SUGGESTED ANSWERS

TO

QUESTIONS

SET AT THE

FINAL EXAMINATION

MAY, 1996 - NOVEMBER, 2008

A COMPILATION

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

BOARD OF STUDIES
THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA
NOIDA

CONTENTS

		Page Nos.
CHAPTER – 1	Basic Concepts of Systems	1 – 6
CHAPTER – 2	Transaction Processing system	7 – 8
CHAPTER – 3	Basic Concepts of MIS	9 – 26
CHAPTER – 4	Systems Approach and Decision Making	27 – 40
CHAPTER – 5	Decision Support and Executive Information Systems	41 – 50
CHAPTER– 6	Enabling Technologies	51 – 58
CHAPTER – 7	System Development Process	59 – 78
CHAPTER – 8	Systems Design	79 – 88
CHAPTER – 9	System's Acquisition, Software Development and Testing	89 – 106
CHAPTER – 10	Systems Implementation and Maintenance	107 – 114
CHAPTER – 11	Design of Computerised Commercial Applications	115 – 132
CHAPTER – 12	Enterprise Resource Planning: Redesigning Business	133 – 144
CHAPTER – 13	Controls In EDP Set-Up: General Controls	145 – 162
CHAPTER – 14	Controls in EDP Set-Up: Application Controls	163 –170
CHAPTER – 15	Detection of Computer Frauds	171 –184
CHAPTER – 16	Cyber Laws and Information Technology Act 2000	185 – 196
CHAPTER – 17	Audit of Information Systems	197 – 208
CHAPTER – 18	Information Security	209 – 220
CHAPTER – 19	Use of Simple CASE Tools, Analysis of Financial Statements Using Digital Technology	221 – 230

1

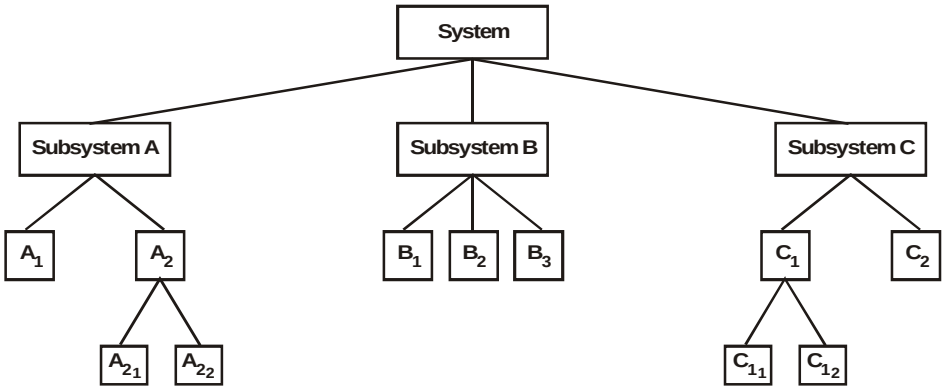
BASIC CONCEPTS OF SYSTEMS

Question 1

Explain the concept of decomposition with the help of an example. *(Final May 2003)*

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:



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

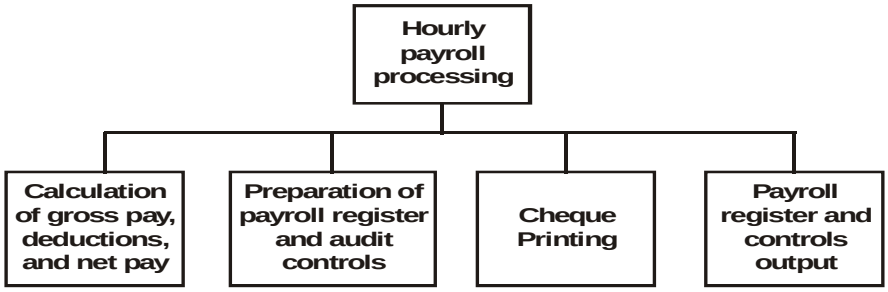
   Hourly payroll processing

   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:



Decomposition into sub systems is used to analyse 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 2

Define the term system stress and system change. *(Final Nov. 2005)*

Answer

Systems, whether they be living or artificial systems, organisational systems, information systems, or systems of controls, change because they undergo stress. A stress is a force transmitted by a system's supra-system that causes a system to change, so that the supra-system can better achieve its goals. In trying to accommodate the stress, the system may impose stress on its subsystems, and so on.

There are two basic forms of stress which can be imposed on a system, separately or concurrently:

1. A change in the goal set of the system. New goals may be created or old goals may be eliminated.
2. A change in the achievement levels desired for existing goals. The level of desired achievement may be increased or decreased.

For example, the goal set for a computer system may change if a requirement is imposed by management (the supra-system) for system data to be shared among multiple users rather than be available only to a single user.

When a supra-system exerts stress on a system, the system will change to accommodate the stress, or it will become pathological; that is, it will decay and terminate.

Systems accommodate stress through a change in form; there can be structural changes or process changes. For example, a computer system under stress for more shareability of data may be changed by the installation of terminals in remote locations – a structural change. Demands for greater efficiency may be met by changing the way in which it stores data – a process change.

It is very unlikely that system changes to accommodate stress will be global change to its structure and processes. Instead, those responsible for the change will attempt to localize it by confining the adjustment processes to only one or some of its subsystems.

Question 3

System analysts develop various categories of information systems to meet a variety of business needs. Discuss any three such systems briefly. *(Final Nov 2007)*

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 organisations 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 4

Differentiate between open and closed systems. *(Final May 2007)*

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 5

Write short notes on the following:

(a) Closed and open systems *(Final May 2008)*

Answer

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

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

Open Systems: Open systems actively interact with their environment. Such systems regularly get inputs and give outputs to its environment. These systems are also subject to unknown inputs and environmental disturbances. Open systems are also able to adapt to environmental changes for their survival and growth. Business organization is an example of such system.

NOTE

2

TRANSACTION PROCESSING SYSTEM

Question 1

What is Transaction Processing Cycle? Discuss briefly four common cycles of a business activity. *(Final May 2007)*

Answer

A Transaction Processing Cycle organizes transactions by an organization's business processes. The nature and types of transaction processing cycles vary, depending on the information needs of a specific organization. Most business organizations have in common, transactions that may be grouped according to four common cycles of business activity. These common Cycles are:

- Revenue Cycle: Events related to the distribution of goods and services to other entities and the collection of related payments.
- Expenditure Cycle: Events related to the acquisition of good and services from other entities and the settlement of related obligations.
- Production Cycle: Events related to the transformation of resources into goods and services.
- Finance Cycle: Events related to the acquisition and management of capital funds including cash.

NOTE

3

BASIC CONCEPTS OF MIS

Question 1

State and explain any five characteristics of a good Management Information System.
(Final May 1996 & May 1999)

Answer

Five important characteristics for a good management information system are briefly discussed below:

1. Management Oriented: It means that effort for the development of the information system should start from an appraisal of management needs and overall business objectives. A good management information system is not necessarily meant for top management only, it may also meet the information requirements of middle level or operating levels of management as well.
2. Management directed: Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts. Mere one time involvement is not enough. For system's effectiveness, it is necessary for management to devote their sufficient time not only at the stage of designing the system but for its review as well, to ensure that the implemented system meets the specifications of the designed system. 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.
3. Integrated: Development of information should be an integrated one. It means that all the functional and operational information sub-systems should be tied together into one entity. An integrated information system has the capability of generating more meaningful information 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.
4. Common data flows: It means that the use of common input, processing and output procedures and media whenever possible is desirable. Data is captured by system analysts only once and as close to its original source as possible. They, then, try to utilise a minimum of data processing procedures and sub-systems to process the data and strive to minimise the number of output documents and reports produced by the system. This eliminates duplication in data collections and documents and procedures. It also simplifies operations and produces an efficient information sytem. However, some duplication is necessary in order to insure effective information system.

