Answer

Please refer the answer of question No. 16 for the answer of the first part of this question.

Constraints in operating MIS:

Major constraints which come in the way of operating an information system are:

- Non-availability of experts, who can diagnose the objectives of the organization and provide a desired direction for installing an operating system.
- Experts usually face the problem of selecting the sub-system of MIS to be installed and operated upon.
- Due to varied objectives of business concerns, the approach adopted by experts for designing and implementing MIS is a non-standardized one.
- Non-availability of cooperation from staff in fact is a crucial problem. It should be handled tactfully. Educating the staff by organizing lectures, showing films, training on system and utility of the system may solve this problem.
- There is high turnover of experts in MIS. Turnover in fact arises due to several factors like pay packet, promotion chances, future prospects, behaviour of top ranking managers etc.

Information Systems Control and Audit

- Difficulty in quantifying the benefits of MIS, so that it is easily comparable with cost.

Question 18

What is Decision Support System? Briefly explain three characteristics of Decision Support System.

Answer

The Decision Support System (DSS) is considered as more flexible and adaptable to changing decision making requirements than traditional Management reporting system. This system emerged from the developments of interactive display technology, micro computing and easy-to-use software tools. It handles unstructured and partially structured problems giving rise to unpredictable and unstructured information needs.

DSS can be defined as a system providing tools to the decision making managers to address unstructured/ partially structured problems in their own personalized manner. It empowers the managers in decision making process. A DSS does not require any high technology.

There are three characteristics of a Decision Support System namely:

- Semistructured or unstructured decision-making.
- Adaptable to the changing needs of decision makers, and
- Ease of learning and use.

Each of these are briefly discussed below:

- Semistructured and Unstructured Decisions:* Unstructured decisions and semistructured decisions are made when information obtained from a computer system is only a portion of the total knowledge needed to make the decision. DSS is well adapted to help with semistructured and unstructured decisions. A well-designed DSS helps in decision making process with the depth to which the available data can be tapped for useful information.
- Ability to adapt to changing needs:* Semistructured and unstructured decisions often do not conform to a predefined set of decision-making rules. DSS provides flexibility to enable users to model their own information needs. Rather than locking the system into rigid information producing requirements, capabilities and tools are provided by DSS to enable users to meet their own output needs.
- Ease of Learning and Use:* DSS software tools employ user-oriented interfaces such as grids, graphics, non-procedural fourth – generation languages (4GL), natural English, and easily read documentation. These interfaces make it easier for users to conceptualize and perform the decision-making process.

Question 19

What is DSS? Explain the components of a DSS in brief.

Answer

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.:

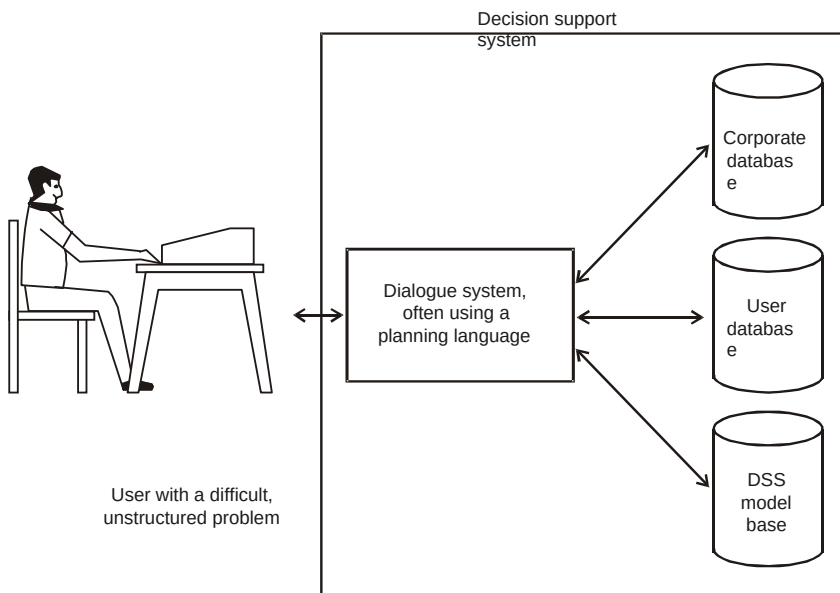


Fig.: The Components of a decision support system

- (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

Information Systems Control and Audit

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.

Question 20

Discuss various examples of DSS in accounting.

Answer

Examples of Decision Support Systems (DSS) 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

Information Systems Control and Audit

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.

Question 21

Explain Executive Information System (EIS). What purpose does it serve?

Answer

An Executive Information System (EIS) is a tool that provides direct on-line access to relevant information in a useful and navigable format. The relevant information is timely, accurate, and actionable information about aspects of a business that are of particular interest to the senior manager. An EIS is easy to navigate so that managers can identify broad strategic issues, and then explore the information to find the root causes of those issues.

EIS serves the following purpose:

- (i) The primary purpose of an Executive Information System is to support managerial learning about an organization, its work processes, and its interaction with the external environment.
- (ii) A secondary purpose is to allow timely access to information so that based on the answers to questions, strategic decisions could be taken by a manager in time.
- (iii) It directs the attention of the management to specific areas of the organization or specific business problems. It makes managers and subordinates to work together to determine the root causes of issues highlighted by EIS

Question 22

Explain various purposes of an Executive Information System (EIS).

Answer

Purposes of an EIS: These are stated below:

- (i) **The primary purpose** of an Executive Information System is to support managerial learning about an organization, its work processes, and its interaction with the external environment. Informed managers can ask better questions and make better decisions.
- (ii) **A secondary purpose** for an EIS is to allow timely access to information. All of the information contained in an EIS can typically be obtained by a manager through traditional methods. However, the resources and time required to manually compile information in a wide variety of formats, and in response to ever changing and even more specific questions usually inhibit managers from obtaining this information.
- (iii) **A third purpose** of an EIS is commonly misperceived. An EIS has a powerful ability to direct management attention to specific areas of the organization or specific business problems. Some managers see this as an opportunity to discipline subordinates. Some subordinates fear the directive nature of the system and spend a great deal of time trying to outfit or discredit it. Neither of these behaviors is appropriate or productive. Rather, managers and subordinates can work together to determine the root causes of issues highlighted by the EIS.

EXERCISE

Question 1

In the context of a business organization, explain the following:

- (a) *Attributes of Information, and*
- (b) *Types of information.*

Question 2

As a member of the system development team, explain the process of decomposition of an organization into various functional blocks to comprehend the information processing system with the help of an example.

Question 3

Briefly describe the executive roles at the strategic level of management.

Question 4

Identify and justify the need for an information system that is designed to meet the special business needs of the strategic level of management in an organization.

Question 5

State the pre-requisites for an effective MIS in brief.

Question 6

Identify the tools of a Decision Support System.

Question 7

“A decision support system supports the human decision-making process rather than providing a means to replace it”. Justify the above statement by stating the characteristics of decision support system.

Question 8

“Decision support systems are widely used as part of an Organization’s Accounting Information system”. Give examples to support this statement.

Question 9

Describe various software tools used in Decision support system.

Question 10

How does an Executive Information System (EIS) differ from a traditional information system?

Question 11

Briefly explain the principles to guide the design of measures and indicators to be included in EIS.

Question 12

Write short notes on the following:

- (a) *Decision Support System*
- (b) *Executive Information System.*
- (c) *Expert systems*

SYSTEM DEVELOPMENT LIFE CYCLE METHODOLOGY

BASIC CONCEPTS

1. System Development Process

- 1.1 **System Development Life Cycle:** Preliminary Investigation, Requirements analysis, Designing of system, Development of Software, Systems Testing, Implementation and Maintenance
- 1.2 **Achieving systems development objectives**
- 1.3 **Approaches to Systems Development:** Traditional and alternative approach

2. Preliminary Investigation

- 2.1 Definition of the scope of the study
- 2.2 **Conducting the Investigation:** Reviewing internal documents, and conducting interviews
- 2.3 Identifying Viable Options
- 2.4 **Testing Project's Feasibility:** Technical Feasibility, Economic Feasibility, Operational Feasibility, Schedule Feasibility, and Legal Feasibility
- 2.5 Estimating costs and benefits
- 2.6 Reporting results to management

3. Requirements Analysis

- 3.1 **Fact finding techniques:** Documents, Questionnaires, Interviews, Observations
- 3.2 **Analysis of the Present System:** Review historical aspects, Analyze inputs, Review data files maintained, Review methods, procedures and data communications, Analyze Outputs, Review Internal controls, Model the existing physical system and logical system, Undertake overall analysis of present system.

Information Systems Control and Audit

3.3 System Development Tools: Systems Flow Chart, Data Flow Diagrams, Layout Forms and Screens, System Components Matrix, CASE Tools, Data Dictionary

4. Systems Design

4.1 Designing Systems Output

4.2 Important Factors in Output Design: Content, Form, Output Volume, Timeliness, Media, Format

4.3 Designing printed output

4.4 Designing visual display output: Layout of display screen, Designing of Windows

4.5 Designing Systems Inputs: Many of the issues involved in input are also similar to those of output

4.6 Guidelines for form design: Making forms easy to fill, Meeting the intended purpose, Ensuring accurate completion, and Keeping forms attractive

4.7 Coding Methods: Some of the desired characteristics are: Individuality, Space, Convenience, Expandability, and Suggestiveness

4.8 Designing efficient data entry

4.9 Data Storage

4.10 Design of data communication

4.11 System Manual

4.12 Reporting to Management

5. Systems Acquisition and Software Development

5.1 Procuring Computer Hardware

5.2 Software acquisition

5.3 Advantages of Application Packages: Rapid Application, Low Risk, Quality, Cost

5.4 Validation of vendors' proposals: The factors have to be considered are: The performance capability of each proposed system in relation to its Costs, The Costs and benefits of each Proposed System, The Maintainability of each Proposed System, The Compatibility of each proposed system with existing systems, Vendor Support

5.5 Method for validating the proposal:

5.5.1 Checklists: Example of software validation checklist and Support Service Checklists

5.5.2 Point Scoring Analysis

5.5.3 Public Evaluation Reports

5.6 Software Development: It involves six stages: Program Analysis, Program Design, Program Coding, Debug the Program, Program documentation, and Program Maintenance

5.7 Alternative Development Methodology

5.7.1 Prototyping Approach: It involves four steps: Identify Information System Requirements, Develop the initial Prototype, Test and Revise, obtain User Signoff for the approved prototype

5.7.2 End User Development Approach

5.7.3 Systematic Approach for development in small organizations

5.7.4 Rapid Application Development (RAD)

6. System Testing

7. System Implementation

7.1 Equipment Installation: Site Preparation, Equipment installation, Equipment Check out

7.2 Training Personnel: Training System Operators, User Training

7.3 Conversion and Start-up from manual to Computerized System

7.3.1 Conversion Strategies: There are five strategies: Direct changeover, Parallel conversion, Gradual conversion, modular prototypes conversion, Distributed Conversion

7.3.2 Activities involved in Conversion: Procedure conversion, File conversion, System conversion, Scheduling personnel and equipment, and alternative plans in case of equipment failure

7.4 Post Implementation Review: Development evaluation, Operation evaluation, and Information Evaluation

8. System Maintenance: Scheduled maintenance and rescue maintenance

9. Organizational Structure of IT Department

9.1 Management Structure: Line Management Structure, and Project Management Structure. In Line Management, there are following management subsystems: Top

Information Systems Control and Audit

Management, IS Management, Systems Development Management, Programming Management, Data Administration, Security Administration, Operations Management, and Quality Assurance Management

9.2 Duties and responsibilities: Data entry, File library, Control Groups, Operations, Security Administration, Physical Security, Data Security, Conducting a security program, Production work flow control, Quality Assurance, System Analysis, Application Programming, Systems Programming, LAN Administration, Help Desk administration

Question 1

State and briefly explain the six stages of System Development Life Cycle (SDLC).

Answer

System Development Life Cycle: The system development process is initiated when it is realized that a particular business process of the organization needs computerization or improvement. The system development life cycle is a set of six activities which are closely related. These activities after a certain stage can be done parallel to each other. For example the development can be started for some components (sub-systems) which are at the advance stage of designing. The systems development life cycle method consists of the following activities:

- (i) Preliminary investigation
- (ii) Requirements analysis or systems analysis
- (iii) Design of system
- (iv) Development of software
- (v) Systems testing
- (vi) Implementation and maintenance

The activities are briefly explained below:

- (i) *Preliminary investigation:* When the user comes across a problem in the existing system or a totally new requirement for computerization, a formal request has to be submitted for system development. It consists of three parts; request classification feasibility study and request approval. Generally the request submitted is not stated clearly hence requires detailed study. On receipt of request and identification of needs, the feasibility study is conducted which includes the aspects related to technical, economic and operational feasibility and is normally conducted by a third party depending upon the quantum and size of the requirements. The approval is sought from top management to initiate the system development.

- (ii) *Requirements analysis or systems analysis*: Once the request of the system development is approved, the detailed requirement study is conducted in close interaction with the concerned employees and managers to understand the detailed functioning, short-comings, bottlenecks and to determine the features to be included in the system catering to the needs and requirements of the users. This process is termed as “System Requirement Study (SRS) or System analysis.
- (iii) *Design of the system*: This activity evolves the methodology and steps to be included in the system to meet the identified needs and requirements of the system. The analyst designs the various procedures, report, inputs, files and database structures and prepares the comprehensive system design. These specifications are then passed on to the Development Team for program coding and testing.
- (iv) *Acquisition and development of software*: Once the system design details are resolved and SRS is accepted by the user, the hardware and software details along with services requirements are determined and procured choosing the best-fit options. Subsequently, choices are made regarding which products to buy or lease from which vendors. The choice depends on many factors such as time, cost and availability of programmers. In case of in-house development, the analyst works closely with the programmers. The analyst also works with users to develop documentation for software and various procedure manuals.
- (v) *Systems testing*: Once all the programs comprising the system have been developed and tested, the system needs to be tested as a whole. System testing is conducted with various probable options and conditions to ensure that it does not fail in any condition. The system is expected to run as per the specifications made in the SRS and users’ expectations. Live test data are input for processing, and results are examined. If it is found satisfactory, it is eventually tested with actual data from the current system.
- (vi) *Implementation and maintenance*: By the time of accomplishment of the above activities, it is ensured that the requisite hardware and software are installed and the users are trained on the new system to carry out operations independently. For sometime, hand-holding may be done by the system development team. The operations are monitored closely to ensure the users satisfaction. The system is maintained and modified to adapt to the changing needs of the users and business to ensure long-term acceptance of the system.

Question 2

Write short notes on the following:

- (a) *Advantages of Application Packages*

Information Systems Control and Audit

(b) *Information System Maintenance*

(c) *System Manual*

Answer

(a) The four most compelling advantages of using pre written application packages are:

- (i) *Rapid implementation:* Application packages are readily available to implement after they are purchased. In contrast, software developed in-house may take months or even years until it is ready for implementation.
- (ii) *Low risk:* Since the application package is available in the finished form, the organisation knows what it is going to get for the price it has paid. With in-house developed software, the long development time breeds uncertainty with regard to both the quality of the final product and its final cost.
- (iii) *Quality:* The firms engaged in application package developments are typically specialist in their products' niche area. Generally, they have a lot of experience in their specialised application field and hence can provide better software. In contrast, in-house programs often have to work over a wide range of application areas; they may not be possessing expertise for undertaking proposed software development.
- (iv) *Cost:* Software cost can be leveraged as copies are generated and sold. Application packages, sometimes, turn out to be cheaper compared to in-house developed software.

(b) **Information Systems Maintenance:** Most information systems require at least some modification after development. The need for modification arises from a failure to anticipate all requirements during system design and/or from changing organizational requirements. Hence periodic system maintenance is required for most Information Systems. Systems maintenance involves adding new data elements, modifying reports, adding new reports, changing calculations, etc. Maintenance can be categorized in the following two ways:

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

One problem that occurs in systems development and maintenance is that as more and more systems are developed, a greater portion of systems analyst and

programmer time is spent on maintenance. An information system may remain in an operational and maintenance mode for several years. The system should be evaluated periodically to ensure that it is operating properly and is still workable for the organization. When a system becomes obsolete i.e. new opportunities in terms of new technology are available or it no longer satisfies the organization's needs, the information system may be replaced by a new one generated from a fresh system development process.

- (c) **System Manual:** The basic output of the system design is a description of the task to be performed, complete with layouts and flowcharts. This is called the job specifications manual or system manual. It contains:
- (i) General description of the existing system.
 - (ii) Flow of the existing system.
 - (iii) Outputs of the existing system - the documents produced by existing system are listed and briefly described, including distribution of copies.
 - (iv) General description of the new system - its purposes and functions and major differences from the existing system are stated together with a brief justification for the change.
 - (v) Flow of the new system - this shows the flow of the system from and to the computer operation and the flow within the computer department. .
 - (vi) Output Layouts.
 - (vii) Output distribution - the distribution of the new output document is indicated and the number of copies, routing and purpose in each department shown. The output distribution is summarized to show what each department will receive as a part of the proposed system.
 - (viii) Input layouts - the inputs to the new system are described and complete layouts of the input documents and input disks or tapes provided.
 - (ix) Input responsibility - the source of each input document is indicated as also the user department responsible for each item on the input documents.
 - (x) Macro-logic- the overall logic of the internal flow will be briefly described by the systems analyst, wherever useful.
 - (xi) Files to be maintained - the specifications will contain a listing of the tape, disk or other permanent record files to be maintained, and the items of information to be included in each file. There must be complete layouts for intermediate or work file; these may be prepared later by the programmer.
-

Information Systems Control and Audit

- (xii) List of programs - a list of the programs to be written shall be a part of the systems specifications.
- (xiii) Timing estimates - a summary of approximate computer timing is provided by the system analyst.
- (xiv) Controls - this shall include type of controls, and the method in which it will be operated.
- (xv) Audit trail - a separate section of the systems specifications shows the audit trail for all financial information. It indicates the methods with which errors and defalcation will be prevented or eliminated.
- (xvi) Glossary of terms used.

Question 3

The top management of company has decided to develop a computer information system for its operations. Is it essential to conduct the feasibility study of system before implementing it? If answer is yes, state the reasons. Also discuss three different angles through which the feasibility study of the system is to be conducted.

Answer

Yes, it is essential to carry out the feasibility study of the project before its implementation. After possible solution options are identified, project feasibility-the likelihood that these systems will be useful for the organization-is determined. A feasibility study is carried out by the system analysts for this purpose. Feasibility study refers to a process of evaluating alternative systems through cost/benefit analysis so that the most feasible and desirable system can be selected for development. It is carried out by the system analysts.

The feasibility study of the system is undertaken from three angles i.e. technical, economic and operational. The proposed system is evaluated from a technical view point first and if technically feasible, its impact on the organization and staff is assessed. If a compatible technical and social system can be devised, it is then tested for economic feasibility.

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:

- (i) Does the necessary technology exist to do what is suggested (and can it be acquired)?

- (ii) Does the proposed equipment have the technical capacity to hold the data required to use the new system?
- (iii) Will the proposed system provide an adequate response to inquiries, regardless of the number or location of users?
- (iv) Can the system be expanded if developed?
- (v) Are there technical guarantees of accuracy, reliability, ease of access, the data security?

Some of the technical issues to be considered are given in the Table-1 below.

Design Considerations	Design Alternatives
Communications channel configuration	Point to point, multidrop, or line sharing
Communications channels	Telephone lines, coaxial cable, fiber optics, microwave, or satellite
Communications network	Centralized, decentralized, distributed, or local area
Computer programs	Independent vendor or in-house
Data storage medium	Tape, floppy disk, hard disk, or hard copy
Data storage structure	Files or database
File organization and access	Direct access or sequential files
Input medium	Keying, OCR, MICR, POS, EDI, or voice recognition
Operations	In-house or outsourcing
Output frequency	Instantaneous, hourly, daily, weekly, or monthly
Output medium	CRT, hard copy, voice, or turnaround document
Output scheduling	Predetermined times or on demand
Printed output	Preprinted forms or system-generated forms
Processor	Micro, mini, or mainframe
Transaction processing	Batch or online
Update frequency	Instantaneous, hourly, daily, weekly, or monthly

Table-1: Technical Issues

Due to tremendous advancements in computer field these days, the technology is available for most business data processing systems but sometimes not within the constraints of the firm's resources or its implementation schedule. Therefore, trade offs

Information Systems Control and Audit

are often necessary. A technically feasible system may not be economically feasible or may be so sophisticated that the firm's personnel cannot effectively operate it.

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

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

The procedure employed is the traditional cost-benefit study.

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

- (i) Is there sufficient support for the system from management and from users? If the current system is well liked and used to the extent that persons will not be able to see reasons for a change, there may be resistance.
- (ii) Are current business methods acceptable to user? If they are not, users may welcome a change that will bring about a more operational and useful system.
- (iii) Have the users been involved in planning and development of the project? Early involvement reduces the chances of resistance to the system and changes in general and increases the likelihood successful projects.
- (iv) Will the proposed system cause harm? Will it produce poorer results in any respect or area? Will loss of control results in any areas? Will accessibility of information be lost? Will individual performance be poorer after implementation that before? Will performance be affected in an undesirable way? Will the system slow performance in any areas?

Question 4

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 |

Answer

- (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.

Information Systems Control and Audit

- 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.

Question 5

What is Prototyping? Discuss its advantages and disadvantages in brief.

Answer

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.

Information Systems Control and Audit

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.

Question 6

Write short notes on the following:

- | | |
|----------------------------------|---------------------------------------|
| (i) <i>Audit Trails</i> | (ii) <i>Crypto systems</i> |
| (iii) <i>Preventive Controls</i> | (iv) <i>Public Key Infrastructure</i> |

Answer

- (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

Information Systems Control and Audit

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.

Question 7

Explain the System Development Life Cycle.

Answer

System Development Life Cycle Activities:

The system development life cycle method can be thought of as a set of activities that analysts, designers and users carry out to develop and implement an information system.

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

- (i) Preliminary investigation
 - (ii) Requirements analysis or system analysis
 - (iii) Design of system
 - (iv) Development of software
 - (v) System testing
 - (vi) Implementation and maintenance.
- (i) Preliminary investigation: A preliminary investigation is undertaken when users come across a problem or opportunity and submit a formal request for a new systems to the MIS department. This activity consists of three parts: request clarification, feasibility study and request approval. Before any system investigations can be considered, the system request must be examined to determine precisely what the originator wants. Thereafter, the analyst tries to determine whether the system requested is feasible or not. Aspects of technical, economic and operational feasibility of the system are

covered in the feasibility study. The third part of the investigation relates to approval of the request. Not all requested systems are desirable or feasible. Based on the observations of the analyst, the management decides which system should be taken up for development.

- (ii) Requirements analysis or system analysis: If, after studying the result of preliminary investigation, management decides to continue the development process, the needs of the users are studied. Several fact-finding techniques and tools such as questionnaires, interviews, observing decision-maker behaviour and their office environment etc. are used for understanding the requirements. All details are gathered, the analysts study the present system to identify its problems and shortcomings and identify the features, which the new system should include to satisfy the new or changed user application environment.
- (iii) Design of system: The design of an information system produces the details that state how a system will meet the requirements identified above. The analyst designs various reports / outputs, data entry procedures, inputs, files and database. He also selects file structures and data storage devices. These detailed design specifications are then passed on to the programming staff so that software development can begin.
- (iv) Acquisition and development of software: After the system design details are resolved, such resources needs as specific type of hardware, software and services are determined. Subsequently, choices are made regarding which products to buy or lease from which vendors. Software developers may install or modify and then install purchased software or they may write new, custom-designed program. The analyst works closely with the programmers if the software is to be developed in-house. During this phase, he analyst also works with users to develop worthwhile documentation for software, including various procedure manuals.
- (v) System testing: Before the information systems can be used, it must be tested. System testing will run according to its specifications and in the way users expect. If it is found satisfactory, it is eventually tested with actual data from the current systems.
- (vi) Implementation and maintenance: After the system is found to be fit, it is implemented with the actual data. Hardware is installed and users are then trained on the new system and eventually work on it is carried out independently. The results of the development efforts are reviewed to ensure that the new system satisfies user requirements. After implementation, the systems is maintained, it is modified to adapt to changing users and business needs so that the system can be useful to the organization as long as possible.

Information Systems Control and Audit

The system development life cycle should be viewed as a continuous interactive process that recycles through each stage for many applications. Thus, even when a system is fully specified, designed, purchased and running, it is continually being enhanced or maintained. Enhancement and maintenance may require returning to one of the earlier stages of system development life cycle.

Question 8

What are the Systems Development Tools? Explain briefly.

Answer

System Development Tools: Tools and Techniques have been developed to improve current information systems and to develop new ones. The major tools used for system development can be grouped into the following four categories based on the systems features each document has:

- (i) **System Components and flows:** These tools help the system analysts to document the data flow among the major resources and activities of an information system. System flow charts are typically used to show the flow of data media as they are processed by the hardware devices and manual activities. A data flow diagram uses a few simple symbols to illustrate the flow of data among external entities (such as people or organization etc) processing activities and data storage elements.
- (ii) **User Interface:** Designing the interface between end users and the computer system is a major consideration of a system analyst while designing the new system. Layout forms and screens are used to construct the formats and contents of input / output media and methods. Dialogue flow diagrams analyse the flow of dialogue between computers and people.
- (iii) **Data attributes and relationships:** The data resources in information system are defined, catalogued and designed by this category of tools. A data dictionary catalogs the description of the attributes (characteristics) of all data elements and their relationships to each other as well as to external systems. Entity-relationships diagrams are used to document the number and type of relationship among the entities in a systems. File layout forms document the type, size and names of the data elements in a system. Grid charts help in identifying the use of each type of data element in input / output or storage media of a system.
- (iv) **Detailed system process:** These tools are used to help the programmer develop detailed procedures and processes required in the design of a computer program. Decision trees and decision tables use a network or tabular form to document the complex conditional logic involved in choosing among the information processing alternatives in a system.

Question 9

What do you understand by feasibility study? Explain various types of feasibility studies.

Answer

Feasibility Study: It refers to the process of evaluating alternative systems through cost / benefit analysis so that the most feasible and desirable system can be selected for development. The feasibility study of a system is undertaken from three angles: technical, economic and operational feasibility.

Technical feasibility: It is concerned with hardware and software. The technical issues usually raised during the feasibility stage of investigation include the following:

- (i) Does the necessary technology exist to do what is suggested (and can it be acquired)?
- (ii) Does the proposed equipment have the technical capacity to hold the data required to use the new system?
- (iii) Will the proposed system provide adequate responses to inquiries, regardless of the number or location of users?
- (iv) Can the system be expanded if developed?
- (v) Are there technical guarantees of accuracy, reliability, ease of access and data security?

Economic Feasibility: It includes an evaluation of all the incremental costs and benefits expected if the proposed system is implemented. The financial and economic questions raised by analysts during the preliminary investigation are for the purpose of estimating the following:

- (i) The cost of conducting full systems investigation.
- (ii) The cost of hardware and software for the class of applications being considered.
- (iii) The benefits in the form of reduced costs or fewer costly errors.
- (iv) The cost if nothing changes.

Operational feasibility: It is concerned with ascertaining the views of workers, employees, customers and suppliers about the use of computer facility.

Some of the questions which help in testing the operational feasibility of a project are:

Is there sufficient support for the system from management? From users? If the current system is well liked and used to the extent that persons will not be able to see reasons for a change, there may be resistance.

Information Systems Control and Audit

Are current business methods acceptable to users? If they are not, users may welcome a change that will bring about a more operational and useful system.

Have the users been involved in planning and development of the project? Early involvement reduces the chance of resistance to the system and changes in general and increases the likelihood of successful projects.

Will the proposed system cause harm? Will it produce poorer results in any aspects or areas? Will loss of control result in any areas? Will accessibility of information be lost? Will individual performance be poorer after implementation than before? Will performance be affected in an undesirable way? Will the system slow performance in any areas?

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

Legal Feasibility: Legal feasibility is largely concerned with whether there will be any conflict between a newly proposed system and the organization's legal obligations. For example, a revised system should comply with all applicable federal and state statutes about financial reporting requirements, as well as the company's contractual obligations.

Question 10

State and explain any five approaches to System Development.

Answer

Organizations vary significantly in the way they automate their business procedures. Also, since each new type of system usually differs from any other, several different systems development approaches are often used within an organization. Five most commonly used approaches are discussed below:

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

This approach is applied to the development of large computer based information systems such as the transaction processing systems.

- (ii) **Prototyping approaches:** This approach is basically used for the development of such systems 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 an useable system or component that is built quickly and at a lesser cost, and with the intention of being modified 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 specifications lists.

- (iii) **End user development approach:** In end-user development, it is the end user and not the computer professional who is responsible for systems development activities. Many different kinds of organizations allow end-users to develop systems. For example, whenever a manager or a department acquires its own, relatively inexpensive microcomputers or office information systems, end-user development often takes place. The number and nature of systems development activities followed by the end-user often differ from those found in formal approaches such as the traditional approach.

- (iv) **Top down approach:** The top down approach assumes a high degree of top management involvement in the planning process and focuses on organizational goals, objectives and strategies. Using the top-down approach, we begin by analyzing organizational objectives and goals and end by specifying application programs and modules that need to be developed to support those goals. The various stages in top down approach are as follows:

- (a) Analyze the objectives and goals of the organization to determine where it is going and what management wants to accomplish. The analysis may be started in terms of profits, growth, expansion of product line or services, diversification, increased market share and so on. It is also determined what resources are available in terms of capital, equipment and raw material.
- (b) Identify the functions of the organization (for example, marketing, production, research and development) and explain how they support the entire organization.
- (c) Based on the functions identified above, ascertain the major activities, decisions and functions of the managers at various levels of hierarchy.

Information Systems Control and Audit

- (d) With activities and decisions identified, we must now identify models that guide managerial decisions processes and find out the information requirements for activities and decisions.
- (e) Prepare specific information processing programs in detail and modules within these programs. We may also identify files and data base for applications.
- (v) **Bottom-up approach:** The bottom up approach to system planning begins by identifying basic transactions and information processing programs.

The development starts from the fundamental or lifestream systems of the personnel processing systems that support day-to-day business activities. As these systems are identified, the data and file requirements for each one can also be specified.

Once the basic transactions and information processing systems are known, data requirements across applications are examined and the files and records combined in order to be usable for several applications. Thus, applications are integrated using data base concepts which enhances the sharability and evolvability of the data base, ensures that uniform data are used by all programs, and reduces the redundancy found so frequently in non-integrated, program-oriented files.

Program, system and data integration are followed by the formulation of models to support higher management level activities. Decisions are then made using the output of the model-based analysis that have been integrated into the computer information systems.

As more and more models are developed and used, model banks are established. A model bank is similar to a data base in that different planning and control models are developed and stored. They can be used to examine many different strategies.

Thus, the bottom-up approach takes us to higher levels of decision making in the organization. As we come closer to the strategic planning level, we need to integrate more and more data and information processing activities.

Question 11

Discuss in detail, how the analysis of present system is made by the system analyst.

Or

A Company is offering a wide range of products and services to its customers. It relies heavily on its existing information system to provide up to date information. The company wishes to enhance its existing system. You being an information system auditor, suggest how the investigation of the present information system should be conducted so that it can be further improved upon.

Answer

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

The following areas may be studied in depth:

1. **Review historical aspects:** A brief history of the organization is a logical starting point for the analysis of the present system. The historical facts should identify the major turning points and milestones that have influenced its growth. A review of annual reports can provide an excellent historical perspective. A historical review of the organization chart can identify the growth of management levels as well as the development of various functional areas and departments. The system analyst should identify what system changes have occurred in the past. These should include operations that have been successful or unsuccessful with computer equipment and techniques.
2. **Analyze inputs:** A detailed analysis of present inputs is important since they are basic to the manipulation of data. Source documents are used to capture the originating data for any type of system. The system analyst should be aware of the various sources from where the data can be initially captured, keeping in view the fact that outputs for one area may serve as an input for another area. The system analyst must understand the nature of each form, what is contained in it, who prepared it, from where the form is initiated, where it is completed, the distribution of the form and other similar considerations. If the analyst investigates these questions thoroughly, he will be able to determine how these inputs fit into the framework of the present system.
3. **Review data files maintained:** The analysts should investigate the data files maintained by each department, noting their number and size, where they are located, who uses them and the number of times per given time interval these are used. Information on common data files and their size will be an important factor, which will influence the new information system. This information may be contained in the systems and procedures manuals. The system analyst should also review all online and off line files which are maintained in the organization as these will reveal information about data that are not contained in any output. The related cost of retrieving and processing the data is another important factor that should be considered by the systems analyst.

Information Systems Control and Audit

4. **Review methods, procedures and data communications:** Methods and procedures transform input data into useful output. A method is defined as a way of doing something; a procedure is a series of logical steps by which a job is accomplished. A procedure's review is an intensive survey of the methods by which each job is accomplished, the equipment utilized and the actual location of the operations. Its basic objective is to eliminate unnecessary tasks or to perceive improvement in opportunities in the present information system. A system analyst also needs to review and understand the present data communications used by the organization. He must review the types of data communication equipment including data interface, data links, modems, dial-up and leased lines and multiplexers. The system analyst must understand how the data communications network is used in the present system so as to identify the need to revamp the network when the new system is installed.
5. **Analyze outputs:** The outputs or reports should be scrutinized carefully by the system analysts in order to determine how well they will meet the organization's needs. The analysts must understand what information is needed and why, who needs it and when and where it is needed. Additional questions concerning the sequence of the data, how often the form reporting it is used, how long it is kept on file, etc. must be investigated. Often many reports are a carryover from earlier days and have little relevance to current operations. Attempt should be made to eliminate all such reports in the new system.
6. **Review internal controls:** A detailed investigation of the present information system is not complete until internal controls are reviewed. Locating the control points helps the analyst to visualize the essential parts and framework of a system. An examination of the present system of internal control may indicate weaknesses that should be removed in the new system. The adoption of advanced methods, procedures and equipment might allow much greater control over the data.
7. **Model the existing physical system and logical system:** As the logic of inputs, methods, procedures, data files, data communications, reports, internal control and other important items are reviewed and analyzed in a top down manner, the process must be properly documented. The logical flow of the present information system may be depicted with the help of system flow charts. The physical flow of the existing system may be shown by employing data flow diagrams. During the process of developing the data flow diagram, work on data dictionary for the new information system should be begun. The data elements needed in the new system will be found in the present system only. Hence, it is wise to start the development of the data dictionary as early as possible.

The flow charting and diagramming of present information not only organizes the facts, but also helps disclose gaps and duplication in the data gathered. It allows a thorough comprehension of the numerous details and related problems in the present operation.

8. **Undertake overall analysis of present system:** Based upon the aforesaid investigation of the present information system, the final phase of the detailed investigation includes the analysis of:
- a. the present work volume
 - b. the current personnel requirements
 - c. the present benefits and costs

Each of these must be investigated thoroughly.

Question 12

What do you understand by "Requirement analysis"? What is the significance of analyzing the present system and how is it carried out? Explain briefly.

Or

What are the facts finding techniques used by a system analyst?

Answer

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

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

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

Detailed investigation of the present system involves collecting, organising and evaluating facts about the system and the environment in which it operates. The survey of existing methods, procedures, data flow diagrams, outputs, files, input and internal controls should be done indepth in order to fully understand the present system and its related problems. While analyzing the present system, the following areas should be studied in depth.

1. Review of historical aspects
2. Analysis of inputs
3. Review of data files maintained

Information Systems Control and Audit

4. Review of methods, procedures and data communication
5. Analysis of output
6. Review of internal controls
7. Model of existing physical & logical systems.

In order to determine the user needs and to find weaknesses and strong points about the present system, analysts use various fact finding techniques.

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

1. **Documents:** Manuals, input forms, output forms, diagrams of how the current system works, organization charts showing hierarchy of users and managers responsibilities, job description for the people who work with current system, procedure manuals, program codes for applications associated with current system etc. should be looked into as thoroughly as possible, since they are the rich source of information.
2. **Questionnaires:** Users and managers are asked to complete questionnaire about the information system when the traditional system development approach is chosen. Using questionnaires, a large amount of data can be collected through a variety of users quickly.
3. **Interviews:** Users and managers may also be interviewed to extract information from them. The information so obtained provides complete picture of the present system. The interview also gives analyst the opportunity to know about the first hand user reactions and to probe for further information.
4. **Observation:** In prototype approach, observation plays a central role in requirement analysis. The analyst visits the user place to watch how the work is taking place. While the user is experimenting with the prototype, the systems analyst observes the user and puts these observations into perspective in order to determine how the prototype should be further designed. This gives him first hand information rather than relying on other methods such as analyzing documents, questionnaires etc.

Question 13

Explain prototyping approaches to systems development.

Answer

Prototyping approach: 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 an 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 support systems that are characterized by 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.

Question 14

What are the advantages of prototyping approaches?

Answer

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.

Other advantages of prototyping include:

- improving the fact finding process;
- improving relations between analysts and users;
- encouraging the users to 'own' the new system;
- reducing the cost of user training;
- identification of system problems;
- ensuring quality for the eventual system.

Information Systems Control and Audit

Question 15

If you are the Project Manager of a Software Company with the responsibility for developing a break-through product, combining state of the art hardware and software, will you opt for prototyping as a process model for a product meant for the intensely competitive entertainment market?

Answer

Prototyping as a process model will be inappropriate and hence inadvisable for the following reasons:

- (i) Prototyping requires user involvement. Here the users are the consumers of the product who are diffused and may not be inclined to join in.
- (ii) When we try to test the product with the involvement of customers, confidential or critical information might get leaked to the competitors on our line of thinking. The element of surprise and also the opportunity to capture the market will be lost.
- (iii) Prototyping requires significant time for experimenting. Since the product is meant for the intensely competitive entertainment market, the project manager may not have that much time to experiment, the competitor may capture the market by entering the market in advance.

Question 16

Describe briefly four categories of the major tools that are used for system development.

Answer

The major tools used for system development can be grouped into four categories based on the systems features each document has. These are:

- (i) Components and flows of a system
- (ii) User interface
- (iii) Data attributes and relationships
- (iv) Detailed system process.

Each of these categories are briefly discussed below:-

- (i) **System components and flows:** For system analysts these tools are helpful to document the data flow among the major resources and activities of an information system. System flow charts are typically used to show the flow of data media as they are processed by the hardware devices and manual activities. A system component matrix provides a matrix framework to document the resources used, the activities performed and the information produced by information system. A data flow diagram uses a few simple symbols to illustrate the flow of data among external entities.

- (ii) **User interface:** Designing the interface between end users and the computer system is a major consideration of system analysts while designing the new system. Layout forms and screens are used to construct the formats and contents of input / output media and methods. Dialogue flow diagrams analyze the flow of dialogue between computers and people. They document the flows among different display screens generated by alternative end user responses to menus and prompts.
- (iii) **Data attributes and relationships:** These tools are helpful to define, catalogue and design the data resources in information systems. A data dictionary catalogs the description of the attributes of all data elements and their relationship to each other as well as to external systems. Entity – relationship diagrams are also used to document the number and type of relationship among the entities in a system. File layout forms document the type, size, and names of the data elements in a system. Grid charts help in identifying the use of each type of data element in input / output or storage media of a system.
- (iv) **Detailed system process:** These tools are used to help the programmer to develop detailed procedures and processes required in the design of a computer program. Decision trees and decision tables use a network or a tabular form to document the complex conditional logic involved in choosing among the information processing alternatives in a system. Structure charts document the purpose, structure and hierarchical relationships of the modules in a program.

Question 17

Bring out the reasons as to why the organizations fail to achieve their Systems Development Objectives?

Answer

Following are some of the reasons due to which the organizations fail to achieve their system development objectives:

- (i) **Lack of senior management support for and involvement in information system development:** In the management of information systems, developers and users depend on the senior management for support and to determine which systems development projects are important. Their tendency is to shift away from the project, which lack senior management attention.
- (ii) **Shifting user needs:** User requirements for information technology are constantly varying. As these changes accelerate, there will be more requests for systems development and more development projects. When these changes occur during a development process, the development team may be faced with the challenge of developing systems whose very purposes have changed since the development process began.

Information Systems Control and Audit

- (iii) **Development of strategic systems:** Because strategic decision-making is unstructured, the requirements, specifications and objectives for such development projects are difficult to define and determining successful development will be elusive.
- (iv) **New technologies:** New technologies are coming in the organizations want to apply these and create a competitive situation. However, later they find that attaining systems development objectives is more difficult because personnel are not familiar with the new technology.
- (v) **Lack of standard project management and systems development methodologies:** Some organizations do not formalize their project management and systems development methodologies, thereby making it very difficult to consistently complete projects on time or within the budget.
- (vi) **Overworked or under-trained development staff:** It is generally established that there is backlog of systems development work due to lack of efficient staff. In addition to being overworked, system developers often lack sufficient educational background. Many companies do little to help their development personnel stay technically updated and in these organizations, a training plan and training budget do not exist.
- (vii) **Resistance to change:** People have a natural tendency to resist change, and information systems development projects signal changes –often radical – in the work place. Business process reengineering is often the catalyst for the systems development project. When personnel perceive that the project will result in personnel cutbacks, threatened personnel will dig in their heels, and the development project is doomed to failure. Personnel cutbacks often result when reengineering projects really attempt at downsizing (or right sizing).
- (viii) **Lack of user participation:** Users must participate in the development effort to define their requirements, feel ownership for project success, and work to resolve development problems. User-participation also helps reduce user resistance to change.
- (ix) **Inadequate testing and user training:** New systems must be tested before installation to determine that they will operate correctly. Users must be trained to effectively utilize the new system. By executing the system development process efficiently and effectively, the above problem can be solved.

Question 18

Write short notes on the following:

- (a) *Data Dictionary*
- (b) *System Development Life Cycle*

Answer

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

It has variety of uses. It serves as an aid to documentation and is also useful for securities. It helps accountants and auditors in establishing audit trails and in planning the flow of transaction data through the system. Finally, it serves as an important aid in investigating or documenting internal control procedures.

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

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

- (i) *Preliminary investigation:* It is undertaken when users come across a problem or opportunity and submit a formal request for a new system to the MIS department. This activity consists of three parts; request clarification, feasibility study and request approval.
- (ii) *Requirements analysis or systems analysis:* In this stage, the analysts work closely with employees and managers of the organization for determining the information requirements of the users. Several fact-finding techniques and tools such as questionnaires, interviews, observing decision-maker behaviour and office environment, etc. are used for understanding the requirements of the users. As details are gathered, the analysts study the present system to identify its problems and shortcomings and identify the features which the new system should include to satisfy the new or changed user application environment.

Information Systems Control and Audit

- (iii) *Design of the system*: It produces the details that state how a system will meet the requirements identified in the previous step. The analyst designs various reports/outputs, data entry procedures, inputs, files and database. He also selects file structures and data storage devices. These detailed design specifications are then passed on to the programming staff for software development.
- (iv) *Acquisition and development of software*: In this stage, resource requirements such as specific type of hardware, software and services are determined. Subsequently, choices are made regarding which products to buy or lease from which vendors. Software developers may modify and then install purchased software or they may write new custom designed programs.
- (v) *System testing*: Before the information system can be used, it must be tested. Special test data are input for processing, and results are examined. If it is found satisfactory, it is eventually tested with actual data from the current system.
- (vi) *Implementation and maintenance*: After system is found to be fit, it is implemented with actual data. After implementation, the system is maintained; it is modified to adapt to changing users and business needs.

Question19

Describe any five functional areas of a system which needs to be analyzed by system analyst for detailed investigation of the present system.

Answer

Analysis of the Present System - Detailed investigation of the present system involves collecting, organizing and evaluating facts about the system and the environment in which it operates. Survey of existing methods, procedures, data flow, outputs, files, input and internal controls should be intensive in order to fully understand the present system and its related problems. There are several functional areas, which should be studied in depth. We have discussed below five major functional areas:

- (i) **Analyze Inputs** – Source documents are used to capture the originating data for any type of the system. The system analyst should be aware of the various sources from where the data are initially captured. He must keep in view the fact that outputs for one area may serve as an input for another area. He must understand the nature of each form, what is contained in it, who prepared it, from where the form is initiated, where it is completed, the distribution of the form and other similar considerations to determine how these inputs fit into the framework of the present system.

- (ii) **Review data files** – The analyst should investigate the data files maintained by each department noting their number and size, where they are located, who uses them and the number of times per given time interval these are used. This information may be contained in the system and procedures manuals. He should also review all online and off-line files which are maintained in the organization as it will reveal information about data that are not contained in any output. The related cost of retrieving and processing the data is another important feature to be considered by the system analyst.
- (iii) **Review methods, procedures and data communication** – Methods and procedures transforms input data into useful output. A procedure review is an intensive survey of the methods by which each job is accomplished, the equipment utilized and the actual location of the operations. Its basic objective is to eliminate unnecessary tasks or to perceive improvement opportunities in the present information system. The analyst must review the types of data communication equipments including data interface, data link, modems, dial-up and leased lines and multiplexers. He must understand how the data communication network is used in the present system so as to identify the need to revamp the network when the new system is installed.
- (iv) **Analyze Outputs** - The outputs or reports should be scrutinized carefully by the system analyst in order to determine how well they will meet the organization's need. The analyst must understand what information is needed and why, who needs it and when and where it is needed. Additional questions concerning the sequence of the data, how often the form reporting it is used, how long it is kept on file etc. must be investigated. Often many reports are a carry-over from earlier days and have little relevance to current operations. Attempts should be made to eliminate all such reports in the new systems.
- (v) **Review internal controls** - A detailed investigation of the present information system is not complete until internal controls are reviewed. Locating the control points helps the analyst to visualize the essential parts and framework of a system. An examination of internal controls may indicate weaknesses that should be removed in the new system. The adoption of advanced methods, procedures and equipments might allow much greater control over the data.

Question 20

What are the various tangible and intangible benefits that can result from the development of a computerized system?

Information Systems Control and Audit

Answer

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

- (i) Increase in sales or profit (improvement in product or service quality)
- (ii) Decrease in data processing costs (elimination of unnecessary procedures and documents)
- (iii) Decrease in operating costs (reduction in inventory carrying costs)
- (iv) Decrease in required investment (decrease in inventory investment required)
- (v) Increased operational ability and efficiency (improvement in production ability and efficiency)
- (vi) New or improved information availability (more timely and accurate information and new types and forms of information)
- (vii) Improved abilities in computation and analysis
- (viii) Improved customer service (more timely service)
- (ix) Improved employee morale (elimination of burdensome and boring job tasks)
- (x) Improved management decision-making (better information and decision analysis)
- (xi) Improve competitive position (faster and better response to actions of competitors)
- (xii) Improved business and community image (progressive image as perceived by customers, investors etc.)

Intangible though, it is important to put a rupee and paise tag to each benefit for purposes of profit and loss statement. The analyst has to quantify the benefits in monetary terms.

Question 21

Write short note on top down approach of system development.

Answer

Top down Approach of system development: The top down approach assumes a high degree of top management involvement in the planning process and focuses on organizational goals, objectives and strategies. The logic here is that, above all, an information system needs to be responsive to and supportive of an organization's basic

reasons for being. Hence the organization's goals should be the driving force behind development of all the computer systems. Thus, using top down approach, we begin analyzing objectives and goals of the organization and end by specifying application programs and modules that are needed to be developed.

Various steps in top-down approach are as follows:

- (a) Analyze the objectives and goals of the organization in terms of profit, growth, diversification etc.
- (b) Identify the functions of the organization and explain how they support the entire organization.
- (c) Ascertain major activities, decisions and functions at various levels of hierarchy. It should be analyzed what decisions are made and what need to be made.
- (d) Identify models that guide managerial decision process and find the information requirements for activities and decisions.
- (e) Prepare specific information processing programs in detail and modules within these programs. Also identify files and database for applications.

Question 22

What are the project management items associated with an I.T. project system failures? Give the elements to be included in the adopted framework to avoid such failures.

Answer

Items associated with IT project system failure are as follows:

- (i) Underestimation of the time to complete the project.
- (ii) Senior management did not monitor the project closely enough.
- (iii) Underestimation of necessary resources.
- (iv) Size and scope of the project underestimated.
- (v) Inadequate project control mechanism.
- (vi) Systems specifications kept changing.
- (vii) Inadequate planning.

Elements to be included in the framework to avoid such failures are as stated below:

- (i) User participation in defining and authorizing the system.
- (ii) Assignment of appropriate staff to the system development and definition of their responsibilities and authorities.

Information Systems Control and Audit

- (iii) A clear written statement of system nature and scope.
- (iv) A feasibility study that is the basis of senior management approval to proceed with the system.
- (v) A system master plan, including realistic time and cost estimates for control of the system.
- (vi) A risk management program to identify and manage risks associated with each project.
- (vii) Division of the system into manageable processes often called phases.
- (viii) Approval of work accomplished in one phase before working on the next phase.
- (ix) Integration of the quality assurance plan including the systems development cycle (SDLC) methodology with the system master plan.

Project management, particularly the planning process and establishing the project schedule can ultimately determine the success of the project.

Question 23

Various software packages serve as aids in analysis of program logic. Explain briefly.

Answer

The following software packages serve as aids in program analysis:

- **Automated flowcharting programs**, which interpret program source code and generate a corresponding program flowchart.
- **Automated decision table programs**, which generate a decision table representing the program logic.
- **Scanning routines**, which search a program for occurrences of a specified variable name or other character combinations.
- **Mapping programs**, which identify unexecuted program code. This software could have uncovered the program code that is developed by the unscrupulous programmer who has inserted code to erase all computer files when he was terminated.
- **Program tracing**, which sequentially prints all application program steps (line numbers or paragraph names) executed during a program run. This list is intermingled with regular output so that the auditors can observe the precise sequence of events that unfold during program execution. Program tracing helps auditors to detect unauthorized program instructions, incorrect logic paths, and unexecuted program code.

Question 24

Explain different conversion strategies used for conversion from manual to computerized system. Enumerate the advantages and disadvantages of each strategy.

Answer

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

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

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

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

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

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

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

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

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

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

- (iv) **Modular Prototype Conversion:** This approach of conversion uses the building of

Information Systems Control and Audit

modular, operational prototypes to change from old system to new in a gradual manner. As each module is modified and accepted, it is put into use.

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

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

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

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

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

Question 25

Discuss briefly, various activities that are involved for successful conversion of an existing manual system to a computerized information system.

Answer

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

1. Procedure conversion;
 2. File conversion;
 3. System conversion;
 4. Scheduling personnel and equipment;
 5. Alternative plans in case of equipment failure
1. **Procedure conversion:** Operating procedures should be completely documented for the new system. This applies to both computer operations and functional area operations. Before any parallel or conversion activities can start, operating procedures must be clearly spelled out for personnel in the functional areas undergoing changes. Information on input, data files, methods, procedures,

outputs, and internal controls must be presented in clear, concise and understandable terms for the average reader. Written operating procedures must be supplemented by oral communication during the training sessions on the system change. Brief meetings must be held when changes are taking place in order to inform all operating employees of any changes initiated. Revisions to operating procedures should be issued as quickly as possible. These efforts enhance the chances of successful conversion.

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

2. **File conversion:** Because large files of information must be converted from one medium to another, this phase should be started long before programming and testing are completed. The cost and related problems of file conversion are significant whether they involve on-line files (common data base) or off-line files. Present manual files are likely to be inaccurate and incomplete where deviations from the accepted formats are common. Computer generated files tend to be more accurate and consistent.

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

3. **System conversion:** After on-line and off-line files have been converted and the reliability of the new system has been confirmed for a functional area, daily processing can be shifted from the existing information system to the new one. A cut-off point is established so that data base and other data requirements can be updated to the cut-off point. All transactions initiated after this time are processed on the new system. System development team members should be present to assist and to answer any questions that might develop. Consideration should be given to operating the old system for some more time to permit checking and balancing the total results of both systems. All differences must be reconciled. If necessary, appropriate changes are made to the new system and its computer programs. The old system can be dropped as soon as the data processing group is satisfied with the new system's performance.
4. **Scheduling personnel and equipment:** Scheduling data processing operations of a new information system for the first time is a difficult task for the system

Information Systems Control and Audit

manager. As users become more familiar with the new system, however, the job becomes more routine.

Before the new design project is complete, it is often necessary to schedule the new equipment. Some programs will be operational while others will be in various stages of compiling and testing. Since production runs tend to push aside new program testing, the system manager must assign ample time for all individuals involved. Schedules should be set up by the system manager in conduction with departmental managers of operational units serviced by the equipment.

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

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

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

Question 26

ABC Technologies Ltd. is in the development of application software for various domains. For the development purposes, the company is committed to follow the best practices suggested by SDLC. SDLC provides the guidelines to follow a sequence of activities. It consists of a set of steps and phases in which each phase of the SDLC uses the results of the previous one. The SDLC is document driven which means that at crucial stages during the process, documentation is produced. A phase of the SDLC is not complete until the appropriate documentation or artifact is produced. These are sometimes referred to as deliverables.

A deliverable may be a substantial written document, a software artifact, a system test plan or even a physical object such as a new piece of technology that has been ordered and delivered. This feature of the SDLC is critical to the successful management of an IS project.

Read the above carefully and answer the following:

- (a) List the possible advantages from the perspective of IS Audit.*
- (b) There are various advantages by following SDLC, but there are some shortcomings also. Briefly explain those shortcomings.*
- (c) Feasibility study is a key activity in the SDLC. What are the issues which are typically considered in the Feasibility Study?*
- (d) In the SDLC, at the end of the analysis phase, the system analyst prepares a document called 'Systems Requirements Specifications (SRS)'. Briefly explain the contents of a SRS.*

Answer

- (a)** From the perspective of the IS Audit, the following are the possible advantages:
 - The IS auditor can have clear understanding of the various phases of the SDLC on the basis of the detailed documentation created during each phase of the SDLC.
 - The IS Auditor on the basis of his examination, can state in his report about the compliance by the IS management of the procedures, if any, set by the management.
 - The IS Auditor, if has a technical knowledge and ability of the area of SDLC, can be a guide during the various phases of SDLC.
 - The IS auditor can provide an evaluation of the methods and techniques used through the various development phases of the SDLC.
- (b)** Some of the shortcomings of the SDLC are as follows:
 - The development team may find it cumbersome.
 - The users may find that the end product is not visible for a long time.
 - The rigidity of the approach may prolong the duration of many projects.
 - IT may not be suitable for small and medium sized projects.
- (c)** The following issues are typically addressed in the Feasibility Study:
 - Determine whether the solution is as per the business strategy.
 - Determine whether the existing system can rectify the situation without a major modification.
 - Define the time frame for which the solution is required.
 - Determine the approximate cost to develop the system.
 - Determine whether the vendor product offers a solution to the problem.

Information Systems Control and Audit

(d) A SRS contains the following:

- **Introduction:** Goals and Objectives of the software context of the computer-based system; Information description.
- **Information Description:** Problem description; Information content, flow and structure; Hardware, software, human interfaces for external system elements and internal software functions.
- **Functional Description:** Diagrammatic representation of functions; Processing narrative for each function; Interplay among functions; Design constraints.
- **Behavioral Description:** Response to external events and internal controls.
- **Validation Criteria:** Classes of tests to be performed to validate functions, performance and constraints.
- **Appendix:** Data flow / Object Diagrams; Tabular Data; Detailed description of algorithms charts, graphs and other such material.
- **SRS Review:** It contains the following :
 - o The development team makes a presentation and then hands over the SRS document to be reviewed by the user or customer.
 - o The review reflects the development team's understanding of the existing processes. Only after ensuring that the document represents existing processes accurately, should the user sign the document. This is a technical requirement of the contract between users and development team / organization.

EXERCISE**Question 1**

What is prototyping approaches to systems development? Describe its advantages and disadvantages also.

Question 2

Write short notes on the following:

- (a) End user development approach in system development*
- (b) Program documentation*

Question 3

State main objectives of system development tools. Briefly describe the major categories of documentation tools that are used for system development with any one simple illustrative example for each.

Question 4

What are the major factors to be considered in designing User inputs? Explain.

Question 5

What are the six important factors which should be considered while designing the user outputs?

Question 6

What are the factors considered to design the ideal layout of a printed output?

Question 7

Read the data flow and activities listed in the table below carefully and draw the data flow diagram for the payroll processing system.

Activities	Data Inputs	Data Outputs
Update employee/roll file	New employee form Employee change form Employee/payroll file	Updated employee/ payroll file
Pay employees	Time cards Employee/ payroll file Tax tables	Employee cheques Payroll register Updated employee/payroll file Payroll cheques

Information Systems Control and Audit

		<i>Payroll cash disbursements voucher</i>
<i>Prepare reports</i>	<i>Employee/ payroll file</i>	<i>Payroll report</i>
<i>Update general ledger</i>	<i>Payroll tax cash Disbursements voucher Payroll cash Disbursements voucher</i>	<i>Updated general ledger</i>

Question 8

As a system analyst, you need to assess the successful implementation and stakeholder's actual requirements of an enterprise system in a retail chain organization across its branches to provide the following features:

- Lower operational costs,
- Better information for managers, and
- Smooth operations for users or better levels of service to customers.

Justify your answer with the necessary techniques used to determine the requirements of a system.

Question 9

Answer in brief the important factors the system analysts should consider while application prototyping to develop display screen output to allow users to react to both the content and form of the output.

Question 10

*What are the cost elements that need to be considered for cost estimate of a system?
What are the major benefits that a system can provide?*

Question 11

Discuss the system development approach whose components are time boxing, incremental prototyping and clean rooms.

Question 12

State the five strategies of conversion from an existing manual system to the new computerized system.

Question 13

Write short notes on the following:

- (a) *Guidelines for input form design,*
- (b) *Factors for validation of vendor's proposals, and*
- (c) *Point-Scoring Analysis.*

Question 14

As an internal IS Auditor of an enterprise which is undergoing the phase of system acquisition, how will you prepare the checklists for the following:

- (a) *Evaluation and validation of the software package to be acquired,*
- (b) *The support service to be given by the vendor, and*
- (c) *Evaluation of the Software License Agreement (SLA).*

Question 15

An organization is in the stage of systems development to implement an enterprise wide information system, where the following conditions exist:

End users are not aware of the information needs.

The new system is mission critical and there is a hasty need.

The business risks associated in implementing the wrong system are high.

Read the above case carefully and answer the following with proper justification/s:

- (a) *Identify the system development approach and the steps to be followed in the above stated conditions.*
- (b) *State the reasons for choosing the particular approach for system development.*
- (c) *Identify the risks, when end-users are involved in the system development process.*

Question 16

Write a short note on System maintenance.

CONTROL OBJECTIVES

BASIC CONCEPTS

1. **Effect of Computers on Internal Audit**
 - 1.1 **Changes in the audit and audit evidence:** Data retention and storage, Absence of input documents, Lack of visible audit trail, Lack of visible output, Audit evidence, Legal Issues
 - 1.2 **Change in the type and nature of internal controls:** Personnel, Segregation of duties, Authorization procedures, Record keeping, Access to assets and records, Management supervision and review
 - 1.3 **New causes and sources of error:** System generated transactions, Systematic error
 - 1.4 **New Audit Processes**
2. **Control Objectives for Information Related Technology (COBIT):** The framework addresses the issue of control from three points or dimensions: Business Objectives, IT Resources, IT Processes
3. **Information Systems Control Techniques:** Accounting Controls, Operational Controls, and Administrative Controls
 - 3.1 **Auditor's Categorization of Controls:** These controls are categorized into four groups: Preventive Controls, Detective Controls, Corrective Controls, and Compensatory Controls
 - 3.2 **Audit Trail Objectives:** Audit trails can be used to support security objectives in three ways: detecting Unauthorized Access, Reconstructing Events, and Personal Accountability
4. **System Development and Acquisition Controls:** It includes the following key elements: Strategic master plan, Project controls, Data processing schedule, System performance measurements, Post implementation review
5. **Controls over system implementation:** Acceptance Testing, Volume Testing, Stress Testing, Security Testing, Clerical procedures checking, Back-up and recovery, Parallel operation

Information Systems Control and Audit

6. **Information Classification:** Top Secret, Highly Confidential, Proprietary, Internal Use only, Public Documents
7. **Data Integrity Controls:** Source data control, Input validation routines, On-line data entry controls, Data processing and storage controls, Output Controls, Data transmission controls
8. **Issues and revelations related with Logical Access**
 - 8.1 **Technical Exposures:** Data Diddling, bombs, Trojan Horse, Worms, Rounding Down, Salami Techniques
 - 8.2 **Asynchronous Attacks:** Data Leakage, Wire tapping, Piggybacking, Shut down of the Computer/ Denial of Service
 - 8.3 **Computer Crime Exposures:** Financial Loss, Legal Repercussions, Loss of Credibility or Competitive Edge, Blackmail/Industrial Espionage, Disclosure of Confidential, sensitive or Embarrassing information, spoofing and Sabotage
9. **Physical Access Controls**
 - 9.1 **Locks on doors:** Cipher locks, Bolting Door Locks, Electronic Door Locks, and Biometric Door Locks
 - 9.2 **Physical Identification Medium:** Personal Identification Number (PIN), Plastic Cards, Cryptographic Control, and Identification Badges
 - 9.3 **Logging on utilities:** Manual logging, and Electronic Logging
 - 9.4 **Other means of controlling Physical Access:** Video Cameras, Security Guards, Controlled Visitor Access, Bonded Personnel, Dead man doors, Non-exposure of sensitive facilities, Computer terminal locks, Controlled Single Entry Point, Alarm System, Perimeter Fencing, Control of out of hours of employee/s, and Secured Report/ Document Distribution Cart
10. **Environmental Controls**
 - 10.1 **Controls for Environmental Exposures:** Water Detectors, Hand-held Fire extinguishers, Manual Fire Alarms, Smoke detectors, Fire Suppression Systems, Strategically Locating the Computer room, Regular Inspection by Fire department, Fireproof Walls, Floors and Ceiling surrounding the computer room, Electrical Surge Protectors, UPS/Generator, Power leads from two substations, Emergency Power-off switch, Wiring placed in electrical panels and conduit, Prohibitions against eating, drinking and smoking within the information processing facility, Fire resistant office materials, and Documented and tested emergency evacuation plans

10.2 Audit and Evaluation Techniques for Environmental Controls: Water and smoke detectors, Hand-held Fire Extinguishers, Fire Suppressions Systems, regular Inspection by Fire Department, Fireproof Walls, Floors and Ceiling Surroundings the Computer Room, Electrical Surge Protectors, Power leads from two stations, Fully documented and Tested Business Continuity Plan, Wiring Placed in Electrical Panels and Conduit, documented and tested Emergency Evacuation Plans, and Humidity/Temperature Control

11. Security Concepts and Techniques

11.1 Cryptosystems: A cryptosystem refers to a suite of algorithms needed to implement a particular form of encryption and decryption.

11.2 Data Encryption Standard (DES): The DES is a cipher (a method for encrypting information) selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976, and which has subsequently widespread use internationally.

11.3 Public Key Infrastructure (PKI): 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 users' identity.

11.4 Firewalls: A firewall is a collection of components (computers, routers, and software) that mediate access between different security domains. These are of four types: Packet Filter Firewalls, Stateful Inspection Firewalls, Proxy Server Firewalls, and Application Level Firewalls

12. Intrusion Detection: This is the attempt to monitor and possibly prevent attempts to intrude into or otherwise compromise the system and network resources of an organization. It falls into two broad categories: Network based systems, and Host based systems.