5. Heavy planning element: A management information system 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.

Question 2

(a) Explain the concept of MIS in terms of its three elements. (Final Nov. 1996 & May 1998)

(b) Discuss the potential impact of computers and MIS on different levels of management. (Final May 1998 & Nov. 2003)

Answer

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

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

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

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

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

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

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

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

Information is the substance on which business decision are based. Therefore, the quality of information determines the quality of action or decision. The management plays the part of converting the information into action through the familiar process of

decision-making. Information has come to occupy a very important position in the survival of a business.

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

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

(b) 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 realise 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. Computerised 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 recentralisation. The new information technology will enable management to view an operation as a single entity whose effectiveness can only be optimised 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 organisation 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 computerisation. 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 revolutionise 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 3

Discuss the three approaches of MIS development. *(Final May 2000)*

Answer

For developing MIS, three approaches are used, viz., Top down approach, Bottom up approach and Integrative approach. Each of these is described below:

(i) Top down approach: The development of MIS under top down approach starts with the defining of the objectives of the organisation, the kind of business it is in, and the constraints under which it operates. The activities or functions for which information would be required are also identified. The crucial strategic and tactical decisions are also defined and the decisions necessary to operate the activities are specified. From the activities or functions and the decisions to be made, the major information requirements are ascertained.

This approach develops a model of information flow in the organization, which acts as a guide for designing the information system. By using the model of information flow, various information sub-systems may be defined. Each sub–system comprises of various modules. The selection of a module for developing system is made on the basis of the priority assigned to it.

The various sub–systems and their modules are coordinated to achieve the objective of integration. The information system so developed is viewed as a total system, which is fully integrated, rather than as a collection of loosely coordinated sub–systems.

It is also evident from the nomenclature that top management takes the initiative in formulating major objectives, policies and plans in a comprehensive manner and communicates them down the line to middle and supervisory management levels for translating them into performance results. Managers other than those at top levels have little role in planning, they have to only concentrate on implementation and day–to–day control.

(ii) Bottom-up approach: The development of information system under this approach starts from the identification of life stream systems. Life stream systems are those systems, which are essential for the day–to–day business activities. The examples of life stream systems include payroll, sales order, inventory control and purchasing etc. The development of information system for each life stream system starts after identifying its basic transactions, information file requirements and information processing programs.

After ascertaining the data/information requirements, files requirement and processing programs for each life stream system, the information system for each is developed. The next step is towards the integration of data kept in different data files of each information system. The data is integrated only after thoroughly examining various applications, files and records. The integrated data enhances the shareability and evolvability of the database. It also ensures that all programs are using uniform data. Integrated data also provides added capability for inquiry processing and ad–hoc requests for reports.

The next step under bottom up approach may be the addition of decision model and various planning models for supporting the planning activities involved in management control. Further, these models are integrated to evolve model base. The models in the model base facilitate and support higher management activities. They are useful for analysing different factors, to understand difficult situations and to formulate alternative strategies and options to deal them.

(iii) Integrative approach: This approach can overcome the limitations of the above two approaches when used objectively. Integrative approach permits managers at all levels to influence the design. Top management identifies the structure and design of MIS suitable to the concern. This design is further presented to lower level managers for their views and modifications. The managers at the lower level are permitted to suggest changes, additions, or deletions and return the design with their suggestions to the top level for approval. The revised design is drawn and evaluated by the top level and sent down again in a modified form for further consideration if required. This evaluation modification and approval process continues until a final design is achieved, that is suitable for all levels.

Question 4

Discuss the various factors on which the information requirements of executives depend.
(Final May 1997, Nov. 1998 & May 2001)

Answer

The factors on which information requirements of executives depend are discussed below:

1. Operational function: The grouping or clustering of several functional units on the basis of related activities into a sub-system is termed as a 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. Information requirement depends upon operational function. The information requirements of different operational functions vary 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 function, the content of information may be about the consumer behaviour, 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.

2. Type of decision making: Organizational decisions can be categorized as programmed and non-programmed ones.

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

   Non-programmed decisions: Decisions which are unstructured, involve high consequence, complex or a major commitment are known as non-programmed decisions, for example, new product line; capital budgeting etc. Non-programmed decision making has no pre-established decision procedure. Also, it is difficult to completely specify the information requirements for taking these decisions.

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

   Strategic Level: Strategic level management is concerned with developing of organizational missions, objectives and strategies. These three components are part of strategic plan and are output of the strategic planning process. Through strategies, top management tries to relate a company with its environment. It is essentially decisions regarding what products to produce and market. Based on strategic decisions, resources will be allocated to the various divisions and units in the organisation.

   Tactical Level: Tactical level lies in middle of managerial hierarchy. At this level managers plan, organize, lead, and control the activities of other managers. They coordinate the activities of a sub-unit, for example marketing. They also ensure that

resources are obtained and used efficiently in the accomplishment of the organizational objectives.

Supervisory Level: This is 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.

At strategic level, information is required on the trends in the external environment (economic, technological, political and social) and on the functioning of the internal organizational sub-systems. The nature of information required at tactical level is less diverse and complex. Much of the information required is internal in nature. Supervisory level managers mostly need internal information on operational aspects of the functioning of activity units.

Question 5

Explain three broad categories of the planning information requirements of executives.

(Final May 2004)

Answer

The planning information requirements of executives can be categorised into three broad categories:

(i) Environment information: It comprises of the following:

Government policies: Information about concessions/benefits, government policies in respect of tax concessions or any other aspects, which may be useful to the organisation in the future period.

Factors of production : Information related with source, cost, location, availability, accessibility and productivity of the major factors of production viz., (i) labour, (ii) materials and parts and (iii) capital.

Technological environment : Forecast of any technological changes in the industry and the probable effect of it on the firm.

Economic trends : It includes information relating to economic indicators like consumer disposal income, employment, productivity, capital investment etc. Such information is valuable for those firms specially whose output is a function of these important variables.

(ii) Competitive information : It includes the following information.

Industry demand : Demand forecast of the industry in respect of the product manufactured and in the area in which the firm would be operating.

Firm demand : Assessment of the firm's product demand in the specified market. It also includes an assessment of firm's capability to meet firm's demand.

The competitive data : Data of competing firms for forecasting demand and making decisions and plans to achieve the forecast.

(iii) Internal information : It usually includes information concerning organisations' (a) sales forecast, (b) financial plan/budget, (c) supply factors, and (d) policies, which are vital for subsidiary planning at all levels in the organisation.

Question 6

Discuss various constraints that come in the way of operating an effective M.I.S. How these constraints could be avoided? *(Nov. 1998 & May 2002)*

Answer

Following constraints come in the way of operating an effective MIS:

1. Non availability of qualified staff: The most important requirement for operating an effective MIS is that of qualified system and management staff. These officers should understand the views of their fellow officers. Moreover, experts should be capable of understanding the objectives of the organization and provide a desired direction for installing and operating system. This problem may be overcome by grooming internal staff. The grooming of staff should be preceded by proper selection and training.
2. Selection of Sub system of MIS: Experts usually face the problem of selecting the sub system of MIS to be installed and operated upon.

   This constraint could be overcome by identifying the need and importance of the function for which MIS can be installed first.
3. Non Cooperation from staff: This is a very crucial problem. It should be handled carefully and tactfully. This problem may be solved by educating the staff about the utility of MIS. The task should be carried out by organizing lectures, showing films and explaining the utility of the system. Besides this, some persons from staff should also be involved in the development and implementation of the system.
4. High turnover of MIS experts: High turnover is on account of several factors such as pay packet, promotion chances, future prospects, behaviour of top managers etc.