13. Hacking: This is an act of penetrating computer systems to gain knowledge about the system and 'how it works'. There are many ways in which a hacker can hack: NetBIOS, ICMP Ping, FTP, RPC statd, HTTP.

14. Virus: A virus is a program (usually destructive) that attaches itself to a legitimate program to penetrate the operating system.

14.1 Anti-Virus Software: There are three types of anti-virus software: Scanners, Active Monitor and Heuristic Scanner, and Integrity Checkers

Information Systems Control and Audit

Question 1

What do you understand by classification of information? Explain different classifications of information.

Answer

Information classification does not follow any predefined rules. It is a conscious decision to assign a certain sensitivity level to information that is being created, amended, updated, stored, or transmitted. The sensitivity level depends upon the nature of business in an organization and the market influence.

The classification of information further determines the level of control and security requirements. Classification of information is essential to understand and differentiate between the value of an asset and its sensitivity and confidentiality. When data is stored, whether received, created or amended, it should always be classified into an appropriate sensitivity level to ensure adequate security.

For many organizations, a very simple classification criteria is as follows:

Top Secret: The information is classified as Top Secret/ confidential that can cause serious damage to the organization if lost or made public. Information relating to pending mergers or acquisitions; investment strategies; plans or designs etc. is highly sensitive. Many restrictions are imposed on the usage of such information and is protected at the highest level of security possible.

Highly Confidential: This class of information, is considered critical for the ongoing business operations and can cause serious impediment, if shared around the organization e.g. sensitive customer information of bank's, solicitors and accountants etc., patient's medical records and similar highly sensitive data. It should not be copied or removed without the consent of appropriate authority and must be kept under operational vigilance. Security at this level should be very high.

Proprietary: Information relating to Procedures, operational work routines, project plans, designs and specifications are of propriety in nature. Such information is for proprietary use to authorized personnel only. Security at this level is high.

Internal Use only: This class of information cannot be circulated outside the organization where its loss would inconvenience the organization or management but disclosure is unlikely to result in financial loss or serious damage to credibility. Internal memos, minutes of meetings, internal project reports are examples of such information. Security at this level is controlled but normal.

Public Documents: This Information is published in the public domain; annual reports, press statements etc.; which has been approved for public use. Security at this level is minimal.

Question 2

Briefly explain the formal change management policies, and procedures to have control over system and program changes.

Answer

Formal change management control policies and procedure for system and program changes include the following:

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

Update all documentation and procedures when changes are implemented.

Information Systems Control and Audit

Question 3

Write short notes on the following:

- (a) *Key elements in System Development and Acquisition Control*
- (b) *Firewalls*

Answer

- (a) **Key elements in System Development and Acquisition Control:** It is important to have a formal, appropriate, and proven methodology to govern the development, acquisition, implementation, and maintenance of information systems and related technologies. Methodology should contain appropriate controls for management review and approval, user involvement, analysis, design, testing, implementation, and conversion.

Key elements in system Development and acquisition controls and given in following table:

Control Category	Threats/Risks	Controls
System development and acquisition controls	System development projects consume excessive resources.	Long-range strategic master plan, data processing schedules, assignment of each project to manage team, project development plan, project milestones, performance evaluations, system performance measurements.
Change management controls	Systems development projects consume excessive resources, unauthorised systems changes.	Change management control policies and procedures, periodic review of all systems for needed changes, standardized format for changes, log and review change requests, assess impact of changes on system reliability, categorise and rank all, changes, procedures to handle urgent matters, communicate changes to management and users, management approval of changes, assign specific responsibilities while maintaining adequate segregation of duties etc.

- (b) **Firewall:** 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 system (IDSs).

There are four primary firewall types from which to choose: packet filtering, stateful inspection, proxy servers, and application-level firewalls. Any product may have characteristics of one or more firewall types. The selection of firewall type is dependent on many characteristics of the security zone, such as the amount of traffic, the sensitivity of the systems and data, and applications. Additionally, consideration should be given to the ease of firewall administration, degree of firewall monitoring support through automated logging and log analysis, and the capability to provide alerts for abnormal activity.

Typically, firewalls block or allow traffic based on rules configured by the administrator. Rule sets can be static or dynamic. A static rule set is an unchanging statement to be applied to packet header, such as blocking all incoming traffic with certain source addresses. A dynamic rule set often is the result of coordinating a firewall and an IDS. For example, an IDS that alerts on malicious activity may send a message to the firewall to block the incoming IP address. The firewall, after ensuring that the IP is not on a "white list", creates a rule to block the IP. After a specified period of time the rule expires and traffic is once again allowed from that IP.

Firewalls are subject to failure. When firewalls fail, they typically should fail closed, blocking all traffic, rather than failing open and allowing all traffic to pass. Firewalls provide some additional services such as network address translation, dynamic host configuration protocols and virtual private network gateways.

Question 4

"While reviewing a client's control system, an information system auditor will identify three components of internal control." State and briefly explain these three components.

Answer

The basic purpose of information system controls in an organization is to ensure that the business objectives are achieved and undesired risk events are prevented or detected and corrected. This is achieved by designing an effective information control framework, which comprises of policies, procedures, practices, and organization structure to give reasonable assurances that the business objectives will be achieved.

Information Systems Control and Audit

While reviewing a client's control systems, the auditor will be able to identify three components of internal controls. Each component is aimed at achieving different objectives as stated below:

- (i) Accounting Controls: These controls are extended to safeguard the client's assets and ensure reliability of financial records.
- (ii) Operational Controls: These deals with the day to day operations, functions and activities to ensure that the operational activities are contributing to business objectives.
- (iii) Administrative Control: These are concerned with ensuring efficiency and compliance with management policies, including the operational controls.

Question 5

A company is engaged in the stores taking data activities. Whenever, input data error occurs, the entire stock data is to be reprocessed at a cost of Rs. 50,000. The management has decided to introduce a data validation step that would reduce errors from 12% to 0.5% at a cost of Rs. 2,000 per stock taking period. The time taken for validation causes an additional cost of Rs. 200. (i) Evaluate the percentage of cost-benefit effectiveness of the decision taken by the management and (ii) suggest preventive control measures to avoid errors for improvement.

Answer

- (i) The percentage of cost benefit effectiveness based on the information is calculated in the following table:

S. No.	Particulars	Without validation Procedure	With Validation Procedure
1.	Cost of reprocessing the stock data	Rs. 50,000	Rs. 50,000
2.	Risk of data errors	12%	0.5%
3.	Expected processing cost	Rs. 6,000	Rs. 250
4.	Cost of validation procedure	Nil	Rs. 2,000
5.	Cost of delay due to validation	Nil	Rs. 200
6.	Total cost involved	Rs. 56,000	Rs. 52,450
7.	Net expected benefit in %		Rs. 3,550 6.3%

Hence there is 6.3% cost benefit effectiveness of the decision taken by the management.

(ii) Preventive Control Measures

Preventive controls are those inputs, which are designed to prevent an error, omission or malicious act occurring. An example of a preventive control is the use of passwords to gain access to a financial system. The broad characteristics of preventive controls are:

- (i) A clear-cut understanding about the vulnerabilities of the asset.
- (ii) Understanding probable threats.
- (iii) Provision of necessary controls for probable threats from materializing.

Any control can be implemented in both manual and computerized environment for the same purpose. Only the implementation methodology may differ from one environment to the other.

Some of the major preventive controls to avoid errors are as follows:

- Employ qualified personnel
- Segregation of duty
- Access controls
- Vaccination against disease
- Maintain proper documentation
- Prescribing appropriate books for a course
- Training and retraining of personnel
- Authorization of transactions
- Validation, edit checks in the application programs
- Firewalls
- Anti-virus software
- Passwords

The above list in no way is exhaustive, but is a mix of manual and computerized preventive controls. The following table enumerates the kind of manual controls and computerized controls applied to a similar scenario.

Scenario	Manual Control	Computerized Control
Restrict unauthorized entry into the premises	Build a gate and post a security guard.	Use access control software, smart card, biometrics, etc.

Information Systems Control and Audit

Restricted unauthorized entry into the software applications	Keep the computer in a secured location and allow only authorized person to use the applications.	Use access control, viz. User ID, password, smart card, etc.
--	---	--

Table-2: Manual & Computerized Controls

Question 6

What are the issues that should be considered by a system auditor at post implementation review stage before preparing the audit report?

Answer

An auditor will consider following issues at PIR (Post Implementation Review) stage before preparing the audit report:

- (i) Interview business users in each functional area covered by the system, and assess their satisfaction with, and overall use of, the system.
- (ii) Interview security, operations and maintenance staff and, within the context of their particular responsibilities, assess their reactions to the system.
- (iii) Based on the User Requirements Specification, determine whether the system's requirements have been met. Identify the reasons(s) why any requirements are not to be provided, are yet to be delivered, or which do not work properly.
- (iv) Confirm that the previous system has been de-commissioned or establish the reasons(s) why it remains in use.
- (v) Review system problem reports and change proposals to establish the number and nature (routine, significant, major) of problems, and changes being made to remedy them. The volume of system change activity can provide an indicator of the quality of systems development.
- (vi) Confirm that adequate internal controls have been built into the system, that these are adequately documented, and that they are being operated correctly. Review the number and nature of internal control rejections to determine whether there are any underlying system design weaknesses.
- (vii) Confirm that an adequate Service Level Agreement has been drawn up and implemented. Identify and report on any area where service delivery either falls below the level specified, or is inadequate in terms of what was specified.
- (viii) Confirm that the system is being backed up in accordance with user requirements, and that it has been successfully restored from backup media.

- (ix) Review the Business Case and determine whether:
- anticipate benefits have / are been achieved;
 - any unplanned benefits have been identified;
 - costs are in line with those estimated;
 - benefits and costs are falling with the anticipated time-frame.
- (x) Review trends in transaction throughput and growth in storage use to identify that the anticipated growth of the system is in line with the forecast.

Question 7

Explain the term “Cryptosystems”. Briefly discuss Data Encryption Standard.

Answer

Cryptosystems: A cryptosystem refers to a suite of algorithms needed to implement a particular form of encryption and decryption. Typically, it consists of following three algorithms:

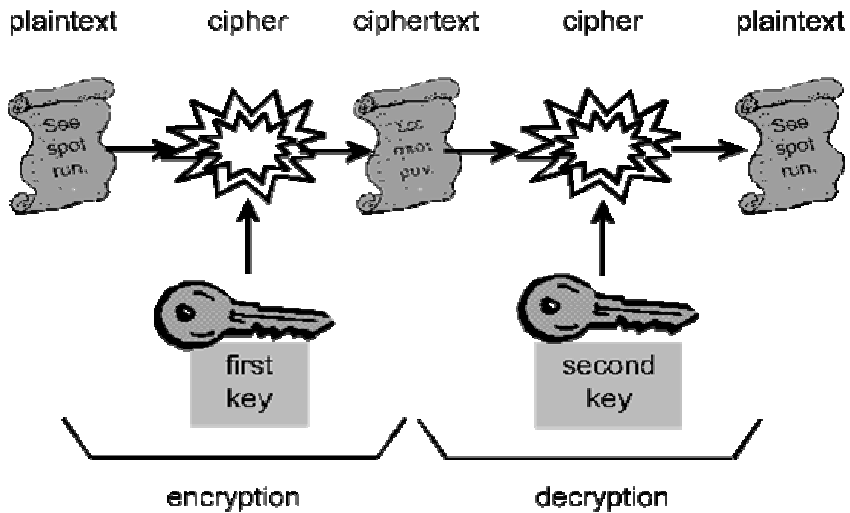
- Key Generation Algorithm,
- Encryption Algorithm and
- Decryption Algorithm.

The pair of algorithms of Encryption and Decryption is referred as Cipher or Cipher.

Data Encryption Standard (DES): It is a cipher. It is a mathematical algorithm for encrypting and decrypting binary coded information. Encrypting of data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. Encryption and Decryption operations are done by using a binary number called a key. A key consists of 64(bits) binary digits. Among these 64 bits, 56 bits are used for encryption/decryption and remaining 8 bits are used for error detection. Authorized users of the encrypted data must have the unique key that was used to encipher the data in order to decrypt it. Selection of a different key causes the cipher that is produced for any given set of inputs to be different. The cryptographic security of the data depends on the security provided for the key used to encipher and decipher the data. A standard algorithm based on a secure key thus provides a basis for exchanging encrypted computer data by issuing the key used to encipher it to those authorized to have the data.

Information Systems Control and Audit

The encryption and decryption processes are depicted in the following diagram:



Some documentation distinguishes DES from its algorithms. It refers algorithms as *DEA* (*Data Encryption Algorithm*).

Question 8

Discuss the three processes of Access Control Mechanism, when an user requests for resources.

Answer

Access control mechanism processes the user request for resources in three steps. They are:

- Identification
- Authentication
- Authorization

The access control mechanisms operate in the following sequence:

1. The users have to identify themselves, thereby indicating their intent to request the usage of system resources,
2. The users must authenticate themselves and the mechanism must authenticate itself, and
3. The users request for specific resources, their need for those resources and their areas of usage of these resources.

The mechanism accesses

- (a) previously stored information about users,
- (b) the resources they can access, and
- (c) the action privileges they have with respect to these resources.

The mechanism verifies this information against the user entries and it then permits or denies the request.

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

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

- *Ticket oriented:* In this approach the access control mechanism assigns the users a ticket for each resource they are permitted to access. Ticket oriented approach operates via a row in the matrix. Each row along with the user resources holds the action privileges specific to that user
- *List oriented:* In this approach, the mechanism associates with each resource a list of users who can access the resource and the action privileges that each user has with respect to the resource.

Question 9

Discuss anti-virus software and its types.

Answer

Anti-virus Software: It is a program that is used to detect viruses, and prevent their further propagation and harm.

Three types of anti-virus software are briefly discussed below:

Scanners: Scanners for a sequence of bits called virus signatures that are characteristic of virus codes. They check memory, disk boot sectors, executables and systems files to find matching bit patterns. As new viruses emerge frequently, it is necessary to frequently update the scanners with the data on virus code patterns for the scanners to be reasonably effective.

Information Systems Control and Audit

Active Monitor and Heuristic Scanner: This looks for critical interrupt calls and critical operating systems functions such as OS calls and BIOS calls, which resemble virus action.

Integrity Checkers: These can detect any unauthorized changes to files on the system. These can detect any unauthorized changes to the files on the system. The software performs a “take stock” of all files resident on the system and computes a binary check data called the Cyclic Redundancy Check (CRC). When a program is called for execution, the software computes the CRC again and checks with the parameter stored on the disk.

Question 10

Discuss Audit and Evaluation techniques for Physical access.

Answer

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.

Question 11

Describe various types of firewalls in brief.

Answer

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:

- 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.
- 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.
- 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

Information Systems Control and Audit

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.

Question 12

What is data privacy? Explain the major techniques to address privacy protection for IT systems.

Answer

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.

Question 13

Describe any three ways in which a hacker can hack the system.

Answer

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.

Information Systems Control and Audit

- **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.

Question 14

Explain the role of IS Auditor with respect to quality control of systems.

Answer

IS Auditor's Role: In case, the auditor intends to carry out detailed reviews of, for example, logical design, it will probably be necessary either to employ expert assistance, or to undertake training in the particular technical skills required.

The following are the general questions that the IS Auditor needs to consider for quality control:

- (a) does system design follow a defined and acceptable standard?
- (b) are completed designs discussed and agreed with the users?
- (c) does the project's quality assurance procedures ensure that project documentation is reviewed against the organization's technical standards and policies, and the user requirements specification.
- (d) do quality reviews follow a defined and acceptable standard?
- (e) are quality reviews carried out under the direction of a technically competent person who is managerially independent from the design team;

- (f) are auditors/security staff invited to comment on the internal control aspects of system designs and development specifications?
 - (g) are statistics of defects uncovered during quality reviews and other forms of quality control maintained and analyzed for trends? Is the outcome of trend analysis fed back into the project to improve the quality of other deliverables?
 - (h) are defects uncovered during quality reviews always corrected?
 - (i) does the production of development specifications also include the production of relevant acceptance criteria?
 - (j) has a configuration manager been appointed? Has the configuration management role been adequately defined?
 - (k) are all configuration items (hardware, software, documentation) that have passed quality review been placed under configuration management and version control?
 - (l) has sufficient IT been provided to assist with the configuration management task?
 - (m) are effective procedures in place for recording, analyzing and reporting failures uncovered during testing?
 - (n) are effective change management procedures in place to control changes to configuration items?
 - (o) has a Training Plan been developed and quality reviewed? Has sufficient time and resources been allocated to its delivery?
 - (p) has a system installation plan been developed and quality reviewed?
 - (q) has an acceptance testing plan been drawn up? Is it to an acceptable standard? Does it cover all aspects of the user requirements specification?
 - (r) does the acceptance test plan clearly allocate roles and responsibilities for undertaking and reviewing the results of acceptance testing?
 - (s) has the acceptance test plan been discussed with, and signed off by the prospective system owner?
 - (t) is the system development environment regularly backed up with copies of backed up configuration item held securely at a remote location?
 - (u) has the development environment been recovered from backup media?
 - (v) are contingency plans commensurate with the criticality of the project.
 - (w) do regular project board meetings take place to review project progress against budget and deadline?
 - (x) is the Business Case regularly updated to ensure that the project remains viable?
-

Information Systems Control and Audit

Question 15

Write short notes on the following:

- (i) *Locks on Doors with respect to physical access control*
- (ii) *Data encryption standard*
- (iii) *Hacking*

Answer

- (i) **Locks on Doors:** Different types of locks on doors for physical security are discussed below:

Cipher Locks (combination Door Locks): The Cipher Lock consists of a pushbutton panel that is mounted near the door outside of a secured area. There are ten numbered buttons on the panel. To enter, a person presses a four digit number sequence, and the door will unlock for a predetermined period of time, usually ten to thirty seconds.

Cipher Locks are used in low security situations or when a large number of entrances and exits must be usable all the time. More sophisticated and expensive cipher locks can be computer coded with a person's handprint. A matching handprint unlocks the door.

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

Electronic Door Locks: A magnetic or embedded chip based plastics card key or token may be entered into a sensor reader to gain access in these systems. The sensor device upon reading the special code that is internally stored within the card activates the door locking mechanism.

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

- (ii) **Data Encryption Standard (DES):** It is a Cipher (a method for encrypting information) selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976, and which has subsequently enjoyed widespread use internationally. It is a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key. A key consists of 64 binary digits ('0's or

'1's) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits which are not used by the algorithm are used for error detection. The 8 error detecting bits are set to make the parity of each 8 bits byte of the key odd, i.e. there is an odd number of "1" in each 8-bits byte.

- (iii) **Hacking:** It is an act of penetrating computer systems to gain knowledge about the system and how it works. Technically, a hacker is someone who is enthusiastic about computer programming and all things relating to the technical workings of a computer.

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

There are many ways in which a hacker can hack. These are:

- ◆ Net BIOS
- ◆ ICMP Ping
- ◆ FTP
- ◆ rpc. statd
- ◆ HTTP.

Question 16

Discuss the role of IS auditor with respect to

- (a) *Physical access controls*
(b) *Environmental controls.*

Answer

- (a) **Role of IS Auditor in Physical Access Controls:** Auditing Physical Access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls. This involves the following:
- (i) **Risk Assessment:** The auditor must satisfy himself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures there from.
 - (ii) **Controls Assessment:** The auditor based on the risk profile evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks.
-

Information Systems Control and Audit

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

(iv) **Testing of Controls:** The auditor should review physical access controls to satisfy for their effectiveness. This involves:

- ◆ Tour of organizational facilities including outsourced and offsite facilities.
- ◆ Physical inventory of computing equipment and supporting infrastructure.
- ◆ Interviewing personnel can also provide information on the awareness and knowledge of procedures.
- ◆ Observation of safeguards and physical access procedures. This would also include inspection of:
 - (i) Core computing facilities.
 - (ii) Computer storage rooms.
 - (iii) Communication closets.
 - (iv) Backup and off site facilities.
 - (v) Printer rooms.
 - (vi) Disposal yards and bins.
 - (vii) Inventory of supplies and consumables.
- ◆ Review of physical access procedures including user registration and authorization, authorization for special access, logging, review, supervision etc. Employee termination procedures should provide withdrawal of rights such as retrieval of physical devices like smart cards, access tokens, deactivation of access rights and its appropriate communication to relevant constituents in the organization.
- ◆ Examination of physical access logs and reports. This includes examination of incident reporting logs and problem resolution reports.

(b) **Role of Auditor in Environment Controls:** The attack on the World Trade Centre in 2001 has created a worldwide alert bringing focus on business continuity planning and environmental controls. Audit of environment controls should form a critical part of every IS audit plan. The IS auditor should satisfy not only the effectiveness of various technical controls but that the overall controls assure safeguarding the business against environmental risks. Some of the critical audit

considerations that an IS auditor should take into account while conducting his audit are given below:

Audit Planning and Assessment: As part of risk assessment:

- ◆ The risk profile should include the different kinds of environmental risks that the organization is exposed to. These should comprise both natural and man-made threats. The profile should be periodically reviewed to ensure updation with newer risk that may arise.
- ◆ The controls assessment must ascertain that controls safeguard the organization against all acceptable risks including probable ones and are in place.
- ◆ The security policy of the organization should be reviewed to access policies and procedures that safeguard the organization against environmental risks.
- ◆ Building plans and wiring plans need to be reviewed to determine the appropriateness of location of IPF, review of surroundings, power and cable wiring etc.
- ◆ The IS Auditor should interview relevant personnel to satisfy himself about employees' awareness of environmental threats and controls, role of the interviewee in environmental control procedures such as prohibited activities in IPF, incident handling, and evacuation procedures to determine if adequate incident reporting procedures exist.
- ◆ Administrative procedures such as preventive maintenance plans and their implementation, incident reporting and handling procedures, inspection and testing plan and procedures need to be reviewed.

Audit of Technical Controls: Audit of environmental controls requires the IS Auditor to conduct physical inspections and observe practices. S/he must verify:

- ◆ The IPF and the construction with regard to the type of materials used for construction.
- ◆ The presence of water and smoke detectors, power supply arrangements to such devices, and testing logs.
- ◆ The location of fire extinguishers, fire fighting equipment and refilling date of fire extinguishers.
- ◆ Emergency procedures, evacuation plans and making of fire exists. If necessary, the IS Auditor may also use a mock drill to test the preparedness with respect to disaster.

Information Systems Control and Audit

- ◆ Documents for compliance with legal and regulatory requirements with regard to fire safety equipment, external inspection certificate and shortcomings pointed out by other inspectors / auditors.
- ◆ Power sources and conduct tests to assure the quality of power, effectiveness of the power conditioning equipment and generators. Also the power supply interruptions must be checked to test the effectiveness of the back-up power.
- ◆ Environmental control equipment such as air-conditioning, dehumidifiers, heaters, ionizers etc.
- ◆ Compliant logs and maintenance logs to assess if MTBF and MTTR are within acceptable levels.
- ◆ Activities in the IPF. Identify undesired activities such as smoking, consumption of eatables etc.

Question 17

Explain the various general components of Disaster Recovery Plan.

Answer

Disaster recovery: The term 'Disaster Recovery' describes the contingency measures that organizations have adopted at key computing sites to recover from, or to prevent any monumentally bad event or disaster. The primary objective of a disaster recovery plan is to assure the management that normalcy would be restored in a set time after any disaster occurs, thereby minimizing losses to the organization. The disaster recovery plan must take into account the physical location of the computer centre, since it can increase or decrease the chance of a disaster. Protection against flood, fire, earthquake or water logging etc. must be considered.

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

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

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

The following steps may be carried out under this plan:

- (i) An inventory of the hardware, application systems, system software, documentation etc. must be taken.
- (ii) Criticality of application systems to the organization and the importance of their loss must be evaluated. An indication must be given of the efforts and cost involved in restoring the various application systems.
- (iii) An application systems hierarchy must be spelt out.
- (iv) Selection of a disaster recovery site must be made. A reciprocal agreement with another organization having compatible hardware and software could be made.
- (v) A formal back agreement with another company must be made. This should cover the periodical exchange of information between the two sites regarding changes to hardware/software, the time and duration of systems availability, modalities of testing the plan etc.

Backup Plan: Organizations no matter how physically secure, their systems are always vulnerable to the disaster. Therefore, an effective safeguard is to have a backup of anything that could be destroyed, be it hardware or software. As regards hardware, stand by must be kept with regard to the needs of particular computer environments. So far as the software is concerned, it is necessary to make copies of important programs, data files, operating systems and test programs etc. The backup copies must be kept in a place, which is not susceptible to the same hazards as the originals.

Question 18

Write short notes on the Control Objectives for Information related Technology (COBIT).

Answer

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

- (i) management to benchmark the security and control, practices of IT environments;
- (ii) users of IT services to be assured that adequate security and control exist, and

Information Systems Control and Audit

- (iii) auditors to substantiate their opinions on internal control and to advice on IT security and control matters.

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

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

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

Question 19

XYZ & Company is dealing in the information systems audit. The audit of an IS environment to evaluate the systems, practices and operations may include one or both of the following:

- *Assessment of internal controls within the IS environment to assure validity, reliability, and security information.*
- *Assessment of the efficiency and effectiveness of the IS environment in economic terms.*

The IS audit process is to evaluate the adequacy of internal controls with regard to both specific computer programs and the data processing environment as a whole. This includes evaluating both the effectiveness and efficiency. The focus (scope and objective) of the audit process is not only on security which comprises confidentiality, integrity and availability but also on effectiveness (result-orientation) and efficiency (optimum utilization of resources).

Read the above carefully and answer the following:

- (a) *The audit objective and scope has a significant bearing on the skill and competence requirements of an IS auditor. There are a set of skills that is generally expected from an IS auditor. Discuss those skills in brief.*
- (b) *Explain various costs involved in the implementation and operation of controls.*

- (c) *Discuss the controls to consider when reviewing the organization and management controls in an Information System.*
- (d) *While reviewing the adequacy of data security controls, what are the items which need to be evaluated by an IS auditor?*

Answer

- (a) The set of skills that is generally expected of an IS auditor include:
- Sound knowledge of business operations, practices and compliance requirements,
 - Should possess the requisite professional technical qualification and certifications,
 - An good understanding of information Risks and Controls,
 - Knowledge of IT strategies, policy and procedure controls,
 - Ability to understand technical and manual controls relating to business continuity, and
 - Good knowledge of Professional Standards and Best practices of IT controls and security.
- (b) Implementing and operating controls in a system involves the following five costs:
- **Initial setup cost:** This cost is incurred to design and implement controls. For example, a security specialist must be employed to design a physical security system.
 - **Executing cost:** This cost is associated with the execution of a control. For example, the cost incurred in using a processor to execute input validation routines for a security system.
 - **Correction costs:** The control has operated reliably in signaling an error or irregularity, the cost associated with the correction of error or irregularity.
 - **Failure cost:** The control malfunctions or not designed to detect an error or irregularity. These undetected or uncorrected errors cause losses.
 - **Maintenance costs:** The cost associated in ensuring the correct working of a control. For example, rewriting input validation routines as the format of input data changes.
- (c) The controls to consider when reviewing the organization and management controls in an Information system shall include:
- **Responsibility:** The strategy to have a senior management personnel responsible for the IS within the overall organizational structure.
 - **An official IT structure:** There should be a prescribed organization structure with all staff deliberated on their roles and responsibilities by written down and agreed job descriptions.
-

Information Systems Control and Audit

- **An IT steering committee:** The steering committee shall comprise of user representatives from all areas of the business, and IT personnel. The committee would be responsible for the overall direction of IT. Here the responsibility lies beyond just the accounting and financial systems, for example, the telecommunications system (phone lines, video-conferencing) office automation, and manufacturing processing systems.
- (d) An IS auditor is responsible to evaluate the following when reviewing the adequacy of data security controls:
- Who is responsible for the accuracy of the data?
 - Who is permitted to update data?
 - Who is permitted to read and use the data?
 - Who is responsible for determining who can read and update the data?
 - Who controls the security of the data?
 - If the IS system is outsourced, what security controls and protection mechanism does the vendor have in place to secure and protect data?
 - Contractually, what penalties or remedies are in place to protect the tangible and intangible values of the information?
 - The disclosure of sensitive information is a serious concern to the organization and is mandatory on the auditor's list of priorities.

EXERCISE**Question 1**

An auditor while evaluating the reliability of a control implemented in a transaction process, had to estimate the reliability per transaction. A test was undertaken and the result indicated that the control was unreliable. The reliability of the process was 0.15 when the control was in place and was 0.09 when the control was absent. The management had estimated the cost of reprocessing the errors as Rs.1000 per transaction procedure. Evaluate the net benefit of the control procedure if the cost of implementation of the control is Rs.10, 000.

Question 2

Identify and briefly discuss the necessary data integrity control techniques for the following processes in a payroll system:

- (a) Addition/deletion/updating of employee data by the HR department,*
- (b) Payroll processing and storage, and*
- (c) Pay slip generation and consolidated pay report department-wise.*

Question 3

The Techno organization is implementing an off-site storage for its critical data. As an internal auditor, what are your recommendations for identifying the physical and environmental exposure and suggest controls for the same.

Question 4

In today's pervasive, internet banking systems with a centralized database environment monitoring of unauthorized intrusion into the banking network is a critical task. Prepare a report on the control methods by which the network can be protected.

Question 5

Do a comparative analysis on the different types of firewalls that mediate the access between different domains.

Question 6

ABC University currently provides the ability to register for classes via an enterprise software system within its intranet. However, the university is in the process of modifying its student registration system to allow registrations via the web.

Based on the given case, answer the following:

- (a) As an IS Auditor, suggest the change controls to be implemented to monitor the change.*

Information Systems Control and Audit

- (b) *Role of an IS auditor in evaluating the logical access controls implemented in the new system.*
- (c) *As an IS Auditor, list the issues that need to be considered for quality control.*

Question 7

The post implementation audit follow-up is an important step in the information systems audit process. What are the major control considerations that are to be addressed by the auditor in this step?

Question 8

Briefly state the need to install a 'Fire Suppression System' in an information processing facility and the various installation techniques.

Question 9

Discuss the various environmental control techniques that can be implemented to prevent the unauthorized access for critical IT infrastructures like server room, storage network devices, and switch/router installations.

Question 10

"A financial institute needs to authenticate its electronic credentials by ensuring its PKI policies and controls". Comment on the statement.

Question 11

The validity of the output generated from application software ultimately depends on the user, who is responsible for data submission and correction of errors. Briefly discuss the various user controls and error correction techniques to be followed.

Question 12

As a member of the system implementation and quality control team, prepare a quality control review checklist from an IS Auditor's perspective.

TESTING – GENERAL AND AUTOMATED CONTROLS

BASIC CONCEPTS

1. **Testing:** This is a process to identify the correctness, completeness, and quality of developed computer software.
2. **Audit Testing:** The auditor must address many considerations that cover the nature, timing, and extent of testing. The auditor must devise an auditing testing plan and a testing methodology to determine whether the previously identified controls are effective. The auditor also tests whether the end-user applications are producing valid and accurate information.
3. **IS Controls Audit Process:** It involves: Obtaining an understanding of an entity and its operations and key business processes, Obtaining a general understanding of the structure of the entity's networks, Identifying key areas of audit interest (files, applications, systems, locations), Assessing IS risk on a preliminary basis, Identifying critical control points (for example, external access points to networks), Obtaining a preliminary understanding of IS controls, and Performing other audit planning procedures.
4. **Substantive Testing:** This type of testing is used to substantiate the integrity of the actual processing. It is used to ensure that processes, not controls, are working as per the design of the control and produce the reliable results.
5. **Compliance Testing** – A compliance test determines if controls are working as designed. As per the policies and procedures, compliance testing results into the adherence to management directives.
6. **Audit Reporting:** After completing the testing phase, the auditor summarizes the results of the audit, draws conclusions on the individual and aggregate effect of identified IS control weaknesses on audit risk and audit objectives and reports the results of the audit. The auditor evaluates the individual and aggregate effect of all identified IS control weaknesses on the auditor's conclusions and the audit objectives. The auditor evaluates the effect of any weaknesses on the entity's ability to achieve each of the critical elements and on the risk of unauthorized access to key systems or files. Also, the auditor evaluates potential control dependencies.

Information Systems Control and Audit

7. **Types of Audit Tools:** Snapshots, Integrated Test facility, System Control Audit Review File (SCARF), Continuous and Intermittent Simulation (CIS)
 - 7.1 **Advantages of Continuous Auditing:** Timely, comprehensive and detailed auditing, Surprise test capability, Information to system staff on meeting of objectives, Training for new users.
8. **Hardware Testing:** Hardware testing may be done to the entire system against the Functional Requirement Specification(s) (FRS) and/or the System Requirement Specification (SRS). This techniques is of following types: Types of Hardware Testing, Functional testing, User Interface testing, Usability testing, Compatibility testing, Model Based testing, Error exit testing, User help testing, Security testing, Capacity testing, Performance testing, Reliability testing, Recovery testing, Installation testing, Maintenance testing, Accessibility testing

Question 1

Explain software testing and state its objectives.

Answer

Testing is a process used to identify the correctness, completeness and quality of developed computer software. In other words, testing is nothing but CRITICISM or COMPARISON, i.e. comparing the actual value with expected one.

One definition of testing is "the process of questioning a product in order to evaluate it", where the "questions" are things the tester tries to do with the product, and the product answers with its behaviour in reaction to the probing of the tester. The word testing means the dynamic analysis of the product—putting the product through its paces. Testing helps in verifying and validating if the software is working as it is intended to be working.

Objectives of Software Testing include:

- Testing is a process of executing a program with the intent of finding an error.
- A good test case is one that has a high probability of finding a yet undiscovered error.
- A successful test is one that uncovers a yet undiscovered error.

The data collected through testing can also provide an indication of the software's reliability and quality. However, testing cannot show the absence of defect, it can only show that software defects are present.

Question 2

Write a short note on Audit Testing.

Answer

The auditor must address many considerations that cover the nature, timing, and extent of testing. The auditor must devise an auditing testing plan and a testing methodology to determine whether the previously identified controls are effective. The auditor also tests whether the end-user applications are producing valid and accurate information. For microcomputers, several manual and automated methods are available to test for erroneous data. An initial step is to browse the directories of the PCs in which the end-user-developed application resides. Any irregularities in files should be investigated. Depending on the nature of the audit, computer-assisted techniques could also be used to audit the application. The auditor should also conduct several tests with both valid and invalid data to test the ability and extent of error detection, correction, and prevention within the application. In addition, the auditor should look for controls such as input balancing and record or hash totals to ensure that the end user reconciles any differences between input and output. The intensity and extent of the testing should be related to the sensitivity and importance of the application. The auditor should be wary of too much testing and limit his or her tests to controls that cover all the key risk exposures and possible error types. The key audit concern is that the testing should reveal any type of exposure of sensitive data and that the information produced by the application is valid, intact, and correct.

One should test the critical controls, processes, and apparent exposures. The auditor performs the necessary testing by using documentary evidence, corroborating interviews, and personal observation.

Secondly, we may test the critical controls, processes, and apparent exposures. The auditor performs the necessary testing by using documentary evidence, corroborating interviews, and personal observation. Validation of the information obtained is prescribed by the auditor's work program. Again, this work program is the organized, written, and pre-planned approach to the study of the IT department. It calls for validation in several ways as follows:

- Asking different personnel the same question and comparing the answers
- Asking the same question in different ways at different times
- Comparing checklist answers to work papers, programs, documentation, tests, or other verifiable results
- Comparing checklist answers to observations and actual system results
- Conducting mini-studies of critical phases of the operation

Such an intensive program allows an auditor to become informed about the operation in a short time. Programs are run on the computer to test and authenticate application programs that are run in normal processing. The audit team selects one of the many generalized audit software (GAS) packages such as Microsoft Access or Excel, IDEA, or ACL and determines

Information Systems Control and Audit

what changes are necessary to run the software at the installation. The auditor is to use one of these software's to do sampling, data extraction, exception reporting, summarize and foot totals, and other tasks to perform in-depth analysis and reporting capability.

Question 3

Auditors need to determine which audit procedures related to information systems controls are needed to obtain sufficient, appropriate evidence to support the audit findings and conclusions. It also provides some factors to assist the auditor in making this determination. Explain those factors, in brief.

Answer

These factors are given as follows:

- (i) The extent to which internal controls that are significant to the audit depend on the reliability of information processed or generated by information systems.
- (ii) The availability of evidence outside the information system to support the findings and conclusions: It may not be possible for auditors to obtain sufficient, appropriate evidence without assessing the effectiveness of relevant information systems controls. For example, if information supporting the findings and conclusions is generated by information systems or its reliability is dependent on information systems controls; there may not be sufficient supporting or corroborating information or documentary evidence that is available other than that produced by the information systems.
- (iii) The relationship of information systems controls to data reliability: To obtain evidence about the reliability of computer generated information, auditors may decide to assess the effectiveness of information systems controls as part of obtaining evidence about the reliability of the data. If the auditor concludes that information systems controls are effective, the auditor may reduce the extent of direct testing of data.
- (iv) Assessing the effectiveness of information systems controls as an audit objective: When assessing the effectiveness of information systems controls is directly a part of audit objective, auditors should test information systems controls necessary to address the audit objectives. For example, the audit may involve the effectiveness of information systems controls related to certain systems, facilities, or organizations.

Question 4

Explain the information which should be included by auditors in the documentation of their preliminary understanding of the design of IS controls, to the extent relevant to the audit objectives.

Answer

The auditor should include the following information in the documentation of their preliminary understanding of the design of IS controls, to the extent relevant to the audit objectives:

- Identification of entitywide level controls (and appropriate system level controls) designed to achieve the control activities for each critical element within each general control area and a determination of whether they are designed effectively and implemented (placed in operation), including identification of control activities for which there are no or ineffective controls at the entitywide level and the related risks;
- Identification of business process level controls for key applications identified as key areas of audit interest, determination of where those controls are implemented (placed in operation) within the entity's systems, and the auditor's conclusion about whether the controls are designed effectively, including identification of control activities for which there are no or ineffective controls and the related risks and the potential impact of any identified design weaknesses on the completeness, accuracy, validity, and confidentiality of application data;
- Any internal or third-party information systems reviews, audits, or specialized systems testing (e.g., penetration tests, disaster recovery tests, and application-specific tests) performed during the last year;
- Management's plans of action and milestones, or their equivalent, that identify corrective actions planned to address known IS weaknesses and IS control weaknesses;

Status of the prior years' audit findings;

- Documentation for any significant computer security related incidents identified and reported for the last year;
- Documented security plans;
- Documented risk assessments for relevant systems (e.g., general support systems and major applications);
- System certification and accreditation documentation or equivalent for relevant systems;
- Documented business continuity of operations plans and disaster recovery plans; and
- A description of the entity's use of third-party IT services
- Relevant laws and regulations and their relation to the audit objectives.
- Description of the auditor's procedures to consider the risk of fraud, any fraud risk factors that the auditor believes could affect the audit objectives, and planned audit procedures to detect any fraud significant to the audit objectives.

Information Systems Control and Audit

- Audit resources planned.
- Current multiyear testing plans.
- Documentation of communications with entity management.
- If IS controls are performed by service organizations, conclusions whether such controls are significant to the audit objectives and any audit procedures performed with respect to such controls (e.g., review of service auditor reports)
- If the auditor plans to use the work of others, conclusions concerning the planned use of the work of others and any audit procedures performed with respect to using the work of others.
- Audit plan that adequately describes the objectives, scope, and methodology of the audit.
- Any decision to reduce testing of IS controls due to the identification of significant IS control weaknesses.

Question 5

Explain the test effectiveness of Information System Controls.

Answer

The auditor should design and conduct tests of relevant control techniques that are effective in design to determine their effectiveness in operation. It is generally more efficient for the auditor to test IS controls on a tiered basis, starting with the general controls at the entitywide and system levels, followed by the general controls at the business process application level, and concluding with tests of business process application, interface, and data management system controls at the business process application level. Such a testing strategy may be used because ineffective IS controls at each tier generally preclude effective controls at the subsequent tier.

If the auditor identifies IS controls for testing, the auditor should evaluate the effectiveness of

- general controls at the entitywide and system level;
- general controls at the business process application level; and
- specific business process application controls (business process controls, interface controls, data management system controls), and/or user controls, unless the IS controls that achieve the control objectives are general controls.

The auditor should determine whether entitywide and system level general controls are effectively designed, implemented, and operating effectively by:

- identifying applicable general controls;
- determining how those controls function, and whether they have been placed in operation; and
- evaluating and testing the effectiveness of the identified controls.

The auditor generally should use knowledge obtained in the planning phase. The auditor should document the understanding of general controls and should conclude whether such controls are effectively designed, placed in operation, and, for those controls tested, operating as intended.

Question 6

To assess the operating effectiveness of IS controls, auditors should perform an appropriate mix of audit procedures to obtain sufficient, appropriate evidence to support their conclusions. Explain these procedures, in brief.

Answer

To assess the operating effectiveness of IS controls, auditors should perform an appropriate mix of audit procedures to obtain sufficient, appropriate evidence to support their conclusions. Such procedures could include the following:

- Inquiries of IT and management personnel can enable the auditor to gather a wide variety of information about the operating effectiveness of control techniques. The auditor should corroborate responses to inquiries with other techniques.
- Questionnaires can be used to obtain information on controls and how they are designed.
- Observation of the operation of controls can be a reliable source of evidence. For example, the auditor may observe the verification of edit checks and password controls. However, observation provides evidence about controls only when the auditor was present. The auditor needs other evidence to be satisfied controls functioned the same way throughout the period.
- The auditor may review documentation of control policies and procedures. For example, the entity may have written policies regarding confidentiality or logical access. Review of documents will allow the auditors to understand and assess the design of controls.
- Inspection of approvals/reviews provides the auditor with evidence that management is performing appropriate control checks. The auditor may combine these tests with discussions and observations.

Information Systems Control and Audit

- Analysis of system information (e.g., configuration settings, access control lists, etc.) obtained through system or specialized software provides the auditor with evidence about actual system configuration.
- Data review and analysis of the output of the application processing may provide evidence about the accuracy of processing. For example, a detailed review of the data elements or analytical procedures of the data as a whole may reveal the existence of errors. Computer-assisted audit techniques (CAAT) may be used to test data files to determine whether invalid transactions were identified and corrected by programmed controls. However, the absence of invalid transactions alone is insufficient evidence that the controls effectively operated.
- Reperformance of the control could be used to test the effectiveness of some programmed controls by reapplying the control through the use of test data. For example, the auditor could prepare a file of transactions that contains known errors and determine if the application successfully captures and reports the known errors.

Based on the results of the IS controls audit tests, the auditor should determine whether the control techniques are operating effectively to achieve the control activities. Controls that are not properly designed to achieve the control activities or that are not operating effectively are potential IS control weaknesses.

For each potential weakness, the auditor should determine whether there are specific compensating controls or other factors that could mitigate the potential weakness. If the auditor believes that the compensating controls or other factors could adequately mitigate the potential weakness and achieve the control activity, the auditor should obtain evidence that the compensating or other control is effectively operating and actually mitigates the potential weakness. If it effectively mitigates the potential weakness, the auditor can conclude that the control activity is achieved; however, the auditor may communicate such weaknesses to the entity. If the potential weakness is not effectively mitigated, the potential weakness is an actual weakness. The auditor evaluates its effects on IS controls in combination with other identified weaknesses in the reporting phase.

Question 7

Explain the information developed in the testing phase that the auditor should document.

Answer

Information developed in the testing phase that the auditor should document includes the following:

- An understanding of the information systems that are relevant to the audit objectives
- IS Control objectives and activities relevant to the audit objectives

- By level (e.g., entitywide, system, business process application) and system sublevel (e.g., network, operating system, infrastructure applications), a description of control techniques used by the entity to achieve the relevant IS control objectives and activities
- By level and sublevel, specific tests performed, including
- related documentation that describes the nature, timing, and extent of the tests;
- evidence of the effective operation of the control techniques or lack thereof (e.g., memos describing procedures and results, output of tools and related analysis);
- if a control is not achieved, any compensating controls or other factors and the basis for determining whether they are effective;
- the auditor's conclusions about the effectiveness of the entity's IS controls in achieving the control objective; and
- for each weakness, whether the weakness is a material weakness, significant deficiency or just a deficiency, as well as the criteria, condition, cause, and effect if necessary to achieve the audit objectives.

Question 8

Describe the advantages and disadvantages of Continuous Auditing techniques in brief.

Answer

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.

Information Systems Control and Audit

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.

Question 9

What is SCARF? Explain in brief.

Answer

System Control Audit Review File (SCARF): The system control audit review file (SCARF) technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written onto a special audit file- the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities.

Question 10

Which types of information may be collected by the auditors by using SCARF?

Answer

Auditors might use SCARF to collect the following types of information:

- **Application system errors** - SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.
- **Policy and procedural variances** - Organizations have to adhere to the policies, procedures and standards of the organization and the industry to which they belong.

SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.

- **System exception** - SCARF can be used to monitor different types of application system exceptions. For example, salespersons might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.
- **Statistical sample** - Some embedded audit routines might be statistical sampling routines, SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.
- **Snapshots and extended records** - Snapshots and extended records can be written into the SCARF file and printed when required.
- **Profiling data** - Auditors can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.
- **Performance measurement** - Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.

Question 11

Write a short note on Continuous and Intermittent Simulation (CIS).

Answer

Continuous and Intermittent Simulation (CIS): This is a variation of the SCARF continuous audit technique. This technique can be used to trap exceptions whenever the application system uses a database management system. During application system processing, CIS executes in the following way:

- The database management system reads an application system transaction. It is passed to CIS. CIS then determines whether it wants to examine the transaction further. If yes, the next steps are performed or otherwise it waits to receive further data from the database management system.
- CIS replicates or simulates the application system processing.
- Every update to the database that arises from processing the selected transaction will be checked by CIS to determine whether discrepancies exist between the results it produces and those the application system produces.
- Exceptions identified by CIS are written to an exception log file.
- The advantage of CIS is that it does not require modifications to the application system and yet provides an online auditing capability.

EXERCISE

Question 1

Describe various concurrent audit tools?

Question 2

What are the advantages and disadvantages of continuous auditing?

Question 3

Describe in short the review methodology for hardware?

Question 4

What are the various kinds of hardware testing?

Question 5

Testing the LAN and its environment is a vital part of IS Audit. Give an overview of the procedure to do so?

RISK ASSESSMENT METHODOLOGIES AND APPLICATIONS

BASIC CONCEPTS

1. **Risk:** A risk is the likelihood that an organization would face a vulnerability being exploited or a threat becoming harmful.
 - 1.1 **Threat:** A threat is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organization.
 - 1.2 **Vulnerability:** This is the weakness in the system safeguards that exposes the system to threats. It may be weakness in an information system, cryptographic system (security systems), or other components (e.g. system security procedures, hardware design, internal controls) that could be exploited by a threat.
 - 1.3 **Exposure:** An exposure is the extent of loss the organization has to face when a risk materializes. It is not just the immediate impact, but the real harm that occurs in the long run.
 - 1.4 **Likelihood:** Likelihood of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event.
 - 1.5 **Attack:** This 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.
 - 1.6 **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.
2. **Threats to the Computerized Environment:** Major threats are: Power Loss, Communication Failure, Disgruntled employees, Errors, Malicious Code, Abuse of access privileges by employees, Natural disasters, Theft or destruction of computing resources, Downtime due to technology failure, Fire etc.

Information Systems Control and Audit

3. **Threats due to cyber crimes:** Major threats are: Embezzlement, Fraud, Theft of proprietary information, Denial of Service, Vandalism or sabotage, Computer Virus etc.
4. **Risk Assessment:** This is a critical step in disaster and business continuity planning. Risk assessment is necessary for developing a well tested contingency plan. Risk assessment is the analysis of threats to resources (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status in the minimum time in case of a disaster. The areas to be focused upon are: Prioritization, Identifying critical applications, Assessing their impact on the organization, Determining recovery time frame, Assess Insurance Coverage, Identification of exposures and implications, Development of recovery plan.
 - 4.1 **Systematic Risks:** These are unavoidable risks - these are constant across majority of technologies and applications. For example the probability of power outage is not dependant on the industry but is dependant on external factors. Systematic risks would remain, no matter what technology is used.
 - 4.2 **Unsystematic Risks:** The risks which are peculiar to the specific applications or technology. One of the major characteristics of these risks would be that they can be generally mitigated by using an advanced technology or system. For example one can use a computer system with automatic mirroring to reduce the exposure to loss arising out of data loss in the event of failure of host computer. Thus by making additional investment one can mitigate these unsystematic risks.
5. **Techniques of Risk Evaluation:** Following are some of the techniques that are available to assess and evaluate risks: Judgment and intuition, The Delphi approach, Scoring, and Quantitative Techniques.
6. **Common Risk Mitigation Techniques:** Some of the common risk mitigation techniques are: Insurance, Outsourcing, and Service Level Agreements.

Question 1

Explain the following terms with reference to Information Systems:

- (i) *Risk*
- (ii) *Threat*
- (iii) *Vulnerability*
- (iv) *Exposure*
- (v) *Attack*
- (vi) *Malicious Code*

Answer

- (i) **Risk:** It is the likelihood that an organization would face a vulnerability being exploited or a threat becoming harmful. Information systems can generate many direct and indirect risks. These risks lead to a gap between the need to protect systems and the degree of protection applied. Some of the factors that cause gaps are widespread use of technology, Interconnectivity of systems and devolution of management and control etc.
- (ii) **Threat:** A threat is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organization. Threat is any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data and denial of services
- (iii) **Vulnerability:** It is the weakness in the system safeguards that exposes the system to threats. It may be weakness in an information system, cryptographic system, internal controls etc, that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system.
- (iv) **Exposure:** It is the extent of loss the organization has to face when a risk materializes. It is not just the immediate impact, but the real harm that occurs in the long run. For example, loss of business, failure to perform the system's mission, loss of reputation, violation of privacy, loss of resources.
- (v) **Attack:** is a set of actions designed to compromise confidentiality, integrity, availability or any other desired feature of an information system. It is an attempt to defeat IS safeguards. The type of attack and its degree of success will determine the consequence of the attack.
- (vi) **Malicious Code:** It is a code such as viruses and worms which freely access the unprotected networks which may affect organizational and business networks that use these unprotected networks.

Question 2

Define the following terms:

- (i) *Likelihood*
- (ii) *Attack*
- (iii) *Residual Risk*

Answer

- (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,

Information Systems Control and Audit

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.

Question 3

"There always exist some Common threats to the computerized environment." Explain these threats.

Or

Discuss various threats to the computerized environment.

Answer

Any computerized environment is dependent on people. They are a critical links in making the entire enterprise computing happen and are responsible for the threats and attacks. The professionals such as analysts, programmers, data administrator, etc. are key links in ensuring that the IT infrastructure delivers to the user requirements and are target key persons who may leak the sensitive information of the enterprise. A few common threats to the computerized environment can be:

- (i) **Power Loss:** Power failure can cause disruption of entire computing equipments since computing equipments depends on power supply.
- (ii) **Communication failure:** Failure of communication lines result in inability to transfer data which is a back bone of the system. Such failures present a significant threat that will have a direct impact on operations. For example, organizations which use communication lines for e-banking, railway reservation –e-ticketing etc., failure of communication link presents a significant threat.
- (iii) **Disgruntled Employees:** Such employees presents a threat since, with access to sensitive information of the organization, they may cause intentional harm to the information processing facilities or sabotage operations.

- (iv) *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.
- (v) *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.
- (vi) *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.
- (vii) *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.
- (viii) *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.
- (ix) *Downtime due to technology failure*: IS facilities may become unavailable due to technical glitches or equipment failure. The period of downtime the facility is not available may vary in criticality depending on the nature of business and the critical business process that the technology supports.
- (x) *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.

Question 4

“Always, there exist some threats due to Cyber Crimes.” Explain these threats.

Or

Explain the threats due to Cyber crimes.

Answer

Any computerized environment is dependent on people. Though they play a critical role in success of an enterprise computing, it is a fact that threats always exist due to cyber crimes committed by people. The special skill sets of IT operational team, programmers; data administrator, etc. are key links in ensuring that the IT infrastructure delivers output as per user requirements. At the same time, social engineering risks target key persons to get sensitive information to exploit the information resources of the enterprise. Threats also arise on account of dependence on external agencies. IT computing services are

Information Systems Control and Audit

significantly dependant on various vendors and service providers for equipment supply and support, consumables, systems and program maintenance, air-conditioning, hot-site providers, utilities, etc. Following are some of the serious threats due to cyber crimes:

- *Embezzlement*: It is unlawful misappropriation of money or other things of value, by the person to whom it was entrusted (typically an employee), for his/her own use or purpose.
- *Fraud*: It occurs on account of internal misrepresentation of information or identity to deceive others, the unlawful use of credit/debit card or ATM, or the use of electronic means to transmit deceptive information, to obtain money or other things of value. Fraud may be committed by someone inside or outside the company.
- *Theft of proprietary information*: It is illegal to obtain of designs, plans, blueprints, codes, computer programs, formulas, recipes, trade secrets, graphics, copyrighted material, data, forms, files, lists, and personal or financial information, usually by electronic copying.
- *Denial of service*: There can be disruption or degradation of service that is dependent on external infrastructure. Problems may erupt through internet connection or e-mail service that result in an interruption of the normal flow of information. Denial of service is usually caused by events such as ping attacks, port scanning probes, and excessive amounts of incoming data.
- *Vandalism or sabotage*: It is the deliberate or malicious, damage, defacement, destruction or other alteration of electronic files, data, web pages, and programs.
- *Computer virus*: Viruses are hidden fragments of computer codes which propagates by inserting themselves into or modifying other programs.
- *Other*: Threat includes several other cases such as intrusion, breaches and compromises of the respondent's computer networks (such as hacking or sniffing) regardless of whether damage or loss were sustained as a result.

Question 5

What do you understand by "Risk Assessment"? Discuss the various areas that are to be explored to determine the risk.

Answer

Risk assessment is a critical step in disaster and business continuity planning. Risk assessment is necessary for developing a well tested contingency plan. Risk assessment is the analysis of threats to resources (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status in the minimum time in case of

a disaster. Disasters may lead to vulnerable data and crucial information suddenly becoming unavailable. Risk assessment is a useful technique to assess the risks involved in the event of unavailability of information, to priorities applications, identify exposures and develop recovery scenarios.

Various areas that are to be explored to determine the risk are briefly discussed below:

- (i) *Prioritization*: All applications are inventoried and critical ones identified. Each of the critical applications is reviewed to assess its impact on the organization, in case a disaster occurs. Subsequently, appropriate recovery plans are developed.
- (ii) *Identifying critical applications*: It is necessary to identify critical applications of the currently running applications. Further analysis is done to determine specific jobs in the applications which may be more critical. Even though the critical value would be determined based on its present value, future changes should not be ignored.
- (iii) *Assessing their impact on the organization*: Business continuity planning should not concentrate only on business disruption but should also take into account other organizational functions which may be affected. The areas to be considered include:
 - Legal liabilities,
 - Interruptions of customer services.
 - Possible losses,
 - Likelihood of fraud and recovery procedures.
- (iv) *Determining recovery time-frame*: Critical recovery time period is the period of time in which business processing must be resumed before the organization incurs severe losses. This critical time depends upon the nature of operations.
- (v) *Assess Insurance coverage*: The information system insurance policy should be a multi-peril policy, designed to provide various types of coverage. It may cover the cost of hardware, software reconstruction, business interruption etc.
- (vi) *Identification of exposures and implications*: It is not possible to accurately predict as to when and how a disaster would occur. So it is necessary to estimate the probability and frequency of disaster.
- (vii) *Development of recovery plan*: The plan should be designed to provide for recovery from total destruction of a site.

Question 6

Describe Risk Management Process.

Information Systems Control and Audit

Answer

Risk Management Process: The broad Risk Management Process comprises of the following:

1. Identify the technology related risks under the gamut of operational risks.
2. Assess the identified risks in terms of probability and exposure.
3. Classify the risks as systematic and unsystematic.
4. Identify various managerial actions that can reduce exposure to systematic risks and the cost of implementing the same.
5. Look out for technological solutions available to mitigate unsystematic risks.
6. Identify the contribution of the technology in reducing the overall risk exposure.
7. Evaluate the technology risk premium on the available solutions and compare the same with the possible value of loss from the exposure.
8. Match the analysis with the management policy on risk appetite and decide on induction of the same.

Question 7

What do you understand by the term Risk Assessment? What areas need to be focused for risk assessment?

Answer

Risk Assessment: A risk assessment can provide an effective approach that will serve as the foundation for avoiding of disasters. Through risk analysis, it is possible to identify, assess and then mitigate the risk.

Risk Assessment is a critical step in disaster and business continuity planning. Risk Assessment is the analysis of threats to resources (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status in the minimum time in case of a disaster. Disasters may lead to vulnerable data and crucial information suddenly becoming unavailable. The unavailability of data may be due to the non-existence or inadequate testing of the existing plan.

The areas to be focused upon are:

- (a) **Prioritization:** All applications are inventoried and critical ones identified. Each of the critical application is reviewed to assess its impact on the organization, in case a disaster occurs. Subsequently, appropriate recovery plans are developed.
- (b) **Identifying critical applications:** Amongst the applications currently being processed the critical applications are identified. Further analysis is done to

determine specific jobs in the applications which may be more critical. Even though the critical value would be determined based on its present value, future changes should not be ignored.

- (c) **Assessing their impact on the organization:** Business continuity planning should not concentrate only on business disruption but should also take into account other organizational functions which may be affected. The areas to be considered include:
- Legal liabilities
 - Interruptions of customer services.
 - Possible losses
 - Likelihood of fraud and recovery procedures.
- (d) **Determining recovery time-frame:** Critical recovery time period is the period of time in which business processing must be resumed before the organization incurs severe losses. This critical time depends upon the nature of operations. It is essential to involve the end users in the identification of critical functions and critical recovery time period.
- (e) **Assess Insurance Coverage:** The information system insurance policy should be a multiperil policy, designed to provide various types of coverage. Depending on the individual organization and the extent of coverage required, suitable modifications may be made to the comprehensive list provided below:
- (i) **Hardware and facilities:** The equipment should be covered adequately. Provision should be made for the replacement of all equipment with a new one by the same vendor.
 - (ii) **Software reconstruction:** In addition to the cost of media, programming costs for recreating the software should also be covered.
 - (iii) **Extra expenses:** The cost incurred for continuing the operations till the original facility is restored should also be covered.
 - (iv) **Business interruption:** This applies mainly to centres performing outsourced jobs of clients. The loss of profit caused by the damaged computer media should be covered.
 - (v) **Valuable paper and records:** The actual cost of valuable papers and records stored in the insured premises should be covered.
 - (vi) **Errors and omissions:** This cover is against the legal liability arising out of errors and omissions committed by system analysts, programmes and other information system personnel.
-

Information Systems Control and Audit

- (vii) **Fidelity coverage:** This coverage is for acts of employees more so in the case of financial institutions which use their own computers for providing services to clients.
- (viii) **Media transportation:** The potential loss or damage to media while being transported to off-site storage / premises should be covered.
- (f) **Identification of exposures and implications:** It is not possible to accurately predict as to when and how a disaster would occur. So, it is necessary to estimate the probability and frequency of disaster.
- (g) **Development of recovery plan:** The plan should be designed to provide for recovery from total destruction of a site.

Question 8

State and explain four commonly used techniques to assess and evaluate risks.

Answer

Four most commonly used techniques to assess and evaluate risks are:

- Judgment and intuition
- The Delphi Approach
- Scoring
- Quantitative Techniques

A brief discussion on each of them is given as follows:

- (i) **Judgment and intuition:** In many situations, the auditors have to use their judgment and intuition for risk assessment. This mainly depends on the personal and professional experience of the auditors and their understanding of the system and its environment. Together with it, systematic education and ongoing professional updating is also required.
- (ii) **The Delphi Approach:** This technique is used for obtaining a consensus opinion. A panel of experts is engaged and each expert is asked to give his opinion in a written and independent method. They enlist the estimate of the cost benefits and the reasons why a particular system is to be chosen, the risks and exposures of the system. These estimates are then compiled together. The estimates falling within a pre-decided acceptable range are taken. The process may be repeated four times for revising estimates falling beyond the range. Then a curve is drawn taking all the estimates as points on the graphs. The median is drawn and this is the consensus opinion.

- (iii) **The Scoring Approach:** In this approach, the risks in the system and their respective exposures are listed. Weights are then assigned to the risks and to the exposures depending on the severity, impact of occurrence and costs involved. The product of the risk weight with the exposure weight of every characteristic gives the weighted score. The sum of these weighted score gives the risk and exposure score of the system. System risks and exposures are then ranked according to the scores.
- (iv) **Quantitative Techniques:** Quantitative techniques involve the calculating of an annual loss exposure value based on the probability of the event and the exposure in terms of estimated costs. This helps the organization to select cost effective solutions. It is the assessment of potential damage in the event of occurrence of unfavorable events, keeping in mind how often such an event may occur.

Question 9

Explain the common risk mitigation techniques.

Answer

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.

EXERCISE

Question 1

An automobile spare parts production company has 10 distribution centers, each of which maintains their inventory status through the company's inventory application software on its Virtual Private Network (VPN). Managers across the distribution centers have identified different types of frauds/errors committed during data entry, transaction processing and fake user logins in the inventory system.

The manager of one of the distribution centre has asked you (IS Auditor) to prepare a report on "how the risk appraisal can be undertaken". Indicate the appropriate approach in this situation and give reasons for your answers.

Question 2

Differentiate between the Systematic and Unsystematic risks.

Question 3

Differentiate between the System Control Audit Review File (SCARF) and Continuous and Intermittent Simulation (CIS).

Question 4

An enterprise is in the process of leveraging Information and Communication Technology (ICT) for its business value chain process. As a member of ICT implementation team, prepare the risk assessment lists for the following issues:

- (a) Insurance Coverage, and*
- (b) Enterprise-wide Application Software Security.*

Question 5

Briefly explain the risk analysis and mitigation measures that a system audit and control professional should consider.

BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

BASIC CONCEPTS

1. **Business Continuity Planning:** Planning is an activity to be performed before the disaster occurs or it would be too late to plan an effective response. Business continuity covers the following areas: Business Resumption Planning, Disaster Recovery Planning, and Crisis Management.
2. **Developing a Business Continuity Plan:** The methodology for developing a business continuity plan can be sub-divided into eight different phases: Pre-Planning Activities (Business continuity plan Initiation), Vulnerability Assessment and General Definition of Requirements, Business Impact Analysis, Detailed Definition of Requirements, Plan Development, Testing Program, Maintenance Program, Initial Plan Testing and Plan Implementation.
3. **Business Impact Analysis:** Business Impact Analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. It enables the business continuity team to identify critical systems, processes and functions, assess the economic impact of incidents and disasters that result in a denial of access to the system, services and facilities, and assess the "pain threshold," that is, the length of time business units can survive without access to the system, services and facilities.
4. **Plan development:** The objective of this phase is to determine the available options and formulation of appropriate alternative operating strategies to provide timely recovery for all critical processes and their dependencies. The recovery strategies may be two-tiered: Business - Logistics, accounting, human resources, etc., and Technical - Information Technology (e.g. desktop, client-server, midrange, mainframe computers, data and voice networks).
 - 4.1 **Types of Plans:** There are various kinds of plans that need to be designed. They include: Emergency Plan, Backup Plan, and Recovery Plan.
5. **Threats and Risk Management:** Various threats, risks and exposures to computer systems are due to: Lack of Confidentiality, Integrity, and Availability,

Information Systems Control and Audit

Unauthorized users attempts to gain access to the system and system resources, Disgruntled employees, Hackers and computer crimes, Terrorism and industrial espionage.