   This problem can be handled by creating the better working conditions and paying at least at par with similar *organizations*.
5. Non-standardised approach: Due to varied objectives of the business organizations, the approach adopted by experts for designing and implementing MIS is a non standardized one. Though in this regard, nothing can be done at the initial stage, but by and by standardization may be arrived at, for the organizations in the same industry.
6. Difficulty in qualifying the benefits of MIS: Due to the difficulties in quantifying the benefits of MIS, the justification of the cost involved is difficult. Therefore, this raises the questions by departmental managers about the utility of MIS. They forget that MIS is a tool which is essential to fight out competition and the state of uncertainty that surrounds business today.

This constraint can be resolved by educating the top managers and telling them about the advantages of MIS. Moreover, the example from similar industries could be brought to the notice of top executives which are having better profits.

Question 7

Differentiate among Strategic, Tactical and Operational categories of Information required for different levels of Managerial decision-making. *(Final Nov. 2002)*

Answer

Strategic-level information systems help senior management to tackle and address strategic issues and long-term trends, both within the firm and external environment. Their principal concern is matching changes in the external environment with existing organisational capability - What will be the cost-trends, where will our firm fit in, what products should be made etc ? In other words, these systems are designed to provide top-management with information that assists them in making long –range planning decisions for the organization.

Tactical-level information systems serve middle level managers and help in taking decisions for a period of 2-3 years. The managers are typically concerned with planning, controlling and use summaries of transactions to aid their decision- making. In other words, these systems provide middle-level managers with the information they need to monitor and control operations and to allocate resources more effectively. In tactical systems, transactions data are summarized, aggregated, or analysed. Their purpose is not to support the execution of operational tasks but to help the manager control these operations.

Operational-level information systems are typically transaction processing systems and help in the operational level managers to keep track of elementary activities and transactions of the organisations such as sales, receipts, cash deposits, flow of materials etc. Their purpose is to answer routine questions and to track flow of transactions. Thus, the primary concern of these systems is to collect, validate, and record transactional data describing the acquisition or disbursement of corporate resources.

Thus, each type of information system serves the requirements of a particular level in the organisation, providing the needed basis for decision making.

Question 8

Discuss the effect of applying computer technology to Management Information System.

(Final Nov. 1996 & May 2003)

Answer

The effects of applying computer technology to Information System are as discussed below:

(i) *Speed of processing and retrieval of data increases*: Modern business situations invariably call for systems capable of providing relevant information with minimal loss of time. Manual system, howsoever well organized, often fails to match the demand

for information for decision-making. Computer with its unbelievably fast computational capability and systematic storage of information with random access facility has emerged as an answer to the problems faced in modern days management. The speed of computer processing is in new range i.e. an operation takes only billionths of a second. This characteristic of computer has accounted for as a major factor in inducing MIS development.

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

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

(iv) *Complexity of system design and operation increased :* After the inclusion of computer for MIS development, system experts faced problems in designing system and their operations because of the non availability of experts in the initial stage. But in the present situation, the computer manufacturers have developed some important programs (software) to help their users. Also, private agencies are there to develop programs to cater to the specified needs of their customers either on consultancy basis or on contract.

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

(vi) *Increases the effectiveness of Information Systems :* Before the existence of computer technology, it was difficult to provide the relevant information to business executives in time even after incurring huge expenses. The use of computer technology has

overcome this problem, by providing timely, accurate and desired information for the purpose of decision-making.

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

Question 9

(i) Describe briefly three levels of Management.

(ii) Mention at least two pieces of information-one internal and one external- required at every one of the levels of Management. *(Final Nov. 2003)*

Answer

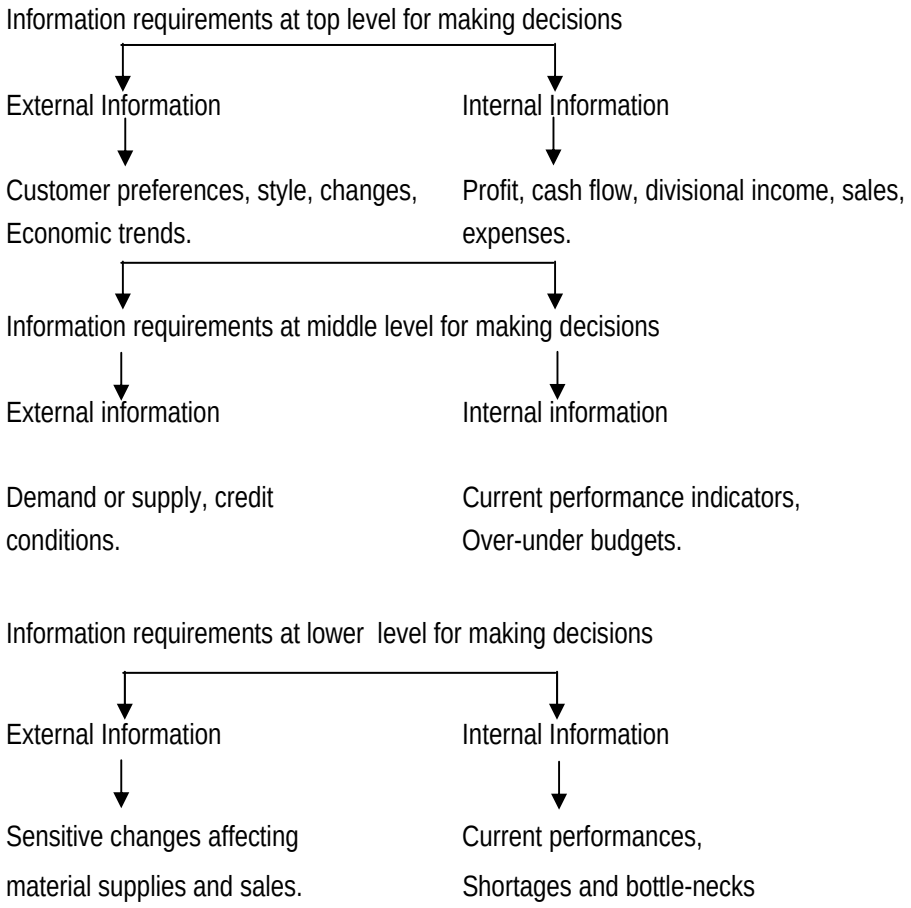
(i) Three levels of management are briefly discussed below:

Strategic level: Strategic level is defined as a set of management positions that is concerned with developing of organisational missions, objectives and strategies, directing and managing the organization in an integrated manner. Decisions made at this level of organization to handle problems critical to the survival and success of the organization are called strategic decisions. Strategic level also establishes a budget framework under which the various departments will operate.

Tactical decisions: This level lies in the 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, are made to implement strategic decisions. Tactical decisions are relatively short, step-like spot solutions to breakdown strategic decisions into implementable packages.

Supervisory level: This is the lowest level in managerial hierarchy. The managers at this level coordinate the work of others who are not themselves managers. At supervisory level, managers are responsible for routine, day-to-day decisions and activities of the organisation which do not require much judgment and discretion. They ensure that specific tasks are carried out effectively and efficiently.

(ii) Two pieces of information - one internal and one external - required at every one of the levels of management are stated on next page:



(In the answer, we have stated sample pieces of information, both internal and external, at each level of management. There can be many different types of information requirements).

Question 10

Describe the main pre-requisites of a Management Information System, which makes it an effective tool. *(Final Nov. 2003,May 2005)*

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 organised in such a way that access to the data is improved and redundancy is reduced. Normally, the database is subdivided into major information sub-sets needed to run. The database should be user-oriented, capable of being used as a common data source, available to authorized persons only and should be controlled by a separate authority such as DBMS. Such a database is capable of

meeting information requirements of its executives, which is necessary for planning, organising 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 organisation should device checks for the information system control.