6. **Types of Backups:** Full Backup, Differential Backup, Incremental Backup, and Mirror Backup. Security administrators should consider the following backup options: Cold Site, Hot Site, Warm Site, and reciprocal Agreement.
7. **Backup Redundancy:** Major points are: Multiple backup Media, Off-site Backup, Where to keep the Backups, Media rotation tactics.
8. **Types of backup Media:** The most common types of backup media available on the market today include: Floppy Diskettes, Compact Disks, Tape Drives, Disk Drives, Removable Disks, DAT (Digital Audio Tape) Drives, Optical Jukeboxes, Autoloader TAPE Systems, USB Flash Drive, and Zip Drive.
9. **Insurance:** Policies usually can be obtained to cover the following resources: Equipment, Facilities, Storage Media, Business Interruption, Extra Expenses, Valuable Papers, Accounts receivable, Media Transportation, Malpractice, errors.
 - 9.1 **Kinds of Insurance:** These are of following types: First-party Insurances-Property Damages, First-party Insurances - Business Interruption, Third-party Insurance – General Liability, Third-party Insurance – Directors and Officers.
10. **Testing Methodology:** With good planning a great deal of disaster recovery testing can be accomplished with moderate expenditure. There are four types of tests: Hypothetical, Component, Module, and Full.
11. **Audit Tools and Techniques:** The best audit tool and technique is a periodic simulation of a disaster. Other audit techniques would include observations, interviews, checklists, inquiries, meetings, questionnaires and documentation reviews. These tools and methods may be categorized as: Automated Tools, Internal Control Auditing, Disaster and Security Checklists, and Penetration Testing.

Question 1

Discuss the objectives and goals of Business Continuity planning.

Answer

Objectives and Goals of Business Continuity Planning: The primary objective of a business continuity planning is to enable an organization to survive a disaster and to re-establish normal business operations. In order to survive, the organization must assure

Business Continuity Planning and Disaster Recovery Planning

that critical operations can resume normal processing within a reasonable time frame. The key objectives of the contingency plan should be to:

- (i) Provide for the safety and well-being of people on the premises at the time of disaster;
- (ii) Continue critical business operations;
- (iii) Minimise the duration of a serious disruption to operations and resources (both information processing and other resources);
- (iv) Minimise immediate damage and losses;
- (v) Establish management succession and emergency powers;
- (vi) Facilitate effective co-ordination of recovery tasks;
- (vii) Reduce the complexity of the recovery effort;
- (viii) Identify critical lines of business and supporting functions.

Therefore, the goals of the business continuity plan should be to:

- (i) Identify weaknesses and implement a disaster prevention program;
- (ii) Minimise the duration of a serious disruption to business operations;
- (iii) Facilitate effective co-ordination of recovery tasks; and
- (iv) Reduce the complexity of the recovery effort

Question 2

What do you understand by the term Disaster? What procedural plan do you suggest for disaster recovery?

Answer

The term disaster can be defined as an incident which jeopardizes business operations and/or human life. It could be due to sabotage (human) or natural. Following is the procedural plans for disaster recovery.

Disaster Recovery Procedural Plan: Normally disaster recovery procedural plan is made when the system is normally working. After visualizing the disaster the action to be taken by different people of the organization are to be documented. This recovery and planning document may include the following areas:

- (i) The conditions for activating the plans, which describe the process to be followed before each plan, are activated.
- (ii) Emergency procedures, which describe the actions to be taken following an incident which jeopardizes business operations and/or human life. This should

Information Systems Control and Audit

include arrangements for public relations management and for effective liaison with appropriate public authorities e.g. police, fire, services and local government.

- (iii) Fallback procedures which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time-scale.
 - (iv) Resumption procedures, which describe the actions to be taken to return to normal business operations.
 - (v) A maintenance schedule, which specifies how and when the plan will be tested, and the process for maintaining the plan.
 - (vi) Awareness and education activities, which are designed to create an understanding of the business continuity, process and ensure that the business continues to be effective.
 - (vii) The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
 - (viii) Contingency plan document distribution list.
 - (ix) Detailed description of the purpose and scope of the plan.
 - (x) Contingency plan testing and recovery procedure.
 - (xi) List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
 - (xii) Checklist for inventory taking and updating the contingency plan on a regular basis.
 - (xiii) List of phone numbers of employees in the event of an emergency.
 - (xiv) Emergency phone list for fire, police, hardware, software, suppliers, customers, back-up location, etc.
 - (xv) Medical procedure to be followed in case of injury.
 - (xvi) Back-up location contractual agreement, correspondences.
 - (xvii) Insurance papers and claim forms.
 - (xviii) Primary computer centre hardware, software, peripheral equipment and software configuration.
 - (xix) Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
 - (xx) Alternate manual procedures to be followed such as preparation of invoices.
 - (xxi) Names of employees trained for emergency situation, first aid and life saving techniques.
 - (xxii) Details of airlines, hotels and transport arrangements.
-

Question 3

Describe the methodology of developing a Business Continuity Plan.

Answer

The methodology for developing a business continuity plan can be sub-divided into eight different phases. The extent of applicability of each of the phases has to be tailored to the respective organisation. The methodology emphasises on the following:

- (i) Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
- (ii) Obtaining commitment from appropriate management to support and participate in the effort;
- (iii) Defining recovery requirements from the perspective of business functions;
- (iv) Documenting the impact of an extended loss to operations and key business functions;
- (v) Focusing appropriately on disaster prevention and impact minimisation, as well as orderly recovery;
- (vi) Selecting business continuity teams that ensure the proper balance required for plan development;
- (vii) Developing a business continuity plan that is understandable, easy to use and maintain; and
- (viii) Defining how business continuity considerations must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.

Question 4

Briefly explain the various types of system's back-up for the system and data together.

Answer

Types of system's Back-ups: When the back-ups are taken of the system and data together, they are called total system's back-up. System back-up may be a full back-up, an incremental back-up or a differential back-up.

- (i) *Full Backup:* Every backup generation contains every file in the backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data. This is the simplest form of backup with a single restoring session for restoring all backed-up files.

Information Systems Control and Audit

- (ii) *Differential Backup*: It contains all the files that have changed since the last full backup. This is in contrast to incremental backup generation, which holds all the files that were modified since the last full or incremental backup. It is faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.
- (iii) *Incremental Backup*: Only the files that have changed since the last full backup / differential backup / or incremental backup are saved. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space. Normally, it is difficult to restore as you have to start with recovering the last full backup, and then recovering from every incremental backup taken since.
- (iv) *Mirror back-up*: It is identical to a full backup, with the exception that the files are not compressed in zip files and they can not be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

Question 5

As a system auditor, what control measures will you check to minimize threats, risks and exposures in a computerized system?

Answer

To minimize threats to the confidentiality, integrity, and availability, of data and computer systems and for successful business continuity, the system auditor should evaluate potential threats to computer systems. Discussed hereunder are various control measures that will be checked by him to minimize threats, risks and exposures in a computerized system:

- (i) *Lack of integrity* : Control measures to ensure integrity include implementation of security policies, procedures and standards, use of encryption techniques and digital signatures, inclusion of data validation, editing, and reconciliation techniques for inputs, processes and outputs, updated antivirus software, division of job and layered control to prevent impersonation, use of disk repair utility, implementation of user identification, authentication and access control techniques, backup of system and data, security awareness programs and training of employees, installation of audit trails, audit of adequacy of data integrity.
- (ii) *Lack of confidentiality*: Control measures to ensure confidentiality include use of encryption techniques and digital signatures, implementation of a system of accountability by logging and journaling system activity, development of a security policy procedure and standard, employee awareness and training, requiring employees to sign a non-disclosure undertaking, implementation of physical and logical access controls, use of passwords and other authentication techniques, establishment of a documentation and distribution schedule, secure storage of

Business Continuity Planning and Disaster Recovery Planning

important media and data files, installation of audit trails, and audit of confidentiality of data.

- (iii) Lack of system availability: Control measures to ensure availability include implementation of software configuration controls, a fault tolerant hardware and software for continuous usage and an asset management software to control inventory of hardware and software, insurance coverage, system backup procedure to be implemented, implementation of physical and logical access controls, use of passwords and other authentication techniques, incident logging and report procedure, backup power supply, updated antivirus software, security awareness programmes and training of employees, installation of audit trails, audit of adequacy of availability safeguards.
- (iv) Unauthorized users attempt to gain access to the system and system resources: Control measures to stop unauthorized users to gain access to system and system resources include identification and authentication mechanism such as passwords, biometric recognition devices, tokens, logical and physical access controls, smart cards, disallowing the sharing of passwords, use of encryption and checksum, display of warning messages and regular audit programs.

Data transmitted over a public or shared network may be intercepted by an unauthorized user, security breaches may occur due to improper use or bypass of available security features, strong identification and authentication mechanisms such as biometric, tokens, layered system access controls, documentation procedures, quality assurance controls and auditing.
- (v) Hostile software e.g. virus, worm, Trojan horses, etc.: Establishment of policies regarding sharing and external software usage, updated anti-virus software with detection, identification and removal tools, use of diskless PCs and workstations, installation of intrusion detection tools and network filter tools such as firewalls, use of checksums, cryptographic checksums and error detection tools for sensitive data, installation of change detection tools, protection with permissions required for the 'write' function.
- (vi) Disgruntled employees: Control measures to include installation of physical and logical access controls, logging and notification of unsuccessful logins, use of disconnect feature on multiple unsuccessful logins, protection of modem and network devices, installation of one time use only passwords, security awareness programs and training of employees, application of motivation theories, job enrichment and job rotation.
- (vii) Hackers and computer crimes: Control measures to include installation of firewall and intrusion detection systems, change of passwords frequently, installation of one time use passwords, discontinuance of use of installed and vendor installed passwords, use of encryption techniques while storage and transmission of data, use of digital signatures, security of modem lines with dial back modems, use of

Information Systems Control and Audit

message authentication code mechanisms, installation of programs that control change procedures, and prevent unauthorized changes to programs, installation of logging feature and audit trails for sensitive information.

- (viii) Terrorism and industrial espionage: Control measures to include usage of traffic padding and flooding techniques to confuse intruders, use of encryption during program and data storage, use of network configuration controls, implementation of security labels on sensitive files, usage of real-time user identification to detect masquerading, installation of intrusion detection programs.

Question 6

What are the audit tools and techniques used by a system auditor to ensure that disaster recovery plan is in order? Briefly explain them.

Answer

Audit tools and techniques used by a system auditor to ensure that the disaster recovery plan is in order, are briefly discussed below:

The best audit tool and technique is a periodic simulation of a disaster. Other audit techniques would include observations, interviews, checklists, inquiries, meetings, questionnaires and documentation reviews. These are categorized as follows:

- (i) Automated tools: They make it possible to review large computer systems for a variety of flaws in a short time period. They can be used to find threats and vulnerabilities such as weak access controls, weak passwords, and lack of integrity of the system software.
- (ii) Internal Control auditing: This includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance for laws and regulations.
- (iii) Disaster and Security Checklists: These checklists are used to audit the system. The checklists should be based upon disaster recovery policies and practices, which form the baseline. Checklists can also be used to verify changes to the system from contingency point of view.
- (iv) Penetration Testing: It is used to locate vulnerabilities to the system.

Question 7

What analysis should be done for understanding the degree of potential loss (such as reputation damage, regulation effects) of an organization? Enumerate the tasks to be undertaken in this analysis. In what ways the information can be obtained for this analysis?

Answer

Business Impact Analysis (BIA) should be done for assessing the potential impacts resulting from various events or incidents. It is intended to help in understanding the degree of potential loss which could occur. It covers not only financial loss but also other losses due to reputation damage, regulatory effects, etc.

For BIA, the following tasks are to be undertaken:

1. Identify organizational risks, and to minimize potential threats that may lead to a disaster.
2. Identify critical business processes.
3. Identify and quantify threats/ risks to critical business processes both in terms of outage and financial impact.
4. Identify dependencies and interdependencies of critical business processes and the order in which they must be restored.
5. Identify the maximum allowable downtime for each business processes.
6. Identify the type and the quantity of resources required for recovery.
7. Determine the impact to the organisation in the event of a disaster, e.g. financial reputation etc.

The information for this analysis can be obtained in many ways, including:

1. Questionnaires,
2. Workshops,
3. Interviews, and
4. 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 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.

Question 8

Describe the methodology and phases of developing a business continuity plan?

Answer

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.

Information Systems Control and Audit

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

Question 9

Explain the significance of a Business Impact Analysis (BIA) phase on developing a business continuity plan.

Answer

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.

Information Systems Control and Audit

Question 10

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*

Answer

- (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

Information Systems Control and Audit

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.

Question 11

Explain briefly the software and data back-up techniques.

Answer

Software and Data Back-up Techniques: When the back-ups are taken of the system and data together, they are called total system’s back-up. Systems back-up may be a full back-up, an incremental back-up or a differential back-up.

- (i) **Full Back-up:** This is the simplest form of back-up. With a full back-up system, every back-up generation contains every file in the backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data. When it comes to restoring data, this type of backup is the simplest to use because a single restore session is needed for restoring all back-up files.
- (ii) **Differential Back-up:** A differential backup generation contains all the files that have changed since the last full backup. This is in contrast to incremental backup generation,

Business Continuity Planning and Disaster Recovery Planning

which holds all the files that were modified since the last full or incremental backup.

Comparing with full back-up, differential back up is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

Restoring from a differential backup is a two-step operation. Restoring from the last full back-up; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup will probably include files that were already included in earlier differential backups.

- (iii) **Incremental Backup:** In an incremental backup generation only the files that have changed since the last full backup / differential back up / or incremental backup are saved. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space.
- (iv) **Mirror backup:** It is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

Question 12

Explain audit tools and techniques used for disaster recovery plan.

Answer

Audit Tools and Techniques: The best audit tool and technique is a periodic simulation of a disaster. Other audit techniques would include observations, interviews, checklists, inquiries, meetings, questionnaires and documentation reviews. These tools and methods may be categorized as under:

- (i) **Automated Tools:** Automated tools make it possible to review large computer systems for a variety of flaws in a short time period. They can be used to find threats and vulnerabilities such as weak access controls, weak passwords, lack of integrity of the system software etc.
- (ii) **Internal Control Auditing:** This includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance of laws and regulations.
- (iii) **Disaster and security checklists:** A checklist can be used against which the systems can be audited. The checklist should be based upon disaster recovery policies and practices, which form the baseline. Checklists can also be used to verify changes to the system from contingency point of view.
- (iv) **Penetration Testing:** Penetration testing can be used to locate vulnerabilities.

Information Systems Control and Audit

Question 13

Describe contents of a disaster recovery and planning document.

Answer

Disaster Recovery Procedural Plan Document: The disaster recovery and planning document may include the following areas:

- ◆ The conditions for activating the plans, which describe the process to be followed before each plan, are activated.
- ◆ Emergency procedures, which describe the action to be taken following an incident which jeopardizes business operations and / or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities e.g. police, fire, services and local government.
- ◆ Fallback procedures which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time-scale.
- ◆ Resumption procedures, which describe the actions to be taken to return to normal business operations.
- ◆ A maintenance schedule, which specifies how and when the plan will be tested, and the process for maintaining the plan.
- ◆ Awareness and education activities, which are designed to create an understanding of the business continuity, process and ensure that the business continues to be effective.
- ◆ The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternative should be nominated as required.
- ◆ Contingency plan document distribution list.
- ◆ Detailed description of the purpose and scope of the plan.
- ◆ Contingency plan testing and recovery procedure.
- ◆ List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
- ◆ Check-list for inventory taking and updating the contingency plan on a regular basis.
- ◆ List of phone numbers of employees in the event of an emergency.
- ◆ Emergency phone list for fire, police, hardware, software suppliers, customers, back-up location, etc.

Business Continuity Planning and Disaster Recovery Planning

- ◆ Medical procedure to be followed in case of injury.
- ◆ Backup location contractual agreement, correspondences.
- ◆ Insurance papers and claim forms.
- ◆ Primary computers Centre hardware, software, peripheral equipment and software configuration.
- ◆ Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
- ◆ Alternate manual procedures to be followed such as preparation of invoices.
- ◆ Names of employees trained for emergency situation, first aid and life saving techniques.
- ◆ Details of airlines, hotels and transport arrangements.

Question 14

Give objectives and goals of business continuity planning.

Answer

Objectives and Goals of Business Continuity Planning: The primary objective of a business continuity plan is to enable an organization to survive a disaster and to re-establish normal business operations. In order to survive, the organization must assure that critical operations can resume normal processing within a reasonable time frame. The key objectives of the contingency plan should be to:

- (i) Provide for the safety and well-being of people on the premises at the time of disaster;
- (ii) Continue critical business operations;
- (iii) Minimize the duration of a serious disruption to operations and resources (both information processing and other resources);
- (iv) Minimize immediate damage and losses;
- (v) Establish management succession and emergency powers;
- (vi) Facilitate effective coordination of recovery tasks;
- (vii) Reduce the complexity of the recovery effort;
- (viii) Identify critical lines of business and supporting functions;

Therefore, the goals of the business continuity plan should be to:

- (i) Identify weaknesses and implement a disaster prevention program;

Information Systems Control and Audit

- (ii) Minimize the duration of a serious disruption to business operations;
- (iii) facilitate effective coordination of recovery tasks;
- (iv) reduce the complexity of the recovery effort.

Question 15

PQR Enterprises uses business continuity and disaster recovery plans in its various operations. Business continuity focuses on maintaining the operations of the organization, especially the IT infrastructure in face of a threat that has materialized. Disaster recovery, on the other hand, arises mostly when business continuity plan fails to maintain operations and there is a service disruption. This plan focuses on restarting the operation using a prioritized resumption list.

Read the above carefully and answer the following:

- (a) *In your opinion, what should be the goals of a business continuity plan?*
- (b) *In the development of a business continuity plan, there are total eight phases; Business Impact Analysis is the third important phase. Discuss various tasks which are to be undertaken in this phase.*
- (c) *There are various available backup techniques e.g. Full backup, Incremental backup, Differential backup, and Mirror backup. Describe differential backup technique in detail.*

Answer

- (a) The goals of the business continuity plan should be to:
 - identify weaknesses and implement a disaster prevention program;
 - minimize the duration of a serious disruption to business operations;
 - facilitate effective co-ordination of recovery tasks; and
 - reduce the complexity of the recovery effort.
- (b) A number of tasks are to be undertaken in this phase as enumerated under:
 - Identify organizational risks - This includes single point of failure and infrastructure risks. The objective is to identify risks and opportunities and to minimize 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.

Business Continuity Planning and Disaster Recovery Planning

- 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 organization in the event of a disaster, e.g. financial reputation, etc.

(c) **Differential Backup:** A differential backup stores files that have changed since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up. Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

Restoring from a differential backup is a two-step operation: Restoring from the last full backup; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup will probably include files that were already included in earlier differential backups.

EXERCISE

Question 1

ABC Company is committed to implement the data backup policy through proper planning. What are the major tips that should be followed by the company for the backup?

Question 2

'With good planning, a great deal of disaster recovery testing can be accomplished with moderate expenditure.' Briefly explain the types of testing techniques.

Question 3

What is Business Continuity Planning? Briefly explain the areas covered by a BCP.

Question 4

A backup plan is to be prepared for XYZ company in order to specify the type of backup to be kept, frequency with which backup is to be undertaken, procedures for making a backup, location of backup resources, site where these resources can be assembled and operations restarted, personnel who are responsible for gathering backup resources and restarting operations, priorities to be assigned to recover various systems, and a time frame for the recovery of each system. But the most difficult part in preparing the backup plan is to ensure that all the critical resources are backed up. List the resources that are to be considered in a backup plan.

Question 5

Briefly explain the control measures to ensure Confidentiality, Integrity, and Availability of data.

Question 6

Differentiate between Incremental Backup and Mirror Backup.

Question 7

Describe various backup devices.

AN OVERVIEW OF ENTERPRISE RESOURCE PLANNING (ERP)

BASIC CONCEPTS

1. **ERP:** An Enterprise resource planning system is a fully integrated business management system covering functional areas of an enterprise like Logistics, Production, Finance, Accounting and Human Resources. It organizes and integrates operation processes and information flows to make optimum use of resources such as men, material, money and machine. ERP is a global, tightly integrated closed loop business solution package and is multifaceted.
 - 1.1 **ERP Characteristics:** An ERP system is not only the integration of various organization processes. Any system has to possess few key characteristics to qualify for a true ERP solution. These features are: Flexibility, Modular and Open, Comprehensive, Beyond the Company, Best Business Practices.
 - 1.2 **Why Companies undertake ERP?:** Companies should undertake ERP because of the following points: Integrate Financial information, Integrate customer order information, Standardize and speed up manufacturing processes, Reduce Inventory, Standardize HR Information.
2. **Business Process Reengineering (BPR):** The most accepted and formal definition for BPR, given by Hammer and Champy is reproduced here: “BPR is the fundamental rethinking and radical redesign of processes to achieve dramatic improvement, in critical, contemporary measures of performance such as cost, quality, service and speed”.
3. **Key Planning and Implementation Decisions:** This discussion looks at a number of the key decisions that need to be made when considering an enterprise integration effort. Major points are: ERP or not to ERP?, Follow Software's Processes or Customize?, In-house or Outsource?, ‘Big Bang’ or Phased Implementation?. Other implementation approaches include: The Wave Approach, Parallel Implementation, Instant cutovers (flip-the-switch).

Information Systems Control and Audit

4. **ERP Implementation Methodology:** Several steps are involved in the implementation of a typical ERP package. These are:
 - Identifying the needs for implementing an ERP package,
 - Evaluating the 'As Is' situation of the business i.e., to understand the strength and weakness prevailing under the existing circumstances,
 - Deciding the 'Would be' situation for the business i.e., the changes expected after the implementation of ERP,
 - Reengineering the Business Process to achieve the desired results in the existing processes,
 - Evaluating the various available ERP packages to assess suitability,
 - Finalizing of the most suitable ERP package for implementation,
 - Installing the required hardware and networks for the selected ERP package,
 - Finalizing the Implementation consultants who will assist in implementation, and
 - Implementing the ERP package.
5. **Risk and Governance Issues in an ERP:** Organizations face several new business risks when they migrate to real-time, integrated ERP systems. Those risks include: Single Point of Failure, Structural Changes, Job Role Changes, Online Real-time, Change Management, Distributed Computing Experience, Broad System Access, Dependency on external assistance, Program interfaces and data conversions, Audit Expertise. More recently, some of the additional risks and good governance issues introduced by the e-enabled ERP environments concern: Single sign on, Data Content Quality, and Privacy and Confidentiality.
6. **Sample List of ERP Vendors:** This list includes: Baan, Business Planning and Control System (BPCS), Mapics XA (Marcam Corporation), MFG/Pro (QAD), Oracle Applications (Oracle), Prism (Marcam Corporation), R/3 (SAP), System 21 (JBA)
7. **ERP Software Package (SAP):** SAP has a number of Application Modules in the package. Some of these modules are: Financials, Controlling, Investment Management, Treasury, Integrated Enterprise Management, Sales and Distribution, Production Planning and Control, Materials Management, Human Resource Management, and Internet and Intranet.
 - 7.1 **Financials:** This includes: Financial Accounting, General Ledger, Accounts receivable and payable, Fixed Asset Accounting.

- 7.2 Controlling Cost:** This includes: Overhead Cost Control, Cost Center Accounting, Overhead Orders, Activity based Costing, Product Cost Control, Cost Object Controlling, Profitability Analysis.
- 7.3 Investment Management:** It includes: Corporate wide budgeting, Appropriation requests, Investment measures, Automatic settlement to fixed assets, Depreciation Forecast.
- 7.4 Treasury:** It includes: Cash Management, Treasury Management, Market risk management, Funds Management,
- 7.5 Enterprise Controlling:** Enterprise can be managed by using an Integrated Enterprise Management. This consists of getting accounting data prepared by subsidiaries for corporate reporting which will be automatically prepared simultaneously within the local books of each subsidiary. This data is transferred to a module called Enterprise Controlling (EC). Enterprise Controlling consists of three modules: EC-CS, EC-PCA, and EC-EIS.
- 7.6 Product Data Management (PDM):** PDM supports in creating and managing product data throughout product lifecycle. SAP supports two basic scenarios in PDM environment.
- 7.7 Sales and Distribution:** The system's Sales and Distribution application offers access to real-time, online information from sales support to the billing process.
- 7.8 Production Planning and Control:** This module is used for planning, executing and controlling production. This covers the complete production process starting from creation of master data, production planning, MRP, capacity planning, production control and costing. Product planning modules are: Sales and Operation Planning (SOP), Production Control Modules, Quality Management, Project System, Project Information System.
- 7.9 Materials Management:** The system's materials management module contains all functions required to simplify business processes in Requirements planning, Purchasing, Inventory Management, Warehouse management and Invoice Verification. It also introduces a high degree of automation into standard procedures.
- 7.10 Human Resource Management (HR):** HR provides comprehensive process driven solutions that can address organization's human resources needs worldwide. The module consists of various components such as Personnel

Information Systems Control and Audit

Management, Personnel administration, Recruitment management, Travel Management, Benefits administration, Salary administration etc.

7.11 Payroll Accounting: R/3 HR payroll accounting addresses payroll functions from a global point of view. It is possible to centralize or decentralize payroll processing based on country or legal entities. It also enables to establish business rules without modifying existing payroll. This includes: Payroll Processing, Integration, Global Solutions, Time Management, Time data, Time evaluation, Time management Review, Integration and Interfaces, and Shift Planning.

7.12 Internet and Intranet: The R/3 system offers a special Internet functionality for large number of business processes. It also gives an opportunity to advertise vacancies to potential applicants all over the world. The application itself could be carried out online by calling up an application form filling it out and returning it by e-mail. The application would be processed automatically in R/3 HR.

Question 1

Briefly explain Enterprise Resource Planning (ERP) and describe five of its characteristics.

Answer

Enterprise Resource Planning (ERP) is the latest high-end solution, which information technology has lent to business applications. ERP solutions streamline and integrate operation processes and information flows in the company to synergize the resources of an organization namely men, material, money and machine through information. An ERP system is a fully integrated business management system covering functional areas of an enterprise like Logistics, Production, Finance, Accounting and Human Resources.

General Model of ERP: ERP is a global, tightly integrated closed loop business solution package and is multifaceted. It promises one database, one application, and one user interface for the entire enterprise, where once disparate systems ruled manufacturing, distribution, finance and sales.

An Overview of enterprise Resource Planning (ERP)

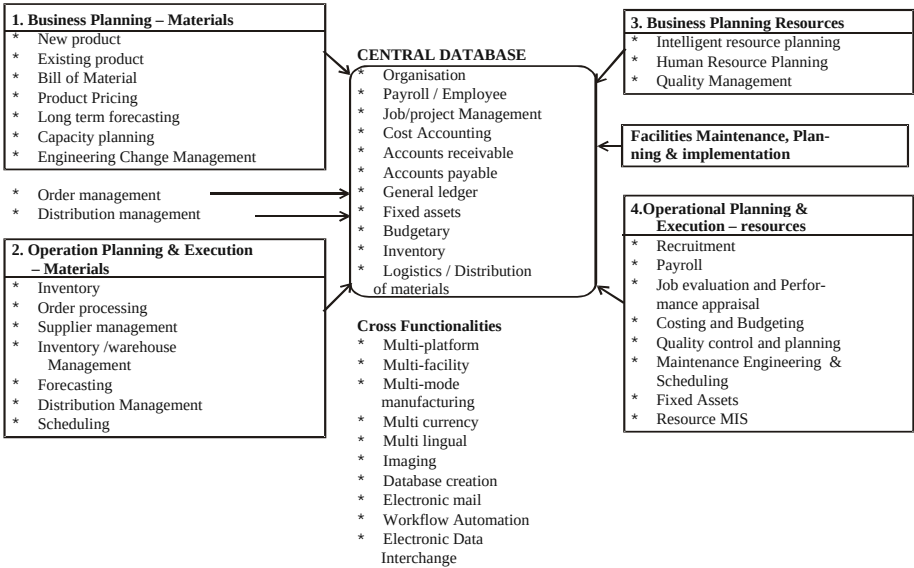


Fig.: General Model of an ERP

Taking information from every function it is a tool that assists employees and manager's plan, monitor and control the entire business. A modern ERP system enhances a manufacturer's ability to accurately schedule production, fully utilize capacity, reduce inventory, and meet promised shipping dates. ERP systems are implemented in a three Tier Client Server Architecture; the server stores the data, maintaining its integrity and consistency and processes the requests of the user from the client desktops. The load of data processing and application logic is divided between the server and the client. As companies implementing ERP solutions have multiple locations of operation and control, online data transfer has to be done across locations. To facilitate these transactions, the important enabling technologies for ERP systems are Workflow, Work group, Group Ware, Electronic Data Interchange (EDI), Internet, Intranet, Data warehousing, etc.

ERP Characteristics: An ERP system is not only the integration of various organization processes, any system has to possess few key characteristics to qualify for a true ERP solution. These features are:

- **Flexibility:** An ERP system should be flexible to respond to the changing needs of an enterprise. The client server technology enables ERP to run across various database back ends through Open Database Connectivity (ODBC).
- **Modular and Open:** ERP system has to have open system architecture. This means that any module can be interfaced or detached whenever required without affecting the other modules. It should support multiple hardware platforms for the

Information Systems Control and Audit

companies having heterogeneous collection of systems. It must support some third party add-ons also.

- **Comprehensive:** It should be able to support variety of organizational functions and must be suitable for a wide range of business organizations.
- **Beyond The Company:** It should not be confined to the organizational boundaries, rather support the on-line connectivity to the other business entities of the organization.
- **Best Business Practices:** It must have a collection of the best business processes applicable worldwide. An ERP package imposes its own logic on a company's strategy, culture and organization.

Question 2

What is an ERP?

Answer

ERP: "An Enterprise resource planning system is a fully integrated business management system covering functional areas of an enterprise like logistics, production, finance, accounting and human resources".

It organizes and integrates operation processes and information flows to make optimum use of resources such as men, material, money and machine.

"Enterprise resource planning promises one database, one application, and one user interface for the entire enterprise, where once disparate systems ruled manufacturing, distribution, finance and sales."

Question 3

What are the major features of ERP?

Answer

Major features of ERP:

- ERP provides multi-platform, multi-mode manufacturing, multi-currency, multi-lingual facilities.
- It supports strategic and business planning activities, operational planning and execution activities, creation of materials and resources. All these functions are effectively integrated for flow and update of information immediately upon entry of any information.
- Has end to end supply chain management to optimize the overall demand and supply data.

An Overview of enterprise Resource Planning (ERP)

- ERP facilitates company-wide integrated information system covering all functional areas like manufacturing, selling and distribution, payables, receivables, inventory accounts, human resources, purchases etc.
- ERP performs core activities and increases customers service, thereby augmenting the corporate image.
- ERP bridges the information gap across organizations.
- ERP provides complete integration of systems not only across departments but also across companies under the same management.
- ERP is the solution for better project management.
- ERP allows automatic introduction of the latest technologies like Electronic Fund Transfer (EFT), Electronic Data Interchange (EDI), Internet, Intranet, Video Conferencing, E-commerce etc.
- ERP eliminates most business problems like materials shortages, productivity enhancements, customer service, cash management, inventory problems, quality problems, prompt delivery etc.
- ERP provides intelligent business tools like decision support system, Executive Information System, Data mining and easy working systems to enable better decisions.