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

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

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

Question 11

Discuss the limitations of the Management Information system. *(Final May, 2006)*

Answer

Limitations of the Management Information System :

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

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

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

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

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

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

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

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

Question 12

What do you mean by Information? Describe the important characteristics of information, which makes it useful to the organization. *(Final May 2006)*

Answer

Information: 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. The term data and information are often used interchangeably. However, the relation of data to information is that of raw material to finished product.

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

(i) Timeliness: Timeliness refers to when user needs information. Some information is required on regular, periodic basis – perhaps daily, weekly, monthly or quarterly, while much other information is generated on the request of the manager. Usually as we proceeds from lower level to higher level of management, the time interval necessary for providing decisions impelling information on a routine or on exception basis increases at strategic level.

(ii) 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 organisations. The basic purpose of information is to inform, evaluate, persuade and organize. It helps in creating new concepts, identifying problems, solving problems, decision making, planning and controlling.

(iii) Mode and Format: The mode of communicating information in business are either visual, verbal or in written form. Format of information should be so designed that it assists in decision-making, solving problems, planning, controlling and searching. Therefore, all the statistical rules of compiling statistical tables and presenting information by means of diagram, graph, curves etc. should be considered. The reports should be preferably supplied on an exception basis to save the manager from an

overload of information. Also the data should be classified into categories, which have relevance to the problem at hand.

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

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

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

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

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

(ix) Cost benefit analysis: The benefits that are derived from the information must justify the cost incurred in procuring information. The information may be categorised into three categories: (i) necessary (ii) normal and (iii) extra. The information of necessary 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. Some of the normal statements can be discontinued or replaced if their costs are too high.

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

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

Question 13

State the factors to be considered for designing an effective Management Information System.

(Final Nov. 2006)

Answer

The following factors should be considered for designing an effective MIS:

1. Management Oriented: The development of Management Information system should start from assessment of management needs and overall business objectives. Such system does not only take care of the information requirements of the top management but it also caters to the information needs of the middle and operating levels of management.
2. Management Directed: As MIS is oriented towards the information needs of the management; it is essential that management should direct the development efforts of such systems on an on-going basis. Management should devote sufficient time not only at the stage of conceptualization and designing, but also for the regular reviews of its effectiveness. In short, management should play the key role in setting the system specifications as well as subsequent trade-off occurring in system development.
3. Integrated: All functional and operational information sub-systems should be integrated into one entity. Such Information system has the potential of generating meaningful and comprehensive information to management.
4. Common Data flows: For such integrated information system, data is captured only once and as close to its original generating source as possible. This eliminates duplication in data collection, documents and procedures. It also simplifies operations and produces an efficient and effective information system. However, the duplication cannot be avoided to some extent in order to ensure such system.
5. Meticulous Planning: It takes 3 to 5 years, sometimes even longer period, to get the MIS system established firmly in an organization. Therefore, there should be meticulous planning in designing and development of MIS system. It should be designed considering the future objectives and information needs of the organization. The system obsolescence should be avoided before it becomes operational.
6. Sub Systems approach: Although MIS is considered to be a single entity, it is broken into various sub systems so that it can be implemented one at a time by developing the systems in phases. This ensures meaningful and effective implementation of information systems.
7. Common Database: The common database holds all functional systems together, consolidates and integrates data of all functional systems. The access to this database is allowed to the users of sub systems on need-to-know and need-to-do basis. It eliminates duplication in data storage, updating and protection as well as optimizes the cost of data storage and management.
8. Computerized: MIS can be established using a manual system. Use of computers increases the effectiveness of the system. In fact, it equips the information system to handle variety of applications by catering quickly to their information requirements.

   While designing an MIS, it should also be considered that computerization has following effects on management Information Systems:

   (1) High speed of data processing and retrieval.

   (2) Expanded scope of use of Information system.

   (3) Wide scope analysis.

(4) Increased complexity of system design and operations.

(5) Integrated functioning of various information sub-systems.

(6) Enhanced effectiveness of Information Systems.

(7) Comprehensive Information.

Question 14

Describe the main prerequisites of a MIS which makes it an effective tool. Explain the major constraints in operating it *(Final May 2008)*

Answer

Please refer to answer to question No. 10 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:

(1) Non-availability of experts, who can diagnose the objectives of the organization and provide a desired direction for installing an operating system.

(2) Experts usually face the problem of selecting the sub-system of MIS to be installed and operated upon.

(3) Due to varied objectives of business concerns, the approach adopted by experts for designing and implementing MIS is a non-standardised one.

(4) 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.

(5) 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.

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

Question 15

XYZ company engaged in manufacturing and installing power plant equipments has installed a new MIS and you have been requested to evaluate its effectiveness. On what parameters would you evaluate the MIS system? *(Final Nov. 2008)*

Answer

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

(1) Examining whether enough flexibility exists in the system, to cope with any expected or unexpected information requirement in future.

(2) Ascertaining the views of users and the designers about the capabilities and deficiencies of the system.

(3) Guiding the appropriate authority about the steps to be taken to maintain effectiveness of MIS.

The following factors should be considered for designing an effective MIS:

Refer question 13 for answer on designing an effective MIS.

4

SYSTEMS APPROACH AND DECISION MAKING

Question 1

Discuss various benefits which are attained by implementing a computerized model for making decision. *(Final May 2003)*

Answer

A growing number of companies are making effective use of MIS in aiding the decision making process. For example, a major chemical company uses a computer model to simulate an industry segment and the company's potential for a share of market and profitability. A computerized model may incorporate accounting, production, transportation, manufacturing and marketing operations of the company. Such models allow a decision maker to consider a large number of factors in decision-making process, which was not possible in manual system. This highlights the need to reduce skepticism that managers have toward sophisticated computerized decision making aids. This type of model puts pertinent information into a analytical framework that aids the management decision making process.

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

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

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

5. The models also estimate the amount of cash that will be received and spent each month i.e. in which months there will be excess funds that might be put to use and in which month there will be insufficient funds. Thus, the information supplied helps managers to make decisions about investing, purchasing and borrowing money. The models also help in tracking cash balances on a day-to-day basis and help the managers in their investment decisions so as to maximize organization income.

6. Computerized models are highly useful for carrying out analysis of historical data speedily, which may be quite difficult or even impossible manually for forecasting the future.

Question 2

Explain the role played by Financial Information System in making financial decisions.
(Final Nov. 2003 & May 2006)

Answer

Financial Information System plays an important role in making following financial decisions:

(i) Estimation of requirements of funds: This is the very important and starting point of making financial decisions. A very careful estimation of funds and the time at which these funds are required is made in this stage. This can be done by forecasting all physical activities of the firm and translating them into monetary units.

(ii) Capital structure decisions: Decisions are to be taken to select an optimum mix of different sources of capital structure. There are many options available for procuring funds. Decision maker has to decide the ratio between debt and equity, long-term and short-term funds etc. He has to ensure that overall capital structure is such that the company is able to procure funds at optimum cost.

(iii) Capital budgeting decisions: Funds procured from various sources are required to be invested in different assets. With the help of capital budgeting, decision maker can determine feasibility of investment in long-term assets. This will help in attainment of financial objectives.

(iv) Profit planning: This part of profit planning is essential for the growth of the organization. The decision maker has to make decision regarding profits and dividends. He has to ensure adequate surplus in future for growth and distribution of dividends.

(v) Tax management: Tax planning is aimed at reducing of outflow of cash resources by way of taxes so that the same may be effectively utilized for the benefit of business. The purpose of tax planning is to take full advantage of exemptions, deductions, concessions, rebates, allowances and other relief.

(vi) Working capital management: Working capital management is concerned with the investment of long term funds into current assets. Decisions are to be taken for effective financing of current assets required for day-to-day running of the organization.

(vii) Current assets management: Policy decisions are taken regarding various items of current assets. Credit policy determines the amount of sundry debtors at any point of time. Inventory policy is to be determined jointly between finance and production department.

Question 3

Define personnel information system. List its various basic sub-systems and explain them in detail. *(Final May 1998, May 2004 & May 2008)*

Answer

The personnel information system deals with the flow of information about people working in the organisation as well as future personnel needs. In most of the organisations, the system is concerned primarily with the six basic sub-systems of the personnel function; recruitment, placement, training, compensation, maintenance and health and safety..

It is generally accepted that the personnel function is one of the least computerised of all the functions. Automated system may not be necessary for small, but large business firms are realising that computer based personnel information systems are necessary for increasing the operational efficiency of personnel management. Originally, many organisations used computer–based information systems to produce pay cheques and payroll reports, maintain personnel records and analyse the use of personnel in business operations. Many organisations have gone beyond these traditional functions and have developed personnel information systems, which also support (i) recruitment, selection and hiring (ii) job placement (iii) performance appraisals, (iv) employee benefit analysis, (v) training and development and (vi) health, safety and security. Such information system support the concept of human resource management (HRM). The goal of HRM is the effective and efficient use of the human resources of a company.

The personnel system should be organised on functional basis. It should have the following information sub–systems to increase the operational efficiency of personnel management.

1. Recruitment: Properly managed recruitment sub–system may forecast personnel needs and skills required for recruiting personnel at the proper time to meet organisational manpower needs. Such a sub-system may not only furnish information concerning skills required for company programmes and processes but also maintains the inventory of skills available within the organisation.

2. Placement: This sub-system is concerned with the task of matching the available persons with the requirements. A good placement sub-system makes use of latest behavioral tools and techniques. It ensures that the capabilities of people are identified before being matched with properly organised work requirements.

3. Training and development: As technological changes and demands for new skills accelerate, many companies find that they must develop much of their requirements from internal sources. In addition, a large part of the workforce must constantly be updated in new techniques and developments. This task is the function of the training and development sub–system.
4. Compensation: This sub-system is concerned with the task of determining pay and other benefits for the workers of the concern. It makes use of traditional payroll and other financial records, government reports and unions expectation before arriving at the final figures of pay and other benefits for each category of workers.
5. Maintenance: This sub-system is designed to ensure that personnel policies and procedures are achieved. It may be extended to the operation of systems of control, work standards which are required to measure performance against financial plans or other programmes, and the many subsidiary records normally associated with the collection, maintenance and dissemination of personnel data.
6. Health & Safety: This sub-system is concerned with the health of personnel and the safety of jobs in the organisation.

Question 4

What are the production information requirements of a GM (Production and Operations Management) with regard to production planning and control ? (Final Nov. 2004)

Answer

The production planning and control system involves two main procedures: the specification of materials and operations requirements and production scheduling. The information requirements of a GM for the materials and operations phase of any organisation are as stated below:

(i) Firm's policy with regard to production of various products.

(ii) Sales order, sales forecast, stock position, order backlog.

(iii) Available labour force with their capabilities

(iv) Standards of labour time, material, machine time and overhead cost etc.

(v) Schedule of meeting the sales orders, region-wise, territory-wise etc.

(vi) Quality norms for materials to be used and for the finished products.

(vii) Break-up of the jobs and their resource requirements.

Planning the specific time at which product items should be manufactured is known as production scheduling. The information is required by the production-scheduling department so as to meet the following objectives:

(i) to determine the stages of production in sequential and rational order;

(ii) to minimise the idle time on the part of the operators and equipments;

(iii) to assess the extent of need for subcontracting to outside parties;

(iv) to ensure that completion dates and target dates of completing the production plans are met fully; and

(v) to study alternative methods to performing the activities so that time taken to perform can be further reduced.

Question 5

What are the variables that the top management should consider during negotiations with the labour unions? (Final Nov. 2004)

Answer

Many types of labour today are unionized. Unionized organisations usually have strict regulations regarding such items as pay scales, hiring and firing, promotions and working conditions. Management has the choice of trade – offs on the following variables during negotiations with the labour unions

(i) Wage raise

(ii) Paid holidays

(iii) Contribution to employees, insurance and pension plan

(iv) Overtime premiums.

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

Question 6

Write short notes on the following:

(a) Materials Requirement Planning (MRP) (Final May 2002 , May 2003, May 2006)

(b) Strategic and Tactical Decisions. (Final Nov. 2004)

Answer

(a) Materials Requirement Planning (MRP): It is eye-opening to note that a major cause of production inefficiency is a lack of integrated production planning, production scheduling, and production control information system. One approach to improve production efficiency is materials requirement planning (MRP). MRP integrates several production related information system so that MRP system can access and extract data from these systems to accomplish production scheduling. MRP's purpose is to greatly improve both inventory management and production scheduling. To achieve the efficiencies of which

they are capable, MRP system require high levels of discipline- such as not requisitioning materials long before they are needed, proper scrap reporting and using well-defined procedures for implementing and recording changes promptly. Accurate input data also is absolutely necessary, for example inventory quantity data must be accurate and interplant transfers must be recorded accurately and promptly.

The benefits of MRP system are:

(i) Significantly decreased inventory levels and corresponding decrease in inventory carrying costs.

(ii) Fewer stock shortage, which cause production interruption and time-consuming schedule juggling by managers.

(iii) Increased effectiveness of production supervisors and less production chaos.

(iv) Better customer service – an increased ability to meet delivery schedules and to set delivery dates earlier and more reliably.

(v) Greater responsiveness to change.

(vi) Closer coordination of the marketing, engineering and finance activities with the manufacturing activities.

(b) Strategic and Tactical Decisions: Decisions made at the strategic level of the organization to handle problems critical to its survival and success are called strategic decisions. They have a vital impact on the direction and functioning of the organization. Some of the examples are decision on plant location, introduction of new products, making major new fund – raising and investment operations, adoption of new technology etc. Much analysis and judgment go into making strategic decisions. Strategic decisions are made under conditions of partial knowledge and generally can not be programmed.

Tactical level decisions are to be taken by middle level of managerial hierarchy. At this level, managers plan, organize, lead and control the activities of other managers. 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 forecasted and quantified without much difficulty and their impact is relatively localized and short-range. Tactical decisions are made with a strategic focus.

The distinction between strategic and operational decisions could be high-lighted by means of an example. Decisions on mobilisation 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.

Question 7

A Company is planning to introduce a new range of products. The top management is advised to get developed a marketing information system which can enhance the decisional capacities in various marketing activities. You being in-charge of this project suggest what information sub-systems are required to be developed. *(Final May 2005)*

Answer

Marketing Information System - It is aimed at supporting the decision making, reporting and transaction processing requirements of marketing and sales management. It consists of following inter-related information sub-systems to enhance the decision-making capacities in various marketing activities:

1. Sales - The objective of the sales manager is to coordinate the sales effort so that the long-term profitability of the company is maximized. Decisions are required in the area of adequate stocks, effective distribution channels, effective motivation of sales personnel, promotion of more profitable products or product lines and good customer relations. Information required for analysis and support of sales is as stated below:

   (a) *Sales Support* – Sales support information system provides information to sales personnel about the following:

      (i) Product descriptions and performance specifications

      (ii) Product prices;

      (iii) Quantity discounts,

      (iv) Sales incentives for salespersons

      (v) Sales promotions;

      (vi) Strengths and weaknesses of competitor's product;

      (vii) Products' inventory levels.