Question 4

What is an ERP system? Bring out the major challenges involved in its implementation.

Answer

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

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

The characteristics of an ERP system are:

(1) Flexibility, (2) Open system architecture, (3) Comprehensive, (4) On-line connectivity to other business entities, (5) Collection of best business practices.

Information Systems Control and Audit

Some of the major features of ERP are:

- (1) Provides multi-platform, multi-facility, multi-currency, etc facilities
- (2) Supports strategic and business planning activities
- (3) Has end-to-end supply chain management
- (4) Provides intelligent business tools
- (5) Provides complete integration of systems
- (6) Better project management
- (7) Automatic introduction of latest technologies like EFT, EDI, Internet, etc.

The challenges involved in ERP implementation are:

- (i) Consultants, vendors and users have to work together to achieve the overall objectives of the organization. The consultants have to clearly understand the user needs and the prevailing business realities and design the business solutions keeping in mind all these factors.
- (ii) Proper customization of package to the organization has to be in tune with the users needs and business objectives.
- (iii) Roles and responsibilities of the employees have to be clearly identified, understood and configured in the system.
- (iv) Acceptance by employees for the new processes and procedures is critical for the success of the package.
- (v) Package to be implemented in totality to achieve the maximum benefit.
- (vi) Defining the implementation methodology to be followed – identifying needs, evaluation of the current situation, predicting the future situation, reengineering the business process, selection of correct package.
- (vii) Installation of hardware, software required for the package.
- (viii) Selection of right kind of consultants.
- (ix) Preparing the implementation guidelines – training users, effective leadership, adapting the new systems and making changes in the working environment etc.
- (x) Post implementation monitoring of Key Performance indicators, Critical success factors etc.

Question 5

What are the steps involved in the implementation of an ERP package?

Answer

Steps of ERP Implementation:

These steps are given as follows:

- (i) Identifying the needs for implementing an ERP package.
- (ii) Evaluating the “As Is” situation of the business i.e. to understand the strength and weakness prevailing under the existing circumstances.
- (iii) Deciding the ‘would be’ situation for the business i.e. the changes expected after the implementation of ERP.
- (iv) Re-engineering the Business Process to achieve the desired results in the existing processes.
- (v) Evaluating the various available ERP packages to assess suitability.
- (vi) Finalizing of the most suitable ERP package for implementation.
- (vii) Installing the required hardware and networks for the selected ERP package.
- (viii) Finalizing the implementation consultants who will assist in implementation.
- (ix) Implementing the ERP package.

Question 6

Write down the general guidelines which are to be followed before starting the implementation of an ERP package.

Answer

Implementation Guidelines For ERP: There are certain general guidelines, which are to be followed before starting the implementation of an ERP package:

- (i) Understanding the corporate needs and culture of the organization and then adopt the implementation technique to match these factors.
- (ii) Doing a business process redesign exercise prior to starting the implementation.
- (iii) Establishing a good communication network across the organization.
- (iv) Providing a strong and effective leadership so that people down the line are well motivated.
- (v) Finding an efficient and capable project manager.
- (vi) Creating a balanced team of implementation consultants who can work together as a team.

Information Systems Control and Audit

- (vii) Selecting a good implementation methodology with minimum customization.
- (viii) Training end-users.
- (ix) Adapting the new system and making the required changes in the working environment to make effective use of the system in future.

Question 7

ABC Limited has recently migrated to real-time Integrated ERP System. As an IS Auditor, advice the company as to what kinds of businesses risks it can face?

Answer

The company, ABC Limited may face several new business risks when they migrate to real-time, integrated ERP systems. These risks include the following:

1. *Single point of failure* – All input data of an organization and transaction processing is within one application system.
2. *Structural Changes* - Significant personnel and organizational structural changes associate with reengineering or redesigning business processes.
3. *Job Role Changes* - Traditional roles of users are changed to empowered-based role. They have more chances to access enterprise information in real-time. This point of control shifts from the back-end financial processes to the front-end point of creation.
4. *Online Real-Time* – This environment requires a continuous business interaction. This warrants the capabilities of utilizing the ERP application and responds quickly to any problem that requires a 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).
5. *Change Management* - It is challenging to bring together a highly integrated environment when different business processes have existed among business units for long. The level of user acceptance of the system has a significant influence on its success. Training and awareness of users is mandatory, to understand that their actions or inaction have a direct impact upon other users and in the performance of their day-to-day duties.
6. *Distributed Computing Experience* - Inexperience with implementing and managing this kind of environment may pose significant challenges.
7. *Broad System Accessibility* – Increased remote access by users and outsiders and high integration among application functions allow increased access to the application and data.

An Overview of enterprise Resource Planning (ERP)

8. *Dependency on External Assistance* – Organization accustomed to in-house legacy systems may find that 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 a greater risk.
9. *Program Interfaces and Data Conversions*–Extensive interfaces and data conversions from legacy systems and other commercial software are necessary. The exposures of data integrity, security and capacity requirements for ERP are much higher.
10. *Audit Expertise* – Specialist expertise is required to effectively audit and control an ERP environment. The relative complexity of ERP systems has created specialization 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 organization's business processes, have to maintain a good grasp of all the core modules to function effectively.
11. *Single sign on* - It reduces the security administration efforts associated with administrating web-based access to multiple systems, but simultaneously introduces additional risks in that an incorrect assignment of access may result in inappropriate access to multiple systems.
12. *Data content quality* - As enterprise applications are opened to external suppliers and customers, the need for integrity in enterprise data becomes paramount.
13. *Privacy and confidentiality* - Regularity and governance issues surrounding the increased capture and visibility of personal information, i.e. spending habits.

Question 8

Identify the risks and governance issues an organization faces while migrating to an integrated ERP system.

Answer

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.

Information Systems Control and Audit

- **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 specialization 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 organization'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 administering 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.

Question 9

Write a detailed note on the expectations, fears and the ground realities that a corporate management faces during the post-implementation phase of ERP.

Answer

Most of the post-implementation problems of ERP can be traced to wrong expectations and fears. Sometimes it is also due to the ERP vendors and their pre-implementation sales hype. Popular expectations are:

- An improvement in processes,
- Increased productivity on all fronts,
- Total automation and disbanding of all manual processes,
- Improvement of all key performance indicators,
- Elimination of all manual record keeping,
- Real time information system available to concerned people on a need basis,
- Total integration of all operations.

ERP software attempts to integrate all departments and functions across the enterprise onto a single computer system that serves the individual requirements of different departments. Instead of having discreet systems for finance and HR, it provides a common system for all. So if required, the materials department can view pending orders and instantly calculate the quantity of raw materials to be purchased. This keeps inventory levels within safe limits and hence controls costs. While all this may sound like a silver bullet to enterprises, ERP has gone sour for many companies in the past. The problems have been primarily with integration. Also, the software required people to change their business processes too drastically.

Information Systems Control and Audit

An ERP implementation impacts people, systems, and the organization as a whole and barriers are expected from these areas since work processes are expected to be altered when ERP is introduced. Business processes, roles, and responsibilities undergo change. And when this happens, the organizations encounter a sticky issue called 'resistance to change'.

In the evaluation stage, users should articulate their business requirements and see whether a particular ERP solution meets their needs. This way one can close the gap between what the package offers and the business requirements. Implementation should not begin without this. Often, employees have high expectations and think ERP will solve most business problems. It is necessary to make realistic and accurate expectations before embarking on an ERP project. This is addressed by preparing a project charter stating the realistic expectations, and key performance parameters to be focused on during the project, and project measurement. Having defined this, it is necessary to communicate this to the stakeholders in the ERP project.

Some of the fears on ERP implementations are:

- Job redundancy.
- Loss of importance as information is no longer an individual prerogative.
- Change in job profile:
- An organizational fear of loss of proper control and authorization.
- Increased stress caused by greater transparency.
- Individual fear of loss of authority.

Since ERP introduces transparency in operations and brings about more discipline, people who are empowered are bound to oppose it. People who are very used to a particular system or a certain set of processes, would not accept an alternative like ERP so easily and would not adapt to the new system. Change management is about handling the issues arising due to differences in legacy processes/ systems and the new ERP system. Business processes may have to be re-engineered for ERP, something that is bound to draw disapproval, especially from function heads.

Balancing the expectations and fears is a very necessary part of the implementation process. The ground realities are:

- Changing the organization involves three levers-strategies, business process and change, and consequential organization change.
- In most companies in India, many process related key performance indicators have not been measured till now, either because the company did not feel it necessary or lacked the tools to do so. Measuring such indicators brings in new culture.

An Overview of enterprise Resource Planning (ERP)

- The genetic nature of the ERP packages is such that there would be processes peculiar to some sectors and organizations, which may have to be kept out of the process.
- Some of the processes are better done manually.

ERP should be treated as a business project—not an IT project driven by the Information Systems. Changing the organization requires mindset change. Without a willingness to change, it would be a classic case of an old organization plus new technology leading to an expensive old organization. So, it is important to get the involvement of the function heads and top business executives. An organization must also be prepared for ERP and be clear about its requirements. This necessitates knowing the business objectives and goals, and mapping the processes to these. ERP is just the enabler that automates the entire process. The objectives for ERP must also be identified, documented, and communicated.

A successful ERP implementation is not the end of the road as far as change is concerned, and continuous improvements are required to reap the benefits. The expectations, fears and reality can most obviously be balanced during the process of implementation itself.

Question 10

Write short notes on the following:

- (a) *Benefits of Enterprise Resource Planning*
- (b) *Business Process Reengineering (BPR).*

Answer

(a) **Benefits of Enterprise Resource Planning (ERP):**

The benefits that are achieved by implementing ERP packages are:

- They make best uses of various resources
- Reduce paper documents by providing online formats for quickly entering and retrieving information.
- Improves timeliness of information by permitting posting daily instead of monthly.
- Greater accuracy of information with detailed content, better presentation, satisfactory for the auditors.
- Improved cost control.
- Faster response and follow up on customers

Information Systems Control and Audit

- More efficient cash collection.
- Better monitoring and quicker resolution of queries.
- Help to achieve competitive advantage by improving its business process.
- Improves supply demand linkage with remote locations and branches in different countries.
- Improves international operations by supporting a variety of tax structures, invoicing schemes, multiple currencies etc.
- Improves information access and management throughout the enterprise.

(b) **Business Process Reengineering (BPR):** ERP is a result of a modern Enterprise's concept of how the Information System is to be configured to the challenging environments of new business opportunities. However, merely putting in place an information system is not enough. Every company that intends to implement ERP has to re-engineer its processes in one form or the other. This process is known as Business Process Reengineering (BPR). BPR is the fundamental rethinking and radical redesign of processes to achieve dramatic improvement in critical, contemporary measure of performance such as cost, quality, service and speed.

Radical Redesign means BPR is reinventing and not enhancing or improving. According to BPR philosophy, whatever was being done in past, it was all wrong, so one has to reassemble the new system to redesign it afresh. There is no point in simplifying or automating a business process, which does not add any value to the customer; such business processes should be eliminated altogether.

BPR aims at major transformation of the business processes to achieve dramatic improvement. Here, the business objectives of the enterprise such as profits, customer– satisfaction through optimal cost, quality, deliveries etc. are achieved by transformation of the business processes which may, or may not, require the use of IT.

The concept of BPR when merges with the concept of IT, the business engineering emerges, which is the rethinking of Business Processes to improve speed, quality and output of materials or services. In other words, business engineering is the method of development of business processes according to changing requirements.

Question 11

Write short notes on Business Engineering.

Answer

Business Engineering has come out of merging of two concepts namely Information Technology and Business Process Reengineering. Business Engineering is the rethinking of Business Processes to improve speed, quality and output of materials or services. The emphasis of business engineering is the concept of Process Oriented Business Solutions enhanced by the client-server computing in information technology. The main point in business engineering is the efficient redesigning of company's value added chains. Value added chains are a series of connected steps running through a business which when efficiently completed, add value to enterprise and customers. Information technology helps to develop business models, which assist in redesigning of business processes.

In short, Business Engineering is the method of development of business process according to changing requirements.

Question 12

Discuss the functions and facilities provided by Treasury Cash Management module of an ERP package.

Answer

Treasury Cash Management: Treasury Cash Management component allows the analysis of financial transactions for a given period. It identifies and records future developments for the purpose of financial budgeting.

In Treasury Cash Management, the company's payment transactions are grouped into cash holdings, cash inflows and cash outflows. Cash Management module provides:

- (i) Information on the sources and uses of funds to secure liquidity to meet payment obligations when they become due.
- (ii) Monitors and controls incoming and outgoing payments flows.
- (iii) Supplies data required for managing short term market investment and borrowings.
- (iv) Enables to know current cash position, short term cash management and medium and long term financial budgeting.
- (v) Enables analysis of liquidity.
- (vi) Helps in cash management decisions.
- (vii) In bank accounting, it helps in electronic banking and control functions for managing and monitoring of bank accounts.

Information Systems Control and Audit

- (viii) The liquidity forecast function integrates anticipated payment flows from financial accounting, purchasing and sales to create liquidity outlook from medium to long term.
- (ix) Covers foreign currency holdings and foreign currency items.

Question 13

List any five ERP Vendors and briefly describe the ERP packages offered by them.

Answer

There are quite a few ERP packages available in the market these days. Some of these are developed indigenously also. However, these indigenous packages may not be able to compete with the global ERP packages in terms of functionality and coverage of business segments and scale. Some of the global packages along with the vendors are listed below:

- **Baan (The Baan Company):** Initially developed for an aircraft company, it was subsequently launched as a generalized package in 1994. It offers sound technology and coverage of broad functional scope.
- **Business Planning and Control System (BPCS):** It targets only manufacturing companies. It offers strong functionality for discrete and Kanban manufacturing. However, it lags in process oriented implementation tools and workflow.
- **Mapics XA (Marcam Corporation):** It is viewed by many as a legacy application.
- **MFG/Pro (QAD):** Strong in repetitive manufacturing, originally designed to meet MRPII standards, it offers reliable manufacturing functionality and straight forward implementation.
- **Oracle Applications (Oracle):** It gives Internet-enabled, network-centric computing. It also offers database, tools, implementation, applications and UNIX operating systems under one stop-shop umbrella. It is currently running on wide choice of hardware.
- **R/3 (SAP):** It is a market leader with excellent philosophy of matching business processes with its modules. It covers almost all business segments.
- **Systems 21 (JBA) :** Its software license revenues are small compared to other major ERP vendors. It offers a rugged, reliable manufacturing solution.

Question 14

Identify the SAP module used to consolidate the financial statements including elimination of inter-company transactions.

Answer

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 three 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.

Question 15

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

Information Systems Control and Audit

Answer

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.

Question 16

XYZ Company, engaged in the manufacturing of several types of electronic goods is having its branches all over the World. The company wishes to centralize and consolidate the information flowing from its branches in a uniform manner across various levels of the Organization.

The factories are already working on legacy systems using an intranet and collating information. But each factory and branch is using different software and varied platforms, which do not communicate with each other. This not only results in huge inflow of data which could not be consolidated for analysis but also the duplication of data. Even one percent change in any data entry or analysis translates into millions of Rupees and can sometimes wipe out the profits of the organization. So the company needs a system that would help them to be responsive and act fast.

Information Systems Control and Audit

Read the above carefully and answer the following with justifications:

- (a) *What are the problems that the company is facing now?*
- (b) *Should the company go for ERP solution? If yes, will the company be able to share a common platform with its dealers to access servers and database to update the information of issues of mutual interest?*
- (c) *For the selection of ERP package, state the issues to be considered.*
- (d) *Suggest how to go about the implementation of ERP package.*

Answer

- (a) XYZ company, having its branches all over the world, is engaged in manufacturing of several types of electronic goods. It is confronted with the problem of centralizing and consolidating the information flowing in from its various branches in uniform manner across various levels of the organization.

No doubt, the factories are working on legacy systems using an intranet and collating information. As each factory is using different type of software on varied platforms, therefore, they are not able to communicate with each other. Because of this reason, there is a huge inflow of data which could not be consolidated for analysis. Lack of communication among factories has not only resulted into duplication of the data entry which is not only costly, slight change in data entry and analysis may translate into millions of rupees that can sometimes wipe out the profits of the organization. Hence, there is an urgent need of a system that would help the branches to be responsive and to act fast.

- (b) Yes, the company should go for ERP solutions. ERP implementation brings different business functions, personalities, procedures, ideologies and philosophies on one platform, with an aim to pool knowledge base to effectively integrate and bring worthwhile and beneficial changes throughout the organization. Some of the major features of ERP are that it provides the support to multi platform, multi facility, multi mode, manufacturing, multi currency, multi lingual facilities. It supports strategic and business planning activities, operational planning and execution activities, creation of material and resources. All these functions are effectively integrated for flow and updation of information immediately upon entry of any information, thereby providing a company-wide Integrated Information System.

In case, the company decides to include a module for dealers which provides limited/restricted access to company databases and server, dealers will be able to update the information of issues of mutual interest.

- (c) While selecting the ERP package, the performance of following issues should be taken into account:
- (i) Better inventory management and control.
 - (ii) Improved financial reporting and control.
 - (iii) Automation of certain tasks that were performed manually to increase productivity.
 - (iv) Improved production planning.
 - (v) Better information on stocks at various locations.
 - (vi) Using an integrated system as opposed to disparate systems at different locations, thereby eliminating errors of duplicate entries.
 - (vii) More accurate costing of products.
 - (viii) Better credit control.
 - (ix) Improved cash flow planning.
 - (x) Automatic quality control and tracking.
 - (xi) Better after sales services.
 - (xii) Better information and reporting to top management.
- (d) In the stated scenario, several steps involved in the implementation of a typical ERP package are enumerated below:
- (i) Identifying the needs for implementing an ERP package.
 - (ii) Evaluating the 'As Is' situation of the business i.e., to understand the strength and weakness prevailing under the existing circumstances.
 - (iii) Deciding the 'Would be' situation for the business i.e., the changes expected after the implementation of ERP.
 - (iv) Reengineering the Business Process to achieve the desired results in the existing processes.
 - (v) Evaluating the various available ERP packages to assess suitability.
 - (vi) Finalizing of the most suitable ERP package for implementation.
 - (vii) Installing the required hardware and networks for the selected ERP package.
 - (viii) Finalizing the Implementation consultants who will assist in implementation.
 - (ix) Implementing the ERP package.

Information Systems Control and Audit

Question 17

Worldwide, a global telecom company is serving to more than 10 million customers in the area of communications through fixed land lines, mobiles, internet services, digital TV and satellite system etc.

The financial analysts of the company are located in different functional groups in six geographical regions. These analysts are missing the access to the same data, as well as timely access to the information. Dated budget and actual numbers for each business unit reside in seven different systems, separating critical components of the Profit and Loss account and inhibiting analyst's ability to assess results. The problem gets further complicated as the field analysts are not able to go to one universal place to retrieve the data themselves and they have to rely upon the home office for the same.

The objective of the company is to set some critical financial goals so that the company could remain competitive and increase market share.

Read the above carefully and answer the following with justifications:

- (a) To overcome the problems which the financial analysts are facing, what kind of software the company should select?*
- (b) The company is advised that the adoption of BS7799 International Standard will help in overcoming the problems and achieving its goals. Discuss.*
- (c) How should the human resources be enriched for effective utilization of the proposed new systems and standards?*

Answer

- (a)** As the financial analysts of the company are working in six different geographical locations and the financial data is stored on seven different systems, located world wide, therefore they are facing several problems. Few of them are as under:
- Missing the access to the same data as well as timely access to information.
 - Dated budget and actual numbers for each business unit reside in seven different systems, separating critical components of the profit and loss account thus failing the financial analysts to assess results.
 - The field analysts are not able to retrieve the data themselves from one universal place and therefore they have to rely upon the home office for the same.

It is therefore important that the company should buy new software for the solution of the problems as mentioned above.

As far as software is concerned, of course the company should select the one which could make same data available to all the financial analysts. One such software is available from Oracle Corporation known as On Line Analytical Processing (OLAP) tool for better control over costs, analyze performance, evaluate opportunities, and formulate future directions. To improve the basis for making decisions quickly and accurately with real time, to provide consistent data which will improve cost control and to simplify and shorten the budgeting process, the software should be capable of the following:

- hands on ability to consolidate budgets, based on actual data in the process,
- enabling business units to make real-time, online decisions based on more accurate information,
- user friendly.

The company is expected to be benefited by significant financial saving and therefore it should reduce the length of the budgeting cycle and the number of people involved in the process, thus keeping the company financially competitive in a growing market. The system should provide online, real time access to the information.

- (b) The **BS 7799** (ISO 17799) consists of 127 best security practices which companies can adopt to build their Security Infrastructure. The model helps the companies to maintain IT security through ongoing, integrated management of policies and procedures, personnel training, selecting and implementing effective controls, reviewing their effectiveness and improvement. The benefits of an Information Security Management Systems (ISMS) tuned to the objective of the company are improved customer confidence, a competitive edge, better personnel motivation and involvement, and reduced incident impact leading to increased profitability.

The company can use BS 7799 for the following reasons:

- Reduced operational risk,
- Increased business efficiency, and
- Assurance that information security is being rationally applied.

This is achieved by ensuring that:

- Security controls are justified.
- Policies and procedures are appropriate.
- Security awareness is good amongst staff and managers.
- All security relevant information processing and supporting activities are auditable and are being audited.

Information Systems Control and Audit

- Internal audit, incident reporting / management mechanisms are being treated appropriately.
- Management actively focuses on information security and its effectiveness.

Note: For details of this topic, please refer Chapter 8.

(c) The human resources involved in the systems and standards can be enriched by the following activities:

- **Training Personnel:** A system can succeed or fail depending on the way it is operated and used. Therefore, the quality of training received by the personnel involved with the system in various capacities helps in the successful implementation of information system and standards. Thus, training is a major component of systems implementation. When a new system is acquired which often involves new hardware and software, both users and computer experts need training organized by the vendor through hands-on learning techniques.
- **Training Systems Operators:** The effective implementation of new systems and standards also depend on the computer-centre personnel, who are responsible for keeping the equipment running as well as for providing the necessary support services. Their training must ensure that they are able to handle all possible operations, both routine and extra-ordinary. As part of their training, operators should be given a trouble shooting list that identifies possible problems and remedies for them. Training also involves familiarization with run procedures, which involve working through the sequence of activities needed to use a new system on an on-going basis.
- **User training:** User training deals with the operation of the system itself. Training in data coding emphasizes the methods to be followed in capturing data from transactions or preparing data for decision support activities. Users should be trained on data handling activities such as editing data, formulating inquiries (finding specific records or getting responses to questions) and deleting records of data. From time to time, users will have to prepare disks, load paper into printers, or change ribbons on printers. Some training time should be devoted to such system maintenance activities. If a micro computer or data entry system uses disks, users should be instructed in formatting and testing disks.

It is also required to have managers directly involved in evaluating the effectiveness of training activities because training deficiencies can translate into reduced user productivity level.

Note: For details of this topic, please refer Chapter 2.

EXERCISE

Question 1

Explain the characteristics of ERP in brief.

Question 2

ABC Limited has migrated from traditional systems to new real-time integrated ERP systems. The technical advisor of the company advised the owner that the company should take necessary steps to analyze several types of risks. Explain those risks in brief.

Question 3

Explain the following terms with respect to ERP:

- (a) *Business Engineering*
- (b) *Business Management*
- (c) *Business Modeling*

Question 4

What is Business Process Reengineering? Explain in brief.

Question 5

Explain the criterion for evaluation of various ERP Packages in brief.

Question 6

What is Enterprise Controlling? Briefly explain its modules.

Question 7

A company is developing several types of biscuits, having its branches all over the country. The owner of the company wishes to centralize and consolidate the information flowing from its branches in a uniform manner across various levels of the organization. The technical advisor of the company recommended that the company should go for the implementation of the ERP Package. Why the company should undertake ERP?

INFORMATION SYSTEMS AUDITING STANDARDS, GUIDELINES, BEST PRACTICES

BASIC CONCEPTS

1. **IS Auditing Standards:** IS audit standards provide audit professionals a clear idea of the minimum level of acceptable performance essential to discharge their responsibilities effectively. There are various standards like: COSO, CoCo, HIPPA, BS 7799, COBIT 4.1.
2. **ISO 27001 – (BS7799 : Part II) – Information Security Management Standard:** BS The requirements of information security system as described by standard are stated below. An organization must take a clear view on these issues before trying to implement an Information Security Management Systems (ISMS).

2.1 Areas of focus of ISMS: There are ten areas of focus of ISMS:

2.1.1: Security Policy: This activity involves a thorough understanding of the organization business goals and its dependence on information security. This entire exercise begins with creation of the IT Security Policy. This is an extremely important task and should convey total commitment of top management. The detailed control and objectives are: information Security Policy, Information System Infrastructure, Security of third party access, Outsourcing.

2.1.2 Organizational Security: A management framework needs to be established to initiate, implement and control information security within the organization. This needs proper procedures for approval of the information security policy, assigning of the security roles and coordination of security across the organization. The detailed control and objectives are: Information System Infrastructure, Security of third party access, Outsourcing.

2.1.3 Asset Classification and Control: One of the most laborious but essential task is to manage inventory of all the IT assets, which could be information assets, software assets, physical assets or other similar services. The detailed control and objectives are: Accountability for assets, Information classification.

- 2.1.4 Personnel Security:** Human errors, negligence and greed are responsible for most thefts, frauds or misuse of facilities. Various proactive measures that should be taken are, to make personnel screening policies, confidentiality agreements, terms and conditions of employment, and information security education and training. Alert and well-trained employees who are aware of what to look for can prevent future security breaches. The detailed control and objectives are: Security in Job definition and Resourcing, User Training, Responding to security incidents and malfunctions.
- 2.1.5 Physical and Environmental Security:** This involves physical security perimeter, physical entry control, creating secure offices, rooms, facilities, providing physical access controls, providing protection devices to minimize risks ranging from fire to electromagnetic radiation, providing adequate protection to power supplies and data cables are some of the activities. Cost effective design and constant monitoring are two key aspects to maintain adequate physical security control. The detailed control and objectives are: Secure areas, Equipment Security, and General Controls.
- 2.1.6 Communications and Operations Management:** Properly documented procedures for the management and operation of all information processing facilities should be established. This includes detailed operating instructions and incident response procedures. The detailed control and objectives are: Operational Procedures and responsibilities, System Planning and Acceptance, Protection against malicious software, Housekeeping, Network Management, Media Handling and Security, and Exchanges of information and software.
- 2.1.7 Access Control:** Access to information and business processes should be controlled on the business and security requirements. The detailed control and objectives are: Business requirements for access control, User access management, User Responsibilities, Network access control, Operating system access control, Application access control, Monitoring system access and use, and Mobile computing and teleworking.
- 2.1.8 Systems Development and Maintenance:** Security should ideally be built at the time of inception of a system. Hence security requirements should be identified and agreed prior to the development of information systems. This begins with security requirements analysis and specification and providing controls at every stage i.e. data input, data

processing, data storage and retrieval and data output. It may be necessary to build applications with cryptographic controls. There should be a defined policy on the use of such controls, which may involve encryption, digital signature, use of digital certificates, protection of cryptographic keys and standards to be used for cryptography. The detailed control and objectives are: Security Requirements of system, Security in application systems, Cryptographic Controls, Security of system files, and Security in development and support process.

2.1.9 Business Continuity Management: A business continuity management process should be designed, implemented and periodically tested to reduce the disruption caused by disasters and security failures. There is only one control: Aspects of business continuity management.

2.1.10 Compliance: It is essential that strict adherence is observed to the provision of national and international IT laws, pertaining to Intellectual Property Rights (IPR), software copyrights, safeguarding of organizational records, data protection and privacy of personal information, prevention of misuse of information processing facilities, regulation of cryptographic controls and collection of evidence. The detailed control and objectives are: Compliance with legal requirements, Review of security policy and technical compliance, and System Audit Consideration.

4. **Capability Maturity Model (CMM):** The Capability Maturity Model for Software provides software organizations with guidance on how to gain control of their processes for developing and maintaining software and how to evolve toward a culture of software engineering and management excellence. This model has total five levels of maturity: Level 1-The Initial Level, Level 2-The Repeatable Level, Level 3-The Defined Level, Level 4- The Managed Level, Level 5- The Optimizing Level.
5. **COBIT- IT Governance Model:** 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. There are four domains identified for the high level classification: Planning and Organization, Acquisition and Implementation, Delivery and Report, Monitoring.
6. **COSO:** 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.

Information Systems Control and Audit

7. **COCO:** The “Guidance on Control” report, known colloquially as CoCo, was produced in 1999 by the Criteria of Control Board of The Canadian Institute of Chartered Accountants. CoCo does not cover any aspect of information assurance. It is concerned with control in general. CoCo is “guidance,” meaning that it is not intended as “prescriptive minimum requirements” but rather as “useful in making judgments” about “designing, assessing and reporting on the control systems of organizations.”
8. **IT Infrastructure Library (ITIL):** The IT Infrastructure Library (ITIL) is so named as it originated as a collection of books (standards) each covering a specific 'practice' within IT management. After the initial published works, the number of publications quickly grew (within ITIL v1) to over 30 books. This basically includes: Service Support, Problem Management, Configuration Management, Release Management, Service Delivery, Service Level Management, Capacity Management, Security Management, ICT Infrastructure Management, Business Perspective, Application Management, and Software Asset Management.
9. **Sys Trust and Web Trust:** SysTrust and WebTrust are two specific services developed by the AICPA that are based on the Trust Services Principles and Criteria. SysTrust engagements are designed for the provision or advisory services or assurance on the reliability of a system. WebTrust engagements relate to assurance or advisory services on an organization's system related to e-commerce.
10. **HIPPA:** The Health Insurance Portability and Accountability Act (HIPAA) were enacted by the U.S. Congress in 1996. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The AS provisions also address the security and privacy of health data.
11. **SAS 70- Statement of Auditing Standards for Service Organizations:** Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). 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.

Question 1

What do you understand by Software Process Maturity? Discuss five levels of Software Process Maturity of Capability Maturity Model (CMM).

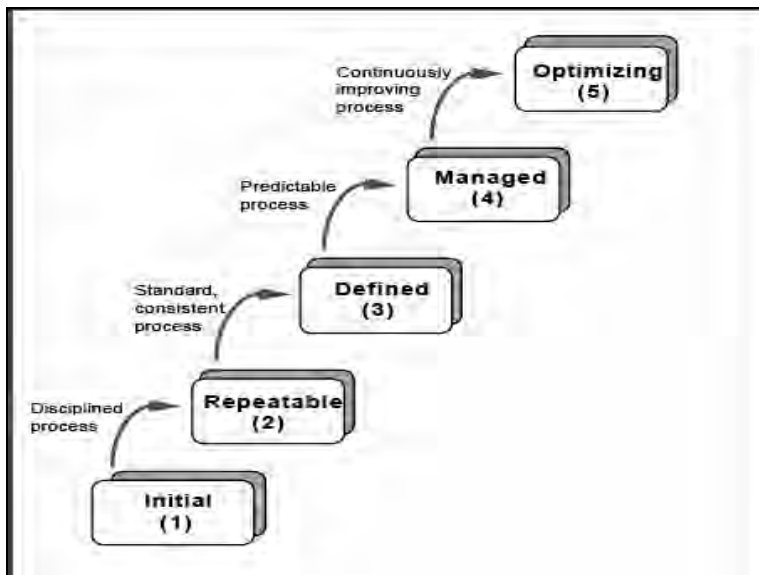
Answer

A software process is a set of activities, methods, practices, and transformations that are used to develop and maintain software and the associated products such as project plans, design documents, code, test cases, and user manuals.

Software process maturity is the extent to which a specific process is explicitly defined, managed, measured, controlled, and effective. Maturity implies a potential for growth in capability and indicates both the richness of an organization's software process and the consistency with which it is applied in projects throughout the organization. As a software organization gains in software process maturity, its institutionalization in software process building takes place.

The Five Levels of Software Process Maturity

Continuous process improvement is based on many small, evolutionary steps rather than revolutionary innovations. The CMM provides a framework for organizing these evolutionary steps into five maturity levels that lay successive foundations for continuous process improvement. These five maturity levels are discussed below and shown in the figure:



- (i) *Level 1 - The Initial Level:* At the Initial Level, the organization typically does not provide a stable environment for developing and maintaining software. At this Level, capability is a characteristic of the individuals, not of the organization. During a crisis of
-

Information Systems Control and Audit

software success depends entirely on having an exceptional manager and a seasoned and effective software team. But if someone leaves the project, it is difficult to handle the crises and a challenging task.

- (ii) *Level 2 - The Repeatable Level:* At this Level, policies for managing a software project and procedures to implement those policies are established. Planning and managing new projects is based on experience with similar projects. An effective process can be characterized as one which is practiced, documented, enforced, trained, measured, and able to improve. This Level makes the organizations to install basic software management controls. Software project standards are defined. The project's process is under the effective control of a project management system, following realistic plans based on the performance of previous projects.
- (iii) *Level 3 - The Defined Level:* At this Level, documentation for development and maintenance is prepared. This standard process is referred to throughout the CMM as the organization's standard software process, to help the software managers and technical staff performs more effectively. A group of experts standardize the process. An organization-wide training program is implemented to ensure that the staff and managers have the knowledge and skills required to fulfill their assigned roles. This process capability is based on a common, organization-wide understanding of the activities, roles, and responsibilities in a defined software process.
- (iv) *Level 4 - The Managed Level:* At the Managed Level, the organization sets quantitative quality goals for both software products and processes. Productivity and quality are measured for important software process activities across all projects as part of an organizational measurement program. An organization-wide software process database is used to collect and analyze the data available from the projects' defined software processes.

This level of capability allows an organization to product trend in process and product quality within qualitative limits. Because of the stability and measured data when some exceptional circumstance occurs, the special cause of variation can be identified and addressed. The software products are of predictably high quality.
- (v) *Level 5 - The Optimizing Level:* The entire organization is focused on continuous process improvement. The organization has the means to identify weaknesses and strengthen the process proactively, with the goal of preventing the occurrence of defects. Data on the effectiveness of the software process is used to perform cost benefit analyses of new technologies and proposed changes to the organization's software process. In short, the cost of development is cut, best engineering practices are developed and used. Continuous improvement is done. Technology and process improvements are planned and managed as ordinary business activities.

Question 2

When an organization is audited for the effective implementation of ISO 27001-(BS 7799: part II)-Information Security Management System, what are to be verified under.

- (i) *Establishing Management Framework*
- (ii) *Implementation*
- (iii) *Documentation.*

Answer

ISO 27001 –(BS7799: Part II) – Specification for Information Security Management Systems

It deals with the Information Security Management Standard (ISMS). In general, organizations shall establish and maintain documented ISMS addressing assets to be protected, organization approach to risk management, control objectives and control, and degree of assurance required.

- (i) **Establishing Management Framework:** This would include the following activities:
 - Define information security policy;
 - Define scope of ISMS including functional, asset, technical, and locational boundaries;
 - Make appropriate risk assessment ;
 - Identify areas of risk to be managed and degree of assurance required;
 - Select appropriate controls;
 - Prepare Statement of Applicability.
- (ii) **Implementation:** Effectiveness of procedures to implement controls to be verified while reviewing security policy and technical compliance.
- (iii) **Documentation:** The documentation shall consist of evidence of action undertaken under establishment of the following:
 - Management control
 - Management framework summary, security policy, control objective, and implemented control given in prepare Statement of Applicability
 - Procedure adopted to implement control under Implementation clause
 - ISMS management procedure

Information Systems Control and Audit

- Document Control: The issues focused under this clause would be
 - o Ready availability
 - o Periodic review
 - o Maintain version control;
 - o Withdrawal when obsolete
 - o Preservation for legal purpose
- Records: The issues involved in record maintenance are as follows:
 - o Maintain to evidence compliance to Part 2 of BS7799.;
 - o Procedure for identifying, maintaining, retaining, and disposing of such evidence;
 - o Records to be legible, identifiable and traceable to activity involved.
 - o Storage to augment retrieval, and protection against damage.

Question 3

Briefly explain Asset Classification and Control under Information Security Management Systems.

Answer

Asset Classification and Control

One of the most laborious but essential task is to manage inventory of all the IT assets, which could be information assets, software assets, physical assets or other similar services. These information assets need to be classified to indicate the degree of protection. The classification should result into appropriate information labeling to indicate whether it is sensitive or critical and what procedure, is appropriate to copy, store, transmit or destruction of the information asset.

An Information Asset Register (IAR) should be created detailing each of the following information assets within the organization:

- Databases
- Personnel records
- Scale models
- Prototypes
- Test samples
- Contracts
- Software licenses
- Publicity material

The Information Asset Register (IAR) should also describe who is responsible for each information asset and whether there is any special requirement for confidentiality, integrity or availability. For administrative convenience, separate register may be maintained under the subject head of IAR e.g. 'Media Register' will detail the stock of software and its licenses. One major advantage of following this practice is that, it provides a good back-up for example, in case the carton/label containing password is accidentally misplaced, media register will provide the necessary information. Similarly, 'Contracts Register' will contain the contracts signed and thus other details. The impact that is an addendum to mere maintenance of a register is control and thus protection of valuable assets of the corporation. The value of each asset can then be determined to ensure that appropriate security is in place.

The detailed **control and objectives** thereof are as follows:

- *Accountability for assets*: to maintain appropriate protection of organizational assets,
- *Information Classification*: to ensure that information assets receive an appropriate level of protection.

Question 4

Discuss 'Physical and Environmental Security with Control and Objectives' with respect to information Security Policy?

Answer

Physical and Environmental Security: This is the beginning point of any security plan. It is designed to prevent unauthorized access, damage and interference to business premises and information. This involves physical security perimeter, physical entry control, creating secure offices, rooms, facilities, providing physical access controls, providing protection devices to minimize risks ranging from fire to electromagnetic radiation, providing adequate protection to power supplies and data cables. Cost effective design and constant monitoring are two key aspects to maintain adequate physical security control.

Maintenance of the physical operating environment in a computer server room is as important as ensuring that paper records are not subject to damage by mould, fire or fading. Supporting equipments such as air conditioning plant etc. should be properly maintained. Physical controls may be difficult to manage as they rely to some extent on building structure, but good physical security can be very effective.

The detailed **control and objectives** for this type of security are:

- *Secure areas*: To prevent unauthorized access, damage and interference to business premises and information,
- *Equipment Security*: To prevent loss, damage or compromise of assets and interruption to business activities, and
- *General Controls*: To prevent compromise or theft of information and information processing facilities.

Information Systems Control and Audit

Question 5

"The effective way a service organization can communicate information about its controls is through the Service Auditor's Reports". Explain.

Answer

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 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 Report	I Type Report	II
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.

Question 6

State the benefits to a service organization from having a SAS 70 engagement performed.

Answer

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).

Information Systems Control and Audit

Question 7

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.

Answer

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.

Question 8

Define COBIT Framework and briefly state its domains of control objectives.

Answer

The **Control Objectives for Information and related Technology (COBIT)** is a set of best practices (framework) for information technology (IT) management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1996. COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company.

COBIT was first released in 1996. Its mission is “to research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors.” Managers, Auditors, and users benefit from the development of COBIT because it helps them understand their IT systems and decide the level of security and control that is necessary to protect their companies’ assets through the development of an IT governance model.

COBIT 4.1 has 34 high level processes that cover 210 control objectives categorized in four domains: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring and Evaluation. COBIT provides benefits to managers, IT users, and auditors. Managers’ benefit from COBIT as it provides them with a foundation upon which IT related decisions and investments can be based. Decision making is more effective because COBIT aids management in defining a strategic IT plan, defining the information architecture, acquiring the necessary IT hardware and software to execute an IT strategy, ensuring continuous service, and monitoring the performance of the IT system. IT users benefit from COBIT because of the assurance provided to them by COBIT’s defined controls, security, and process governance. COBIT benefits auditors because it helps them identify IT control issues within a company’s IT infrastructure. It also helps them corroborate their audit findings.

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

Information Systems Control and Audit

PO3	Determine Technological Direction
PO4	Define the IT Processes, Organization 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 : 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 : 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

Information Systems Auditing Standards, Guidelines, Best Practices

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 : 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 : Monitor and Evaluate**Question 9**

What do you mean by Software Process Maturity?

Answer

Software Process Maturity: This is the extent to which a specific process is explicitly defined, managed, measured, controlled and effective. Maturity implies a potential for growth in capability and indicates both the richness of an organization's software process and the consistency with which it is applied in project throughout the organization. As a software organization gains in software process maturity it institutionalizes its software process via policies, standards and organizational structures. Institutionalization entails building an infrastructure and a corporate culture that supports the methods, practices and procedures of the business so that they endure after those who originally defined them have gone.

Question 10

What are the types of service auditor's reports under SAS 70?

Answer

Service Auditor's Report: The most effective ways a service organization can communicate information about its controls is through a service Auditor's Report.

Information Systems Control and Audit

There are two types of Service Auditor's Report:

- (1) Type I: A type I report describes the service organizations description of controls at a specific point in time (e.g. June 30, 2003). A type II report not only includes the service organization 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:

S. No.	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

- (2) Type II: 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 organizations controls that had been placed in operation as of a specific data 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.

Question 11

Discuss the various issues that are of primary concerns for an auditor involved in information system audit.

Answer

Auditors involved in reviewing an information system should focus their concerns on the system's control aspects. They must look at the total systems environment not just the computerized segment. This requires their involvement from the time that a transaction is initiated until it is posted to the organization's general ledger. Specifically, auditors must ensure that provisions are made for:

Information Systems Auditing Standards, Guidelines, Best Practices

- An adequate audit trail so that transactions can be traced forward and backward through the system.
- Controls over the accounting for all data (i.e. transactions) entered into the system and controls to ensure the integrity of those transactions throughout the computerized segment of the system.
- Handling exceptions to and rejections from the computer system.
- Testing to determine whether the systems perform as stated.
- Control over changes to the computer system to determine whether the proper authorization has been given.
- Authorization procedures for system overrides.
- Determining whether organization and Government policies and procedures are adhered to in system implementation.
- Training user personnel in the operation of the system.
- Developing detailed evaluation criteria so that it is possible to determine whether the implemented system has met predetermined specifications.
- Adequate controls between interconnected computer systems.
- Adequate security procedures to protect the user's data.
- Backup and recovery procedures for the operation of the system.
- Technology provided by different vendors (i.e. operational platforms) is compatible and controlled.
- Databases are adequately designed and controlled to ensure that common definitions of data are used throughout the organization, that redundancy is eliminated or controlled and that data existing in multiple databases is updated concurrently.

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

Question 12

What is the sole purpose of an Information System (IS) Audit?

Answer

The sole purpose of an Information system audit is to evaluate and review the adequacy of automated information systems to meet processing needs, to evaluate the adequacy of internal controls, and to ensure that assets controlled by those systems are adequately safeguarded.

Information Systems Control and Audit

Question 13

What is the role of an IS Auditor?

Answer

The Information System (IS) auditor is responsible for establishing control objectives that reduce or eliminate potential exposure to control risks. After the objectives of the audit have been established, the auditor must review the audit subject and evaluate the results of the review to find out areas that need some improvement. IS auditor should submit a report to the management, recommending actions that will provide a reasonable level of control over the assets of the entity.

Question 14

While performing an IS Audit, the Auditor should make sure that various objectives are met. Briefly describe them.

Answer

While performing an IS audit, auditors should ascertain that the following objectives are met:

- (i) Security provisions protect computer equipments, programs, communications and data from unauthorized access, modification, or destructions.
- (ii) Program development and acquisition is performed in accordance with management's general and specific authorization.
- (iii) Program modifications have the authorization and approval of management.
- (iv) Processing of transactions, files, reports and other computer records is accurate and complete.
- (v) Source data that is inaccurate or improperly authorized is identified and controlled according to prescribed managerial policies.
- (vi) Computer data files are accurate, complete and confidential.

Question 15

Briefly describe the various objectives to be met while performing an IS audit.

Answer

While performing an IS audit, auditors should ascertain that the following objectives are met:

- (i) Security provisions protect computer equipments, programs, communications and data from unauthorized access, modifications or destruction.
- (ii) Program development and acquisition is performed in accordance with management's general and specific authorization.

- (iii) Program modifications have the authorization and approval of the management.
- (iv) Processing of transactions, files, reports and other computer records is accurate and complete.
- (v) Source data that is inaccurate or improperly authorized is identified and handled according to prescribed managerial policies.
- (vi) Computer data files are accurate, complete, and confidential.

Question 16

A XYZ Company receives orders from customers either by telephone, facsimile or electronic data interchange. A clerk then transcribes the order into one of the company's order form to be keyed into the order entry system.

You being the information system auditor of the company, suggest various internal control procedures to be adopted to prevent inaccurate or unauthorized source data entry?

Answer

The auditor should ensure that the source data controls such as proper authorization and editing data input are integrated with the processing controls and are independent of other functions. If source data controls are inadequate, user department control over data preparation, batch control totals, and edit programs etc. should be stronger.

The following control procedures may be adopted:

- Effective handling of source data input by data control personnel.
- User authorization of source data input.
- Preparation and reconciliation of batch control totals.
- Logging of the receipt, movement and disposition of source data input.
- Check digit verification.
- Key verification.
- Use of turnaround documents.
- Computer data editing routines.
- File change listings and summaries prepared for user department review.

Although source data controls may not change often, the auditor should test them on regular basis by evaluating samples of source data.

Question 17

RST Consultants is in the process of launching a new unit to provide various services to the organizations worldwide, to assist them right from the beginning i.e. from development to

Information Systems Control and Audit

maintenance including strategic planning and e-governance areas. The company believes in the philosophy of green world i.e. uses papers to a minimum extent. COBIT is positioned to be comprehensive for management and to operate at a higher level than technology standards for information systems management. 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 e. g. Quality Requirements, Fiduciary requirements, and Security Requirements.

Read the above carefully and answer the following:

- (a) *Explain various domains covered under COBIT.*
- (b) *Describe the relevance of COBIT with other standards.*

Answer

(a) COBIT structure

COBIT covers four domains which are given as follows:

- Plan and Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

Plan and Organize

The Plan and Organize domain covers the use of information & technology and how best it can be used in a company to help achieve the company's goals and objectives. It also highlights the organizational and infrastructural form IT is to take in order to achieve the optimal results and to generate the most benefits from the use of IT. The following table lists the IT processes contained in the Planning and Organization domain.

IT PROCESSES Plan and Organize

PO1	Define a Strategic IT Plan and direction
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Processes, Organization 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

Acquire and Implement

The Acquire and Implement domain covers identifying IT requirements, acquiring the technology, and implementing it within the company's current business processes. This domain also addresses the development of a maintenance plan that a company should adopt in order to prolong the life of an IT system and its components. The following table lists the IT processes contained in the Acquire and Implement domain.

IT PROCESSES
Acquire and Implement

AI1	Identify Automated Solutions
AI2	Acquire and Maintain Application Software
AI3	Acquire and Maintain Technology Infrastructure
AI4	Enable Operation and Use
AI5	Procure IT Resources
AI6	Manage Changes
AI7	Install and Accredited Solutions and Changes

Deliver and Support

The Deliver and Support domain focuses on the delivery aspects of the information technology. It covers areas such as the execution of the applications within the IT system and its results as well as the support processes that enable the effective and efficient execution of these IT systems. These support processes include security issues and training. The following table lists the IT processes contained in the Deliver and Support domain.

IT PROCESSES
Deliver and Support

DS1	Define and Manage Service Levels
DS2	Manage Third-party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS6	Identify and Allocate Costs
DS7	Educate and Train Users
DS8	Manage Service Desk and Incidents
DS9	Manage the Configuration

Information Systems Control and Audit

DS10	Manage Problems
DS11	Manage Data
DS12	Manage the Physical Environment
DS13	Manage Operations

Monitor and Evaluate

The Monitor and Evaluate domain deals with a company's strategy in assessing the needs of the company and whether or not the current system still meets the objectives for which it was designed and the controls necessary to comply with regulatory requirements. Monitoring also covers the issue of an independent assessment of the effectiveness of IT system in its ability to meet business objectives and the company's control processes by internal and external auditors. The following table lists the IT processes contained in the Monitor and Evaluate domain.

IT PROCESSES Monitor and Evaluate

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

(b) *COBIT and other standards*

- COBIT, Val IT and Risk IT:** Building on the success of COBIT, and focusing on key IT governance areas of value delivery and risk management, ISACA developed two additional IT governance frameworks, Val IT™ and Risk IT. These frameworks are closely aligned with and complement COBIT, but deliver value to enterprises in their own right. While COBIT ensures that IT is working as effectively as possible to maximize the benefits of technology investment, Val IT helps enterprises make better decisions about where to invest, ensuring that the investment is consistent with the business strategy. And while COBIT provides a set of controls to mitigate IT risk in IT processes, Risk IT provides a framework for enterprise to identify, govern and manage IT-related risks.
- COBIT and ISO/IEC 27002:2007:** COBIT was released and used primarily by the IT community, and has become the internationally accepted framework for IT governance and control. ISO/IEC 27002:2007 (The Code of Practice for Information Security Management) is also an international standard and is best practice for implementing security management. The two standards do not compete with each other and actually complement one another. COBIT typically covers a broader area while ISO/IEC 27002 is deeply focused in the area of security.

Information Systems Auditing Standards, Guidelines, Best Practices

The table below describes the inter-relation of the two standards as well as how ISO/IEC 27002 can be integrated with COBIT.

COBIT DOMAIN	1	2	3	4	5	6	7	8	9	10	11	12	13
Plan and Organize	-	+	-	-	+	+	+	+	-	-	0	.	.
Acquire and Implement	+	0	0	-	0	+	.	.	.	.	.	.	.
Deliver and Support	-	+	0	+	+	.	+	0	0	0	+	0	0
Monitor and Evaluate	-	0	-	0	.	.	.	.	.	.	.	.	.

(+) Good match (more than two ISO/IEC 27002:2007 objectives were mapped to a COBIT process)

(0) Partly match (one or two ISO/IEC 27002:2007 objectives were mapped to a COBIT process)

(-) No or minor match (no ISO/IEC 27002:2007 objective was mapped to a COBIT process)

(.) Does not exist

- COBIT and Sarbanes Oxley:** Public companies that are subject to the U.S. Sarbanes-Oxley Act of 2002 are encouraged to adopt COBIT and/or the Committee of Sponsoring Organizations of the Treadway Commission (COSO) "Internal Control - Integrated Framework." In choosing which of the control frameworks to implement in order to comply with Sarbanes-Oxley, the U.S. Securities and Exchange Commission suggests that companies follow the COSO framework.

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. COBIT approaches IT control by looking at information — not just financial information — that is needed to support business requirements and the associated IT resources and processes. COSO control objectives focus on effectiveness, efficiency of operations, reliable financial reporting, and compliance with laws and regulations. The two frameworks have different audiences. COSO is useful for management at large, while COBIT is useful for IT management, users, and auditors. COBIT is specifically focused on IT controls. Because of these differences, auditors should not expect a one-to-one relationship between the five COSO control components and the four COBIT objective domains.

EXERCISE

Question 1

As an auditor, what will be your suggestion about the control and objectives for Access Control?

Question 2

Explain the following terms in brief:

- (a) Software process capability,
- (b) Software process performance, and
- (c) Software process maturity.

Question 3

ABC Company is implementing The Health Insurance Portability and Accountability Act (HIPPA). There is a security rule issued under the Act which lays out three types of security safeguards required for compliance. What are those conditions under these safeguards for which the company should look after?

Question 4

Explain the control and objectives of Organizational Security in brief.

Question 5

Explain the various domains of COBIT, identified for high level control objectives to manage IT resources.

Question 6

Briefly explain the control and objectives of System Development and Maintenance.

DRAFTING OF IS SECURITY POLICY, AUDIT POLICY, IS AUDITING REPORTING- A PRACTICAL PERSPECTIVE

BASIC CONCEPTS

1. Information System Security:

Security relates to the protection of valuable assets against loss, disclosure, or damage. Securing valuable assets from threats, sabotage, or natural disaster with physical safeguards such as locks, perimeter fences, and insurance is commonly understood and implemented by most organizations.

1.1 Security Objective: For any organization, the security objective comprises three universally accepted attributes:

Confidentiality: Prevention of the unauthorized disclosure of information.

Integrity: Prevention of the unauthorized modification of information.

Availability: Prevention of the unauthorized withholding of information.

1.2 Sensitive Information: The sensitive information is: Strategic Plans, Business Operations, and Finances.

1.3 Establishing better Information Protection: The major points to be considered are: Not all data has the same value, Know where the critical data resides, Develop an access control methodology, Protect Information stored on media, Review hardcopy output.

2. Preventive Information Protection: This type of protection is based on use of security controls. Information system security controls are generally grouped into three types of control: Physical, Logical, and Administrative. Organizations require all three types of controls.

3. Information Security Policy: A Policy is a plan or course of action, designed to influence and determine decisions, actions and other matters. The security policy is a set of laws, rules, and practices that regulates how assets, including sensitive information are managed, protected, and distributed within the user organization. An information Security policy addresses many issues such as disclosure, integrity and

Information Systems Control and Audit

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.

3.1 Members of Security Policy: Security has to encompass managerial, technological and legal aspects. Security policy broadly comprises the following three groups of management: Management members who have budget and policy authority, Technical group who know what can and cannot be supported, and Legal experts who know the legal ramifications of various policy charges.

4. Types of Information Security Policy: Various policies are: Information Security Policy, User Security Policy, Acceptable Usage Policy, Organizational Information Security Policy, Network and System Security Policy, Information Classification Policy, Conditions of Connection.

4.1 Components of Security Policy: A good security policy should clearly state the following: Purpose and Scope of the Document and the intended audience, The Security Infrastructure, Security policy document maintenance and compliance requirements, Incident response mechanism and incident reporting, Security organization Structure, Inventory and Classification of assets, Description of technologies and computing structure, Physical and Environmental Security, Identity Management and access control, IT Operations management, IT Communications, System Development and Maintenance Controls, Business Continuity Planning, Legal Compliances, Monitoring and Auditing Requirements, and Underlying Technical Policy.

5. Audit Policy: Purpose of this audit policy is to provide the guidelines to the audit team to conduct an audit on IT based infrastructure system. The Audit is done to protect entire system from the most common security threats which includes the following: Access to confidential data, Unauthorized access of the department computers, Password disclosure compromise, Virus infections, Denial of service attacks, Open ports, which may be accessed from outsiders, and Unrestricted modems unnecessarily open ports. Audits may be conducted to ensure integrity, confidentiality and availability of information and resources.

5.1 Scope of IS Audit: The scope of information system auditing should encompass the examination and evaluation of the adequacy and effectiveness of the system of internal control and the quality of performance by the information system. 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, and People.

Drafting of IS Security Policy, Audit Policy, IS Auditing Reporting-A Practical Perspective

- 6. IS Audit Reports:** Audit reports broadly include the following sections: title page, table of contents, summary (including the recommendations), introduction, findings and appendices. The 'Introduction' section includes: Context, Purpose, Scope, Methodology, Findings, Opinion, and Appendices.

Question 1

Discuss various types of Information Security policies and their hierarchy.

Answer

Various types of information security policies are:

1. *Information Security Policy* – This policy provides a definition of Information Security, its overall objective and the importance that applies to all users.
2. *User Security Policy* – This policy sets out the responsibilities and requirements for all IT system users. It provides security terms of reference for Users, Line Managers and System Owners.
3. *Acceptable Usage Policy* – This sets out the policy for acceptable use of email and Internet services.
4. *Organizational Information Security Policy* – This policy sets out the Group policy for the security of its information assets and the Information Technology (IT) systems processing this information. Though it is positioned at the bottom of the hierarchy, it is the main IT security policy document.
5. *Network & System Security Policy* – This policy sets out detailed policy for system and network security and applies to IT department users
6. *Information Classification Policy* - This policy sets out the policy for the classification of information
7. *Conditions of Connection* – This policy sets out the Group policy for connecting to their network. It applies to all organizations connecting to the Group, and relates to the conditions that apply to different suppliers' systems.

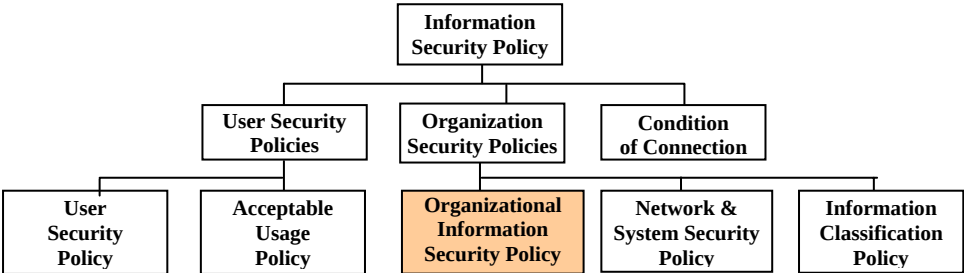


Fig: The hierarchy of Information Security Policies

Information Systems Control and Audit

Question 2

State and briefly explain the contents of a Standard Information System Audit Report.

Answer

According to the recommendations, IS Audit reports broadly include the following sections: title page, table of contents, summary including the recommendations, introduction, findings and appendices. These components of an audit report are discussed below:

- (i) *Cover and Title Page*: Audit reports should use a standard cover, with a window showing the title: "Information System Audit" or "Data Audit", the department's name and the report's date of issue (month and year). These items are repeated at the bottom of each page. The title page may also indicate the names of the audit team members.
- (ii) *Table of Contents*: The table lists the sections and sub-sections with page numbers including summary and recommendations, introduction, findings (by audit field) and appendices (as required).
- (iii) *Summary / Executive Summary* : The summary gives a quick overview of the salient features at the time of the audit in light of the main issues covered by the report. It should not normally exceed three pages, including the recommendations.
- (iv) *Introduction*: Since readers will read the summary, the introduction should not repeat details. It should include the following elements:
 - *Context*: This sub-section briefly describes conditions in the audit entity during the period under review, for instance, the entity's role, size and organization especially with regard to information system management, significant pressures on information system management during the period under review, events that need to be noted, organizational changes, IT disruptions, changes in roles and programs, results of internal audits or follow-up to our previous audits, if applicable.
 - *Purpose*: This sub-section is a short description of what functions and special programs were audited and the clients' authorities.
 - *Scope*: The scope lists the period under review, the issues covered in each function and program, the locations visited and the on-site dates.
 - *Methodology*: This section briefly describes sampling, data collection techniques and the basis for auditors' opinions. It also identifies any weaknesses in the methodology to allow the client and auditee to make informed decisions as a result of the report.

Drafting of IS Security Policy, Audit Policy, IS Auditing Reporting-A Practical Perspective

- (v) *Findings*: Findings constitute the main part of an audit report. They result from the examination of each audit issue in the context of established objectives.
- (vi) *Opinion*: If the audit assignment requires the auditor to express an audit opinion, the auditor shall do so in consonance to the requirement.
- (vii) *Appendices*: Appendices can be used when they are essential for understanding the report. They usually include comprehensive statistics, quotes from publications, documents, and references.

Question 3

The Information Security Policy of an organization has been defined and documented as given below:

“Our organization is committed to ensure Information Security through established goals and principles. Responsibilities for implementing every aspect of specific applicable proprietary and general principles, standards and compliance requirements have been defined. This is reviewed at least once a year for continued suitability with regard to cost and technological changes.”

Answer

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.

Issues to address: This policy does not need to be extremely extensive, but clearly state senior management's commitment to information security, be under change and version control and be signed by the appropriate senior manager. The policy should at least address the following issues:

- a definition of information security,
- reasons why information security is important to the organization, and its goals and principles,
- a brief explanation of the security policies, principles, standards and compliance requirements,
- definition of all relevant information security responsibilities, and

Information Systems Control and Audit

- reference to supporting documentation.

The auditor should ensure that the policy is readily accessible to all employees and that all employees are aware of its existence and understand its contents. The policy may be a stand-alone statement or part of more extensive documentation (e.g. a security policy manual) that defines how the information security policy is implemented in the organization. In general, most if not all employees covered by the ISMS scope will have some responsibilities for information security, and auditors should review any declarations to the contrary with care. The auditor should also ensure that the policy has an owner who is responsible for its maintenance and that it is updated responding to any changes affecting the basis of the original risk assessment.

In the stated scenario of the question, the ISMS Policy of the given organization does not address the following issues:

- (i) Definition of information security,
- (ii) Reasons why information security is important to the organization,
- (iii) A brief explanation of the security policies, principles, standards and compliance, and
- (iv) Reference to supporting documents.

Question 4

What purpose the information system audit policy will serve? Briefly describe the scope of information system audit.

Answer

Purpose of the Audit Policy

Purpose of the audit policy is to provide the guidelines to the audit team to conduct an audit of 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 by outsiders
- Unrestricted modems, unnecessarily open ports

Drafting of IS Security Policy, Audit Policy, IS Auditing Reporting-A Practical Perspective

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
- Maintenances 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.

Scope of IS Audit

The scope of information system auditing should encompass the examination and evaluation of the adequacy and effectiveness of the system of internal control and the quality of performance by the information system. Information System Audit will examine and evaluate the planning, organizing, and directing processes to determine whether reasonable assurance exists that objectives and goals will be achieved. Such evaluation, in the aggregate, provides information to appraise the overall system of internal control.

The scope of the audit will also include the internal control system (s) for the use and protection of information and the information system, as under:

- Data
- Application systems
- Technology
- Facilities
- People

The information System auditor will consider whether the information obtained from the above reviews indicates coverage of the appropriate areas. The information system auditor will examine, among other, 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 Systems Control and Audit

- Information system budget 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.

Question 5

You have been asked to conduct an I.S. Audit for a bank. (i) How will you develop a documented audit program? (ii) What kind of working papers and documentation you will prepare?

Answer

- (i) The **documented audit program** is developed with the help of following activities:
- Documentation of the IS auditor's procedures for collecting, analysing, interpreting, and documenting information during the audit.
 - Objectives of the audit.
 - Scope, nature, and degree of testing required to achieve the audit objectives in each phase of the audit.
 - Identification of technical aspects, risks, processes, and transactions which should be examined.
 - Procedures for audit will be prepared prior to the commencement of audit work and modified, as appropriate, during the course of the audit.
- (ii) **Audit Working Papers and Documentation**
- Working papers should record the audit plan, the nature, timing and extent of auditing procedures performed, and the conclusions drawn from the evidence

Drafting of IS Security Policy, Audit Policy, IS Auditing Reporting-A Practical Perspective

obtained. All significant matters which require the exercise of judgment, together with the auditor's conclusion thereon, should be included in the working papers. The form and content of the working papers are affected by matters such as:

- The nature of the engagement
- The form of the auditor's report
- The nature and complexity of client's business
- The nature and condition of client's records and degree of reliance on internal controls.

In case of recurring audits, some working paper files may be classified as permanent audit files which are updated currently with information of continuing importance to succeeding audits, as distinct from the current audit files which contain information relating primarily to audit of a single period.

The permanent audit file normally includes:

- The organization structure of the entity.
- The IS policies of the organization.
- The historical background of the information system in the organization.
- Extracts of copies of important legal documents relevant to audit.
- A record of the study and evaluation of the internal controls related to the information system.
- Copies of audit reports and observations of earlier years.
- Copies of management letters issued by the auditor, if any.