      (viii) The histories of customers' relations with the company.

      (ix) Sales policies and procedures established by the company

      (x) Buying habits of customers

(b) Sales analysis – The sales analysis is a major activity in most companies involved in sales. Its purpose is to provide information for analysis of

(i) Product sales trends;

(ii) Product profitability on the product-by-product basis;

(iii) The performance of each sales region and sales branch;

(iv) The performance of respective sales persons.

Information for sales analysis is derived primarily from the sales order entry system; the majority of information from actual sales transactions and is contained on sales invoice. It includes information on product type, product quality, price, customer identity and type, sales region and salesperson etc.

2. Market Research and Intelligence –The objective of marketing research is to investigate problems confronting the other managers in the marketing function. These problems may involve sales, product development, advertising and promotion, customer service, or general marketing management needs. To satisfy these decision-making and reporting requirements, the market research department must either periodically or upon demand gather information from a wide variety of sources. The investigations undertaken by market research helps in satisfaction of following informational needs of managers:

(i) Information about the economy and economic trends and the probable impact of these trends on demand for the product.

(ii) Information about the past sales; and sales trends for the entire industry;

(iii) Information about potential new markets for product;

(iv) Information about competitors, its product, strength, weaknesses, new product plans, strategies and so on.

The decision-maker can use the information provided by marketing research in a number of ways for decision making process.

3. Advertising and Promotions - The promotion and advertising development devotes its attention to planning and executing advertising campaign and to carry out various product promotions. This includes:

(i) Promotion through limited budget;

(ii) Allocating resources in most effective manner

(iii) Analysing an array of information, sales people, locations, products, styles, sizes etc.;

(iv) Storing information that can be combined with past experiences of managers ;

(v) Establishing a body of knowledge on the response of market for each of the several types of promotional activities such as coupons, contests, trade show;

(vi) Continuously refreshing and modifying the information base in accordance with rapid changing environment.

4. Product Development and Planning – Product development involves analysing a possible opportunity for a new product and evaluating preferred specifications and probable market success. Often the market research activity initially perceives the opportunity and passes along information about it to the new product development group.Alternatively,

   - Sales persons may be aware of their need for a new product;
   - Customer call reports may help elicit information about new product needed which may encourage sales persons to think about new product possibilities.
   - Sales analysis system indicates the most desirable characteristics for the new product;
   - Market researchers gather information about the size and structure of the market place for the product.

   The product development department uses all these information to develop specifications for a new product. Product planning system provides marketing management with packaging, promotion, pricing and style recommendations throughout the life of product.

5. Product Pricing System – Product pricing is a complex managerial activity that is affected by product cost, customer demand, market psychology, competitors, prices and various actions taken by competitors. Prices may be determined on a full cost or marginal cost basis which is usually seen as the starting point in setting prices. Pricing information system almost always utilizes information about product cost. Past sales profitability information is useful to help in determining how much prices should be adjusted for changes in cost to ensure that margins are maintained.

6. Customer Service – The objective of marketing department is to satisfy customers with product and customer service. To achieve these objectives, management provides customers with technical assistance and product maintenance. Decisions are required in the area of training of service personnel, capabilities of equipment and location facilities to serve customers and assist in the dissemination of technical information to the customers. These decisions must be congruent with the marketing management strategy regarding customer satisfaction and service.

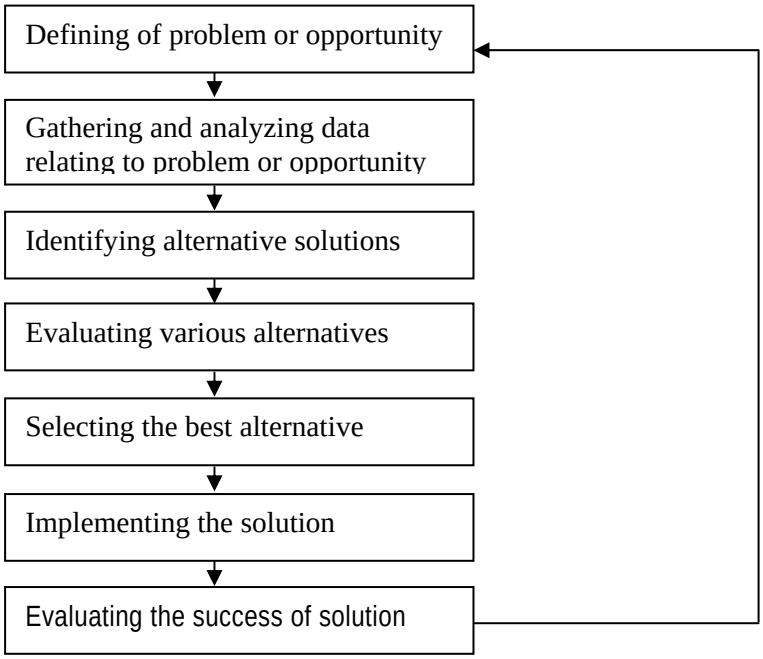
Question 8

How system approach can be used for solving problems? *(Final Nov. 2005)*

Answer

The system approach to management is in fact a way of thinking about management problems. It visualizes an organization as a group of interacting and interdependent parts with a purpose. Managers are not in a position to deal with individual parts separately since action of one part is going to affect other parts. Each problem should be examined in its entirety to the extent possible and economically feasible from the point of view of the overall system of which the problem under consideration is one part. Under this approach, a manager should make conscious attempt to understand the relationship among various parts of the organization and their role in supporting the overall performance of the organization. Before solving problem in any financial area, or in any specific sector of the organization, he should understand fully how the overall system would respond to changes in its component parts.

To understand how the system approach to problem solving is applied, let us consider the problem of long delays between receipts of orders and delivery in some hypothetical company. To seek a solution for the problems by applying systems approach, we would make use of the following steps as shown in the figure given below:



(i) Defining of the problem: The problem involved here is of inordinate delay between the receipt of orders and their delivery. This problem affects the vendor in various ways, e.g., a bad reputation, loss of customers, reduction in profits etc.

(ii) Gathering and analyzing data: The problem of delay may be because of following reasons:

  (a) Excessive orders in the hand of vendors

  (b) Shortage of power

(iii) Identification of alternative solutions: To overcome the stated problem by system approach, suppose the following two solutions exist:

  (a) Refusals of orders, in case the total size of the orders exceeds the plant capacity of one shift.

  (b) To run the plant in double shift to meet the commitment in time. Any shortfall in power supply may be met by installing a generator.

(iv) Evaluation of alternative solutions: Out of the two solutions as stated above, the second solution say accounts for an overall increase in the profitability of the concern after off-setting additional cost for the generator produced power. It also helps in retaining customers and growth of the concern.

(v) Selection of the best alternative: Under this step, the management closely examines the alternatives and chooses the best alternative. In this case, the second alternative is finally chosen.

(vi) Implementation of the solution: The implementation of the solution requires the necessary policy changes. Besides this, the resources required to run the plant in double shift and installation of the generator are also to be arranged. Finally, appropriate procedures are developed to exercise smooth production and timely supply to customers. The concerned officers are accordingly instructed.

Question 9

"Information is necessary to executive for performing the function of planning". Substantiate the above statement with regard to information requirements of a marketing system.

(Final May 2006)

Answer

Information requirements of a Marketing System

The information required for the purpose of planning in the case of a marketing system can be classified into three types:

(i) Environmental Information: It includes the following:

(a) Political and Governmental considerations: To forecast market plan, political stability etc., information plays an important role as it enables executives to guess quite accurately the financial policies, taxation and their effect on the organization.

(b) Demographic and social trends: Information about demography, its compositions and location is also useful to business organisation for planning its products, services or outputs.