The current file normally includes:

- Correspondence relating to the acceptance of appointment and the scope of the work.
- Evidence of the planning process of the audit and audit programme.
- A record of the nature, timing, and extent of auditing procedures performed, and the results of such procedures.
- Copies of letters and notes concerning audit matters communicated to or discussed with the client, including material weaknesses in relevant internal controls.
- Letters of representation and confirmation received from the client.

Information Systems Control and Audit

- Conclusions reached by the auditor concerning significant aspects of the audit, including the manner in which the exceptions and unusual matters, if any, disclosed by the auditor's procedures were resolved and treated.
- Copies on the data and system being reported on and the related audit reports.

Working papers are the property of the auditor. The auditor may, at his discretion, make portions of, or extracts from his working papers available to the client. The auditor should adopt reasonable procedures for custody and confidentiality of his working papers and should retain them for a period of time sufficient to meet the needs of his practice and satisfy any pertinent legal and professional requirements of record retention.

Question 6

Explain the basic types of Information Protection that an Organization can use.

Answer

Types of Information Protection: The two basic types of information protection that an organization can use are given as follows:

1. Preventative Information Protection, and
2. Restorative Information Protection.

Preventative Information Protection: It is based on use of security controls, which itself is a group of three types of controls such as Physical, Logical, and Administrative.

- *Physical controls* deal with Doors, Locks, Guards, Floppy Disk Access Locks, Cables locking systems to desks/walls, CCTV, Paper Shredders, Fire Suppression Systems,
- *Logical controls* deal with Passwords, File Permissions, Access Control Lists, Account Privileges, Power Protection Systems, and
- *Administrative controls* deal with Security Awareness, User Account Revocation, and Policy.

Restorative Information Protection: If an organization cannot recover or recreate critical information systems in an acceptable time period, the organization will suffer and possibly have to go out of business. Hence, the key requirement of any restorative information system protection plan is that the information systems can be recovered. The claim of back program to backup data automatically cannot be

Drafting of IS Security Policy, Audit Policy, IS Auditing Reporting-A Practical Perspective

reliable. It has so many problems. The restorative information protection program must address the following:

- Whether the recovery process has been evaluated and tested recently?
- The time taken for restoration,
- The quantum of productivity loss,
- The strict adherence of plan, and
- The time needed to input the data changes since the last backup.

Question 7

Describe the role of information systems audit policy in ensuring information security with respect to:

- Scope of IS Audit
- Purpose of IS Audit

Answer

- (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.

Information Systems Control and Audit

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.

Drafting of IS Security Policy, Audit Policy, IS Auditing Reporting-A Practical Perspective

- 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.

Question 8

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*

Answer

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.

Information Systems Control and Audit

- 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.

Drafting of IS Security Policy, Audit Policy, IS Auditing Reporting-A Practical Perspective

(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.

Information Systems Control and Audit

- 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

Question 9

What are the various types of Information Security Policies? What are the hierarchical relationships between these policies? Discuss briefly.

Answer

Types of Information Security Policies and their Hierarchy:

- ◆ *Information Security Policy:* This policy provides a definition of Information Security, its overall objective and the importance applies to all users.
- ◆ *User Security Policy:* This policy sets out the responsibilities and requirements for all IT system users. It provides security terms of reference for users, line managers and system owners.
- ◆ *Acceptance Usage Policy:* This sets out the policy for acceptance use of e-mail and internet services.
- ◆ *Organizational Information Security Policy:* This policy sets out the Group Policy for the security of its information assets and the Information Technology (IT) Systems processing this information.
- ◆ *Network and System Security Policy:* This policy sets out detailed policy for system and network security and applies to IT department users.
- ◆ *Information classification policy:* This policy sets out the policy for the classification of information.
- ◆ *Conditions of connection:* This policy sets out the group policy for connecting to their network. It applies to all organizations connecting to the group, and relates to the conditions that apply to different supplies systems.

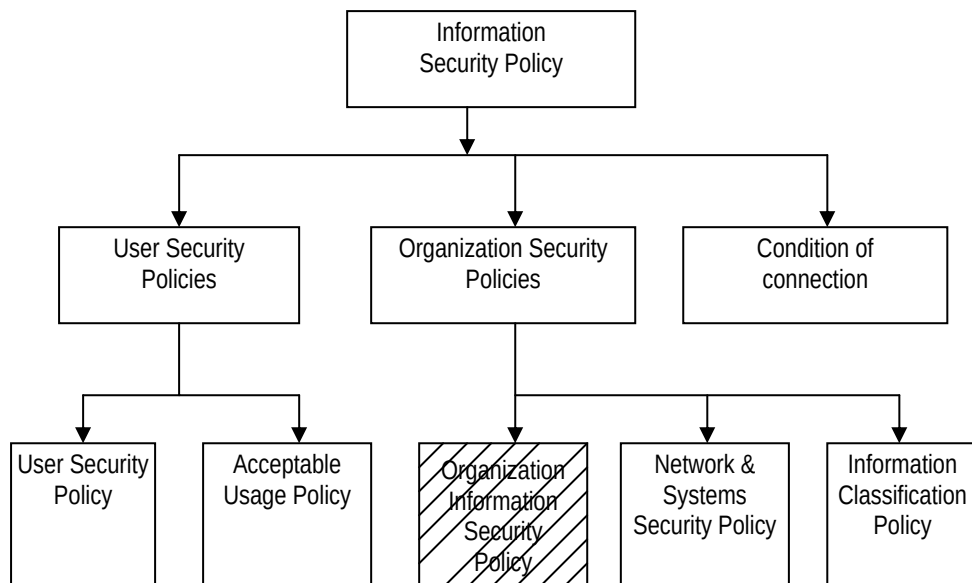


Fig. : The hierarchy of Information Security Policies

Question 10

What are the components of the Security Policy?

Answer

Components of the Security Policy: A good security policy should clearly state the following:

- ◆ Purpose and scope of the document and the intended audience.
- ◆ The security infrastructure.
- ◆ Security policy document maintenance and compliance requirements.
- ◆ Incident response mechanism and incident reporting.
- ◆ Security organization structure.
- ◆ Inventory and classification of assets.
- ◆ Description of technologies and computing structure.
- ◆ Physical and environmental security.
- ◆ Identify management and access control.
- ◆ IT operations management.
- ◆ IT communications.

Information Systems Control and Audit

- ◆ System development and maintenance controls.
- ◆ Business continuity planning.
- ◆ Legal compliances.
- ◆ Monitoring and Auditing Requirements.
- ◆ Underlying technical policy.

Question 11

What is meant by physical and environmental security?

Answer

Physical and Environmental Security:

- ◆ Physical security should be maintained and checks must be performed to identify all vulnerable areas within each site.
- ◆ The IT infrastructure must be physically protected.
- ◆ Access to secure areas must remain limited to authorized staff only.
- ◆ Confidential and sensitive information and valuable asserts must always be securely locked away when not in use.
- ◆ Computers must never be left unattended whilst displaying confidential or sensitive information or whilst logged on to systems.
- ◆ Supplies and equipment must be delivered and loaded in an isolated area to prevent any unauthorized access to key facilities.
- ◆ Wherever practical, premises housing computer equipment and data should be located away from and protected against threats of deliberate or accidental damage such as fire and natural disaster.

The location of the equipment room (s) must not be obvious. It should practically be located away and protected against threats of unauthorized access and deliberate or accidental damage, such as system infiltration and environmental failures.

Question 12

What is meant by SYSTRUST and WEBTRUST? Discuss in brief.

Answer

SYSTRUST and WEBTRUST: Systrust and Webtrust are two specific services developed by the AICPA that are based on the trust services principles and criteria. Systrust engagements are designed for the provision or advisory services or assurance on the

Drafting of IS Security Policy, Audit Policy, IS Auditing Reporting-A Practical Perspective

reliability of a system. Webtrust engagements relate to assurance or advisory services on an organization. System related to e-commerce. Only Certified Public Accountants (CPAs) may provide the assurance services of trust services that result in the expression of a trust services, webtrust, or systrust opinion and in order to issue systrust or webtrust reports, CPA firms must be licensed by the AICPA.

The following principles and related criteria have been developed by the AICPA/CICA for use by practitioners in the performance of Trust services engagements such as systrust and webtrust.

- ◆ *Security*: The system is protected against unauthorized access (both physical and logical).
- ◆ *Availability*: The system is available for operation and use as committed or agreed.
- ◆ *Processing integrity*: System processing is complete, accurate, timely and authorized.
- ◆ *On-line privacy*: Personal Information obtained as a result of e-commerce is collected, used, disclosed and retained as committed or agreed.
- ◆ *Confidentiality*: Information designated as confidential is protected as committed or agreed.

Each of these principles and criteria are organized and presented in four broad areas:

- ◆ *Policies*: The entity has defined and documented its policies relevant to the particular principle.
- ◆ *Communications*: The entity has communicated its defined policies to authorized users.
- ◆ *Procedures*: The entity uses procedures to achieve its objectives in accordance with its defined policies.
- ◆ *Monitoring*: The entity monitors the system and takes action to maintain compliance with its defined policies.

Question 13

ABC Technologies is a leading company in the BPO sector. Its most of the business processes are automated. The company is relying on Information Technology for information and transaction processing. The growth of E-commerce supported by the growth of the Internet has completely revolutionized and reengineered business processes. The company's new business models and new methods presume that the information required by the business managers is available all the time; it is accurate, it is reliable and no unauthorized disclosure of the same is made. Further, it is also presumed that the virtual business organization is up

Information Systems Control and Audit

and running all the time on 24×7 basis. However, in reality, the technology-enabled and technology-dependent organizations are more vulnerable to security threats than ever before.

Read the above carefully and answer the following:

- (a) Discuss the security objective of the organization.*
- (b) There are certain basic ground rules that must be addressed sequentially, prior to know the details of 'how to protect the information systems'. Explain those rules in brief.*
- (c) Describe various groups of management, comprised by security policy.*

Answer

- (a) Security Objective :** The objective of information system security is “the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of confidentiality, integrity, and availability”.

For any organization, the security objective comprises three universally accepted attributes:

- Confidentiality: Prevention of the unauthorized disclosure of information.
- Integrity: Prevention of the unauthorized modification of information.
- Availability: Prevention of the unauthorized withholding of information.

The relative priority and significance of confidentiality, integrity and availability vary according to the data within the information system and the business context in which it is used.

- (b)** Prior to know the details of 'how to protect the information systems', we need to define a few basic ground rules that must be addressed sequentially. These rules are:
- Rule #1: We need to know that 'what the information systems are' and 'where these are located'.
 - Rule #2: We need know the value of the information held and how difficult it would be to recreate if it were damaged or lost.
 - Rule #3: We need to know that 'who is authorized to access the information' and 'what they are permitted to do with the information'.
 - Rule #4: We need to know that 'how quickly information needs to be made available should and it become unavailable for whatever reason (loss, unauthorized modification, etc.) '
- (c)** Security has to encompass managerial, technological and legal aspects. Security policy broadly comprises the following three groups of management:

Drafting of IS Security Policy, Audit Policy, IS Auditing Reporting-A Practical Perspective

- Management members who have budget and policy authority,
- Technical group who know what can and cannot be supported, and
- Legal experts who know the legal ramifications of various policy charges.

Information security policies must always take into account business requirements. Business requirements are the principles and objectives adopted by an organization to support its operations and information processing. E-commerce security is an example of such business requirements.

Furthermore, policies must consistently take into account the legal, statutory, regulatory and contractual requirements that the organization and its professional partners, suppliers and service providers must respect. The respect of intellectual property is a good example of such requirements.

EXERCISE

Question 1

An organization is committed to implement the information security policy through established goals and principles. The major problem, organization is facing through its employees. There is neither any proper allocation of duties/ responsibilities between employees nor a proper reporting hierarchy. Suggest a proper security organization structure and responsibility allocation, to come out of these problems.

Question 2

An Information Systems Audit Report contains various components: Cover and title page, Table of contents, Summary/Executive summary, and Appendices. But after submission, the principal auditor raised the query that the report is not correct as it missed various important components. Explain the missing components in brief.

Question 3

An Information System Audit Report includes various sections: Title Page, Table of Contents, Summary, Introduction, Findings and Appendices. Explain various elements, included in the 'Introduction' section.

Question 4

It is clear from various instances that there are not only many direct and indirect benefits from the use of information systems, but also many direct and indirect risks related to the use of information systems. These risks have led to a gap between the need to protect systems and the degree of protection applied. Briefly explain the causes of this gap.

Question 5

Briefly discuss end user computing policies with respect to a sample IS Security Policy.

Question 6

Differentiate between the responsibilities of a Facilities Management Security Officer and Divisional System Security Officer with respect to the organizational security structure.

INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

BASIC CONCEPTS

1. **The Act:** In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000. This Act aims to provide the legal infrastructure for e-commerce in India and would have a major impact for e-businesses and the new economy in India. Therefore, it is important to understand 'what are the various perspectives of the IT Act, 2000 and what it offers?'. The Information Technology Act, 2000 also aims to provide the legal framework under which legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability.

This Act was amended by Information Technology Amendment Bill 2006, passed in Lok Sabha on Dec 22nd and in Rajyasbha on Dec 23rd of 2008. Information Technology (Amendment) Bill 2006 was amended by Information Technology Act Amendment Bill 2008 and in the process, the underlying Act was renamed as Information Technology (Amendment) Act 2008 i.e. referred to as ITAA 2008.

2. **Arrangement of Sections:** The Act consists of 90 sections spread over 13 chapters.

Question 1

Explain briefly the scope of the Information Technology (Amendment) Act 2008 along with the relevant definitions that are used.

Answer

Scope of the Information Technology (Amendment) Act 2008: This Act is meant for whole of India unless otherwise mentioned. It applies also to any offence or contravention there under committed outside India by any person. The Act was enforced by the Central Government from October 17, 2000.

Information Systems Control and Audit

The Act shall not apply to the following:

- A negotiable instrument as defined in Section 13 of the Negotiable Instruments Act, 1881;
- A power - of - attorney as defined in Section 1A of the Powers –of-Attorney Act, 1882.
- A trust as defined in Section 3 of the Indian Trusts Act, 1882.
- A will as defined in Section (h) of Section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called.
- Any contract for the sale or conveyance of immovable property or any interest in such property.
- Any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

The Act consists of 94 Sections spread over thirteen Chapters and four Schedules to the Act. The Schedules to the Act contain related amendments made in other Acts as outlined in the Objectives of the Act, namely, the Indian Penal code, the Indian Evidence Act, 1972, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India, 1934.

Section 2 contains some of the important terms that are defined below.

- (a) "Access" means gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network.
- (b) "Addressee" – a person who is intended by the originator to receive the electronic record but does not include any intermediary.
- (c) "Affixing digital signature" – adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature.
- (d) "Appropriate Government" – Central Government except in the following two cases where it means the State Government.
 - in the matters enumerated in List II of the Seventh Schedule to the Constitution.
 - relating to any state law enacted under List III of the Seventh Schedule to the Constitution.
- (e) "Asymmetric crypto system" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

- (f) “*Computer*” – any electronic, magnetic or optical or other high speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network.
- (g) “*Computer network*” – The interconnection of one or more, computers through
 - (i) the use of satellite, microwave, terrestrial line or other communication media and
 - (ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.
- (h) “*Computer resource*” – computer, computer system, computer network, data, computer data base or software.
- (i) “*Computer system*” – a device or collection of devices including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions.
- (j) “*Data*” – a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.
- (k) “*Digital signature*” – authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3.
- (l) “*Electronic form*” with reference to information means any information generated , sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.
- (m) “*Electronic record*” – data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.
- (n) “*Function*” – in relation to a computer, includes logic, control arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer.
- (o) “*Information*” includes data, text, images, sound, voice, codes, computer programs, software and databases or micro film or computer generated micro fiche.

Information Systems Control and Audit

- (p) “*Intermediary*” with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.
- (q) “*Key pair*”, in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.
- (r) “*Originator*” – a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary.
- (s) “*Prescribed*” – prescribed by rules made under this Act.
- (t) “*Private key*” – the key of a key pair used to create a digital signature.
- (u) “*Public key*” – the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate.
- (v) “*Secure system*” means computer hardware, software and procedure that
- are reasonably secure from unauthorized access and misuse.
 - provide a reasonable level of reliability and correct operation.
 - are reasonably suited to performing the intended function and
 - adhere to generally accepted security procedures.
- (w) “*Verify*” – in relation to a digital signature electronic record on public key with its grammatical variations and cognate expressions means to determine whether
- the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber.
 - the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

Question 2

Define the following terms with reference to section 2 of Information Technology (Amendment) Act 2008:

- (i) *Digital signature*
- (ii) *Electronic form*
- (iii) *Key pair*
- (iv) *Asymmetric crypto system*
- (v) *Adjudicating officer.*
-

Answer

- (i) **Digital Signature:** It is a authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3:
- (ii) **Electronic form:** It is reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated micro fiche or similar device.
- (iii) **Key Pair:** It is an asymmetric cryptosystem, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.
- (iv) **Asymmetric crypto system:** It is a system of secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.
- (v) **Adjudicating Officer:** It means an adjudicating Officer appointed under sub-section (1) of section 46.

Question 3

What are the conditions subject to which electronic record may be authenticated by means of affixing digital signature?

Answer

Chapter-II of Information Technology (Amendment) Act 2008 gives legal recognition to electronic records and digital signatures. It contains only **section 3**.

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

Information Systems Control and Audit

For the purposes of this sub-section, “hash function” means an algorithm mapping or translation of one sequence of bits into another, generally smaller set known as “hash result” such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible- to derive or reconstruct the original electronic record from the hash result produced by the algorithm; that two electronic records can produce the same hash result using the algorithm.

Question 4

How does the Information Technology (Amendment) Act 2008 enable the authentication of records using digital signatures?

Answer

Chapter-II, Section 3 of Information Technology (Amendment) Act 2008 provides conditions subject to which an electronic record is authenticated by means of affixing digital signature.

- The digital signature is created in two distinct steps. First the electronic record is converted into a message digest by using a mathematical function known as “hash function” which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record.

Any tampering with the contents of the electronic record will immediately invalidate the digital signature.

- Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the corresponding public key.

This will enable anybody to verify whether the electronic record is retained intact or has been tampered with; since it was fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message.

Question 5

How does the Information Technology (Amendment) Act 2008 enable the objective of the Government in spreading e-governance?

Answer

In Information Technology (Amendment) Act 2008, chapter III is related with the objective of the government in spreading e-governance. It deals with the procedures to be followed for sending and receiving of electronic records. This chapter contains sections 4 to 10.

Section 4 - This section provides the legal recognition of electronic records.

Section 5 - This section provides the legal recognition of Digital Signatures.

Section 6 – It 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 license or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form.

Section 7 – This section provides that the documents, records or information which is to be retained for any specified period shall be deemed to have been retained in the electronic form with the following conditions:

- (i) the information therein remains accessible so as to be usable subsequently,
- (ii) it is retained in its original format ,
- (iii) the details such as origin, destination, dates and time of dispatch or receipt of such electronic record.

Section 8- It provides for the publication of rules, regulations and notifications in the Electronic Gazette.

Question 6

Discuss the main provisions provided in Information Technology (Amendment) Act 2008 to facilitate E-governance.

Answer

E-Governance sections of chapter III 6, 7 and 8 are the main sections for provisions related to E-governance provided in Information Technology (Amendment) Act 2008 to facilitate e-governance.

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

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

- (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.

Information Systems Control and Audit

- (iii) The details which will facilitate the identification of the origin, destinations, dates and time of dispatch or receipt of such electronic record to be dispatched or received.

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, order, bye-law and notifications in the official Gazette in an electronic form. 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, 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.

Question 7

What are the regulations relating to the appointment and powers of the certifying authorities under Chapter VI, Section 17 to 25 of Information Technology (Amendment) Act 2008?

Answer

Regulation of Certifying Authorities [Chapter VI – Section 17–25]:

Chapter VI contains detailed provisions relating to the appointment and powers of the Controller and Certifying Authorities.

Section 17 provides for the appointment of Controller and other officers to regulates the Certifying Authorities.

Section 18 lays down the functions which the controller may perform in respect of activities of Certifying Authorities.

Section 19 provides for the power of the Controller with the previous approval of the Central Government to grant recognition to foreign certifying Authorities subject to such conditions and restrictions as may be imposed by regulations.

Section 20 This Section provides that the controller shall be acting as repository of all Digital Signature Certificates issued under the Act. He shall also adhere to certain security procedure to ensure secrecy and privacy of the digital signatures and also to satisfy such other standards as may be prescribed by the Central Government. He shall maintain a computerized database of all public keys in such a manner that they are available to the general public.

Section 21 This section provides that a license to be issued to a certifying authority to issue digital signature certificates by the controller shall be in such form and shall be accompanied with such fees and other documents as may be prescribed by the Central Government. Further, the Controller after considering the application may either grant the licence or reject the application after giving reasonable opportunity of being heard.

Section 22 This Section provides that the application for license shall be accompanied by a certification practice statement and statement including the procedures with respect to identification of the applicant. It shall be future accompanied by a fee not exceeding Rs. 25,000 and other documents as may be prescribed by the Central Government.

Section 23 provides that the application for renewal of a license shall be in such form and accompanied by such fees not exceeding Rs. 5,000 which may be prescribed by the Central Government.

Section 24 deals with the procedure for grant or rejection of license by the Controller on certain grounds.

No application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

Section 25 provides that the controller may revoke a licence on grounds such as incorrect or false material particulars being mentioned in the application and also on the ground of contravention of any provisions of the Act, rule, regulation or order made there under.

Question 8

What are the duties of a certifying authority under Section 30 of the Information Technology (Amendment) Act 2008?

Answer

Duties of Certifying Authorities {Section 30}:

This section provides that every Certifying Authority shall follow certain procedures in respect of Digital Signatures as given below:

- (a) make use of hardware, software and procedures that are secure from intrusion and misuse;
- (b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions.
- (c) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured and
- (d) Observe such other standards as may be specified by regulations.

Information Systems Control and Audit

Question 9

What is a Digital Signature? How is it used? What are the duties of certifying authorities in regard to its usage?

Answer

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

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

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

Duties of Certifying Authority:

1. According to Section 30 of the Information Technology (Amendment) Act 2008, Certifying Authority shall follow certain procedures in respect of Digital Signatures as given below:
 - Make use of hardware, software and procedures that are secure from intrusion and misuse.
 - Provide a reasonable level of reliability in its services, which are reasonably suited to the performance of intended functions.
 - Adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured and
 - Observe such other standards, as specified by the regulation.
2. Every Certifying Authority shall ensure that every person employed by him complies with the provisions of the Act, or rules, regulations or orders made there under.

3. A Certifying Authority must display its licence at a conspicuous place of the premises in which it carries on its business. A Certifying Authority whose licence is suspended or revoked shall immediately surrender the license to the Controller.
4. Every Certifying Authority shall display its Digital Signature Certificate, which contains the public key corresponding to the private key used by that Certifying Authority and other relevant facts.

Question 10

Write short notes on the following:

- (a) *Digital Signature Certificate*
- (b) *Encryption.*

Answer

- (a) **Digital Signature Certificate:** A digital signature certificate is a mechanism for authenticating and securing the information that is transmitted between the two parties. It is an authoritative identification about a person or a company. It is simply a public key, along with some identifying information, that has been digitally signed by a certificate authority. It identifies the subscriber, certification authority, and its operational period and contains the subscriber public key. The certificate is thus protected so that it cannot be altered without detection. It is like an electronic passport that authenticates identity of an entity. The identifying information in the certificate can be trusted because the digital signature is cryptically strong.

Legal recognition of digital signature, electronic records and authentication is necessary in an electronically formed contract. The Information Technology Act provides legal status on the use of the electronic records and signatures. Authentication and non-repudiation are secured through the mechanism of digital signature. The digital signature certificate ensures that the purported sender is in fact the person who sent the message. By certifying that a particular public key does indeed belong to a specific person, it authenticates and makes digital signature conclusive. For verification of such signature, the verifier must have the signer's public key and have an assurance that it corresponds to his private key. Digital certificate associates a particular person to that pair. Its basic purpose is to serve the need of the person seeking to verify a digital signature who would want to know that:

- The public key corresponds to the private key used to create the digital signature;
- Whether the public key is identified with the signer.

Section 35 of the Act deals with the issue of the digital certificate by the Certifying Authority, on an application being made in the prescribed form.

Information Systems Control and Audit

- (b) **Encryption:** Encryption refers to conversion of data into a secret code for storage in databases and transmission over networks. The sender uses an encryption algorithm to convert the original message called clear text into a coded equivalent called cipher text. At the receiving end, the cipher text is decoded (decrypted) back into clear text. The encryption algorithm uses a key, which is a binary number that is typically from 56 to 128 bits in length. The more bits in the key, the stronger the encryption method. Today, nothing less than 128 bit algorithms are considered truly secure. Two general approaches to encryption are private key and public key encryption.

Private Key Encryption: Data encryption standard (DES) is a private-key encryption technique designed in the early 1970s by IBM. The DES algorithm uses a single key known to both the sender and the receiver of the message. To encode a message, the sender provides the encryption algorithm with the key, which is used to produce a cipher text message. The message enters the communication channel and is transmitted to the receiver's location, where it is stored. The receiver decodes the message with a decryption program that uses the same key employed by the sender.

Public Key Encryption: The public key encryption technique uses two different keys: one for encoding messages and the other for decoding them. Each recipient has a private key that is kept secret and a public key that is published. The sender of a message uses the receiver's public key to encrypt the message. The receiver then uses his or her private key to decrypt the message. Users never need to share their private keys to decrypt messages, thus reducing the likelihood that it may fall into the hands of criminal.

Question 11

State the duties of the subscriber of a digital signature as specified in Section 40 to 42 of Chapter VIII of Information Technology (Amendment) Act 2008.

Answer

The duties of the subscriber of a Digital Signature as specified in Section 40 to 42 of Chapter VII of Information Technology (Amendment) Act 2008 are as follows:

On acceptance of the Digital Signature Certificate the subscriber shall generate a key pair using a secure system.

A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate-

- (i) to one or more persons;

- (ii) in a repository, or otherwise demonstrates his approval of the Digital Signature
- (iii) certificate in any manner.

By accepting a Digital Signature Certificate, the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that –

- (i) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;
- (ii) all representations made by the subscriber to the Certificate Authority and all material relevant to the information contained in the Digital Signature Certificate are true;
- (iii) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

The subscriber shall exercise all reasonable care to retain control of his private key corresponding to the public key. If such private key has been compromised (i.e., endangered or exposed), the subscriber must immediately communicate the fact to the Certifying Authority.

Otherwise, the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

Question 12

Explain with reference to “Information Technology (Amendment) Act 2008”:

- (i) *Penal Provisions*
- (ii) *Electronic Governance*

Answer

- (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;

Information Systems Control and Audit

- (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

Information Systems Control and Audit

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.

Question 13

Describe the composition and powers of Cyber regulatory appellate tribunal.

Answer

Cyber Regulatory Appellate Tribunal: The cyber regulation appellate tribunal shall consist of one person only called the Presiding Officer of the Tribunal who shall be appointed by the Central Government. The person must be qualified to be a Judge of a High Court or is or has been a member of Indian Legal Services in the post in Grade I of that service for at least three years. The Presiding Officer shall hold the office for a term of five years or upto a maximum age limit of 65 years, whichever is earlier.

Some of the powers specified are following:

- (i) Summoning and enforcing the attendance of any person and examining him on oath.
- (ii) Requiring production of documents and other electronic records.
- (iii) Receiving evidence on affidavits
- (iv) Reviewing its decisions.
- (v) Issuing commissions for examination of witness etc.

Question 14

Write short notes on the Powers of Cyber Appellate Tribunal.

Answer

Powers of Cyber Appellate Tribunal: Section 58 provides for the procedure and powers of the Cyber Appellate Tribunal. The Tribunal shall also have the powers of the Civil Court under the Code of Civil Procedure, 1908. Some of the powers specified are in respect of the following matters:

- (i) summoning and enforcing the attendance of any person and examining him on oath;
- (ii) requiring the discovery and production of documents or other electronic records;
- (iii) receiving evidence on affidavits;

Information Systems Control and Audit

- (iv) issuing commissions for the examination of witnesses or documents;
- (v) reviewing its decisions;
- (vi) dismissing an application for default or deciding it ex-parte;
- (vii) any other matter which may be prescribed.

The appellant may either appear in person or may be represented by a legal practitioner to present his case before the Tribunal.

Question 15

State the liabilities of companies under section 85 of Information Technology (Amendment) Act 2008.

Answer

Liability of Companies under Section 85 of Information Technology (Amendment) Act, 2008: Where a company commits any offence under this Act or any rule there under, every person who, at the time of the contravention, was in charge of and was responsible for the conduct of the business of the company shall be guilty of the contravention. However, he shall not be liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent the contravention.

Further, where a contravention has been committed by a company, and it is proved that the contravention took place with the connivance or consent of or due to any negligence on the part of any director, manager, secretary or other officer of the company, such officer shall be deemed to be guilty and shall be liable to be proceeded against and punished accordingly.

For the purposes of this section, 'company' includes a firm or other association of persons and 'director' in relation to a firm means a partner in the firm.

The Information Technology Act will go a long way in facilitating and regulating electronic commerce. It has provided a legal framework for smooth conduct of e-commerce. It has tackled the following legal issues associated with e-commerce:

- Requirement of writing
- Requirement of a document
- Requirement of a signature and
- Requirement of legal recognition for electronic messages,
- Records and documents to be admitted in evidence in a court of law.

Question 16

Please read carefully the following three scenarios and answer the questions given below:

(a) Scenario 1:

Nobody told you that your Internet use in the office was being monitored. Now you have been warned you will be fired if you use the Internet for recreational surfing again. What are your rights?

(b) Scenario 2:

Your employees are abusing their Internet privileges, but you don't have an Internet usage policy. What do you do?

(c) Scenario 3:

Employee Mr. X downloads adult material to his PC at work, and employee Miss Y sees it. Miss Y then proceeds to sue the company for sexual harassment. As the employer, are you liable?

Answer

- (a) **Scenario 1:** When you are using your office computer, you have virtually no rights. You would have a tough time convincing the court that the boss invaded your privacy by monitoring your use of the company PC during office hours. You should probably be grateful that you only got a warning stating that you will be fired if you use the Internet for recreational surfing again.
- (b) **Scenario 2:** Although the law is not fully developed in this area, courts are taking a straightforward approach. If it is a company computer, the company can control the way in which it is to be used by its employees. You really don't need an Internet usage policy to prevent inappropriate use of your company's computer. To protect the company in future, it is advisable to distribute an Internet usage policy to your employees as soon as possible to stop your employees from abusing their Internet privileges.
- (c) **Scenario 3:** Whether it comes from the Internet or from a magazine, adult material simply has no place in the office. So Miss Y could certainly sue the company for making her work in a sexually hostile environment. The best defense for the company is to have an Internet usage policy that prohibits employees to access adult sites. Of course, you have to follow-through and monitor. Today, software is available for monitoring the employees whenever they visit adult sites. It will shut down the computer and alert the person who is monitoring Internet usage. If someone is caught browsing adult material in the office, you must at least send a written communication to the offending employee. If the company lacks a strict Internet usage policy, Miss Y could prevail in the Court.

EXERCISE

Question 1

What are the major objectives of Information Technology (Amendment) Act 2008? Explain in brief.

Question 2

Briefly explain the power of central government to make rules with respect to the Section 10 of Information Technology (Amendment) Act 2008.

Question 3

Explain the power of Controller to make regulations under Section 89 of the Information Technology (Amendment) Act 2008.

Question 4

What are the powers of a Police Officer under the Information Technology (Amendment) Act 2008 to enter and search etc?

Question 5

Define 'Electronic Signature' and 'Electronic Signature Certificate' in the light of the Information Technology (Amendment) Act 2008.

Question 6

Briefly explain the Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form as per Section 67 A of the Information Technology (Amendment) Act 2008.