(c) Economic trends: This includes information related to the GNP level and trend, disposable income of consumers, employment, productivity, capital investments, prices, wage level and numerous other economic indicators which provide valuable planning information for those firms whose output is function of these variables.

(ii) Competitive information: Data related to business operations of competing firms is quite useful for forecasting individual firm's product demand, making decisions and plans to achieve the forecast.

(iii) Internal information: Information available from internal sources affects the planning decisions at different levels in the organizations. The main sources of internal information are: (a) Sale forecast, (b) Financial plans , (c) Supply factors and (d) Policies .

Question 10

Enumerate various information which is required for sales support and sales analysis.

(Final Nov. 2006)

Answer

Information requirements for sales support and sales analysis are enumerated below:

(i) Sales support: A specialized sales support information system must provide the following information to sales personnel:

- Products descriptions and performance specifications.
- Product Prices.
- Quantity discounts and other product discount information.
- Sales incentives for salespersons.
- Sales promotions.
- Financing plans for customers.
- The strengths and weaknesses of competitors' products.
- The histories of customers ' relations with the company.
- Sales policies and procedures established by the company.

- Products that have not yet been introduced.
- Products' inventory levels.
- Buying habits of consumers.

These and other information come from a variety of sources. Product performance specifications, for example, may come from the engineering department.

(ii) Sales Analysis:

To keep abreast with the competitors in the market, the sales analysis is a very vital activity. It must provide the following information:

- Sales trends (product-wise)
- Product wise profitability
- Region, branch wise sales performance
- Sales person wise performance

The above information is derived from Sales Transaction Processing System as well as from other systems like Financial Accounting System and HR Management System etc. The majority of information comes from actual sales transactions and is contained on sales invoices. To fully support the sales analysis system, invoices should contain information about product type, product quality, price discount terms, customer identity and type, sales region, and salesperson.

Information from other sources should also be included in the sales reports. Specifically, the sales reports must contain information about the profitability of products, product lines, sales territories, and individual sales persons. Profitability reporting requires information about product administrative and selling costs.

Question 11

Write short notes on Programmed decisions *(Final May 2008)*

Answer

Programmed Decisions: Such decision procedures are applicable to situations and problems which are routinely recurring, are more familiar and can be structured. Programmed decisions have built-in pre-decided rules or procedures which are well-structured in advance and are time tested for their validity. Thus, programmed decisions are said to refer to decisions made on problems and situations by reference to a predetermined set of precedents, procedures, techniques and rules. As a consequence, by applying these rules to a problem, a decision emerges. Manager's judgement or discretion is not required. Thus, decision making is simplified.

Organisations evolve a repertory of procedures, rules, processes and techniques for handling routine and recurring problem situations. For example, for many organisations there is a set

procedure for receipt of materials, payment of bills etc. These are examples of programmed decisions which tend to be consistent over situations and time.

Question 12

What is Financial decision making? Which Financial decisions are made with the help of Financial information system? (Final Nov. 2008)

Answer

(a) Financial Decision Making: It deals with procurement of funds and their effective utilization in the business. There are two important aspects of financial decision making – first relates to decisions regarding procurement of funds and second to decisions regarding effective utilization of funds in the business.

Procurement of funds is a complex problem since there are number of sources from where the funds may be raised for long-term such as equity, debentures, bonds etc. or on short-term such as banks, suppliers, credit etc. These sources have different characteristics in terms of risk, control and cost.

Effective utilization of funds implies deployment of funds in several long term and short term assets, properly and profitably. The funds are procured at a certain cost with a certain level of risk. If they are not utilized in a manner as to generate higher income over their cost, they will cause losses to business. Thus, each decision should be properly analysed while investing in fixed assets.

For the answer on Financial Decisions by Financial Information Systems refer Question No.2.

5

DECISION SUPPORT AND EXECUTIVE INFORMATION SYSTEMS

Question 1

In what ways does an Executive Information System differ from the Traditional Information System? *(Final Nov. 2002 & May 2008)*

Answer

Executive Information System (EIS) is a tool that provides direct on-line access to relevant information, in a useful and navigable format, about aspects of a business that are of particular interest to the senior manager.

These systems are designed in such a format so that they can be used by individuals with limited time, and limited knowledge of operating computers to search information relating to broad strategic issues and then explore the information to find the root causes of those issues.

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

1. They are specifically tailored to executive's information needs.
2. They are able to access data about specific issues and problems as well as aggregate reports.
3. They provide extensive on-line analysis tools including trend analysis and exception reporting etc.
4. They can access a broad range of internal and external data.
5. They are particularly easy-to-use (typically mouse or touch- screen driven).
6. They are used directly by executives without assistance.
7. All EISs are delivered through terminals using easy-to-use software.
8. Information tends to be presented by pictorial or graphical means, whereas in most traditional information systems, information is usually presented in numerical or textual form, usually in printed report format.
9. Information is presented in summary format e.g. sales for the whole company. There is the facility to drill down to the other levels of information to see how the sales figures were arrived at – by geographical location, by product group etc.

10. The ability to manipulate data, to project `what if' outcomes and to work with modeling tools within the system are also evident in EIS. This is particularly so with external information that can be super imposed on to the company's information e.g. sales forecasts with information from the meteorological office about the weather.

Question 2

Successful executives take decisions relying more on intuition than on any quantitative analytical decision technique. Mention five characteristics of the types of information that are responsible for this phenomenon in executive decision-making. (Final Nov. 2004)

Answer

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

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

(i) Lack of structure: Many of the decisions made by executives are relatively unstructured. For Instance, what general direction should the company take? Or what type of advertising campaign will best promote the new product line? These types of decisions are not so clear-cut as deciding how to debut a computer program or how to deal with an overdue account balance. Also, it is not always obvious which data are required or how to weigh available data when reaching at a decision.

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

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

(iv) Informal source: Executives rely heavily on informal source for key information. For example, lunch with a colleague in another firm might reveal some important competitor strategies. Some other important information sources of information are meetings, tours around the company's facilities to chat with employees, brainstorming with a trusted

colleague or two, and social events. Informal sources such as television might also feature news of momentous concerns to the executives.

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

Question 3

Write short notes on the following:

(a) Decision Support System *(Final Nov. 2002)*

(b) Executive Information System (EIS) *(Final May 2001 & Nov. 2003)*

(c) Expert systems *(Final May 2004)*

Answer

(a) Decision Support System: A 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. They are easy to use and are flexible enough to respond to the changing needs of decision makers. It may be noted that a DSS is not intended to make decisions for managers, but rather to provide managers with a set of capabilities that enable them to generate the information required by them in making decisions. In other words DSS supports human decision-making processes rather than providing a means to replace it. The components of a DSS are (1) the user, (2) one or more data bases, (3) a planning language and (4) a model base. The tools for DSS include a variety of software supporting database query, modeling, data analysis and display.

Some examples of DSS in accounting are Cost accounting system; Capital budgeting system; Budget variance analysis system and General decision support system.

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

EIS require large amounts of capacity and processing power within both the system and the network. Although most computer systems may contain some of the above characteristics, they can be differentiated from EIS in a number of ways. Most MIS and operational systems are based on transaction processing carried out by a variety of on-line and batched inputs. Unilike the EIS, information is usually presented in numberical or

textual form and reporting is by exception, usually in printed report format. Also, EISs tend to be externally-focused, strategically-based systems using both internal and external data, whereas other computer systems mainly concentrate on internal control aspects of the organsiation.

An EIS serves many purposes. 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.

Secondly, EIS allows timely access to information. Timely access also influences learning. When a manager obtains the answer to a question, that answer typically sparks other related questions in the manager's mind. If those questions can be posed immediately, and the next answer retrieved, the learning cycle continues unbroken. Using traditional methods, by the time the answer is produced, the context of the question may be lost, and the learning cycle will not continue.

Finally, 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.

(c) Expert Systems: They are designed to replace the need for a human expert. They are particularly important where expertise is scarce and therefore expensive. This is not 'number-crunching' software, but software that expresses knowledge in terms of facts and rules. This knowledge will be in a specific area, and therefore expert systems are not general, as are most decision support systems, which can be applied to most scenarios, an expert system for oil drilling is not of much use in solving company taxation problems.

While there may have been a progression from transaction-processing systems, through management information systems, to decision-support and executive information systems, expert systems have arisen largely from academic research into artificial intelligence. The expert system should be able to learn, i.e. change or add new rules. They are developed using very different programming languages such as PROLOG, which are referred to as fifth generation languages, or expert systems shells, which can make the process quicker and easier. It has been suggested that expert systems would be of greater use in the tactical and strategic level. This has been the case in banking, where expert systems scrutinize applications for loans, and lower level staff accepts the system's decision. This has replaced the somewhat subjective decision-making of more senior managers.

Question 4

"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. *(Final May 2005)*

Answer

A decision support system (DSS) is defined as a system that provides tools to managers to assist them in solving semistructured and unstructured problems in their own way. 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. The DSS are characterised by following three properties:

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

(ii) Ability to adapt to changing need – Semi-structured / unstructured decisions often do not conform to a predefined set of decisions-making rules. Because of this, their decision support system must provide for enough flexibility to enable users to model their own information needs. The DSS designer understands that managers usually do not know in advance what information they need and, even if they do, those information needs keep changing constantly. Thus, rather than locking the system into rigid information producing requirements, capabilities and tools are provided by DSS to enable users to meet their own output needs.

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

Question 5

What is an Executive Information system? Discuss its various purposes. (Final Nov. 2005)

Answer

An Executive Information System (EIS) is a tool that provides direct online access to relevant information in a useful and navigable format. Relevant information is timely, accurate, and actionable information about aspects of a business that are of particular interest to the senior manager. The useful and navigable format of the system means that it is specifically designed to be used by individuals with limited time, limited key boarding skills and little direct experience with computers. An EIS is quite easy to navigate so that mangers can identify broad strategic issues and then explore the information to find the root causes of those issues.

Executive Information Systems can be used for wide range of applications. In government, EIS have been constructed to track data about ministerial correspondence, case management, workers productivity, finances and human resources etc. EIS have also been used to monitor information about competitors in the news media and data bases of public information etc.

EIS require large amounts of capacity and processing power within both the system and the network since information is in summary format by pictorial or graphical means. However, EIS has the facility to "drill down" to other levels of information to see the details. The ability to manipulate data, to project "what if" outcomes and to work with modeling tools. Within the system are also evident in EIS.

Purposes of EIS:

(i) The primary purpose of an EIS is to support managerial learning about an organisaiton, its work processes and its interaction with the external environment. Informed managers can ask better questions and make better decisions.

(ii) Second 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 requirements often inhibit managers from obtaining this information. Often, by the time a useful report can be compiled, the strategic issues facing the manager change, and the report can not be used. Timely access also influences learning. When a manger obtains the answer to a question, that answer typically sparks other related questions in the manger's mind. This way learning cycle continues unbroken.

(iii) 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 look upon this as an opportunity to discipline subordinates.

(iv) Sometimes misaligned reporting systems can result in inordinate management attention to things that are not so important. An EIS system can provide information that is actually important and represents a balanced view of the organisation's objectives.

Question 6

Describe various software tools used in Decision support system. *(Final May 2006)*

Answer

Software tools of DSS: Decision support system includes a variety of software supporting database query, modelling, data analysis and display. These tools fall under following four categories:

(i) Database languages: Tools supporting database query and report generation use mainframe, mini computer and microcomputer based databases. FOCUS, RAMIS and NOMAD II are mainframe based languages supporting data base query, report generation and analysis. FOCUS, RAMIS are also available in PC version. MS Access is one of the most popular database query package used in Window based PC.

(ii) Model based Software: Model based analysis tools such as spreadsheet software enable manager to design models that incorporate business rules and assumptions. Lotussuits and MS-Excel supports model building and "what if" type analysis. Modelling tools like IFPS are designed to support financial modelling and analysis.

(iii) Statistics and Data Manipulation tools: Statistical analysis software such as SAS, SPSSS supports market researchers, operation research analysts and other professionals using statistical analysis functions and are generally used on mainframe computers. Microcomputer-based statistical packages are available as well.

(iv) Display based DSS: Graphic displays of output generated from MS-Excel are very effective in management presentation. Graphics tools running in a mainframe environment include DISSPLA, TELLAGRAF and SASGRAPH. Microcomputer based tools such as Harward Graphics, and Power Point display output in the form of pie charts, bar charts and graphs.

An integrated module of MS-Excel and Power-Point that provides the ability to generate, manipulate and statistically analyse data is best example of query, modelling and display software.

Question 7

"Decision support systems are widely used as part of an Organisation's Accounting Information system". Give examples to support this statement. (Final May. 2007)

Answer

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

- Cost Accounting System: The health care industry is well-known for its cost complexity. Managing cost in this industry requires controlling costs of supplies, expensive machinery, technology, and a variety of personnel. Cost Accounting applications help health care organisations calculate product costs for individual procedures or services. Decision support systems can accumulate these product costs to calculate total costs per patient. Combining cost accounting DSS and Productivity system applications allows managers to measure the effectiveness of specific operating processes to improve its management decision-making.
- Capital Budgeting System: Companies require new tools to evaluate high-technology investment decisions. Decision makers need to supplement analytical techniques with decision support tools that consider some benefits of new technology. One decision support system designed to support decisions about investments in automated manufacturing technology that is AutoMan, which allows decision makers to consider financial, non-financial, quantitative, and qualitative factors in their decision-making processes. Using this decision support system, accountants, managers, and engineers

identify and prioritize these factors. They can then evaluate up to seven investment alternatives at once.

- Budget Variance Analysis System: Financial institutions rely heavily on their budgeting systems for controlling costs and evaluating managerial performance. DSS allows comptrollers to graph, view, analyse, and annotate budget variances, as well as create additional one-and five year budget projections using the forecasting tools provided in the system. The decision support system thus helps the comptrollers create and control budgets for the cost-center managers reporting to them.
- General Decision Support System: These types of decision support systems are a decision-maker's tools that are used to input the data and answer questions about a specific problem domain to make use of this type of decision support system. An example is a program called Expert Choice. This program supports a variety of problems requiring decisions. The user works interactively with the computer to develop a hierarchical model of the decision problem. The decision support system them asks the users to compare decision variables with each other. Expert Choice analyses investment judgments and presents the decision maker with the best alternative.

Question 8

Discuss any five benefits which are attained by implementing a computerised model for making decision. *(Final Nov. 2007)*

Answer

A computerized model may incorporate accounting, production, transportation, manufacturing and marketing operations of the company. Such models allow a decision maker to consider a large number of factors in decision-making process which was not possible in manual system. This highlights the needs to reduce skepticism that managers have toward sophisticated computerized decision-making aids. This type of model puts pertinent information into an analytical framework that aids the management decision-making process. Some of the benefits offered by a computerised model are:

(i) Makes a fairly accurate forecast of net income for one year.

(ii) Prepares short-term profit plans and long-range projections.

(iii) Provides preplanning information in budget preparation.

(iv) Calculates variances between budgeted and actual results.

(v) Triggers revised forecasts if not proceeding in accordance with plan.

(vi) Acts as early warning system for monitoring activities and signaling necessary reactive plans.

(vii) Indicates effect on income and cash flow by following alternative investment strategies.

(viii) Assists in planning the addition of new facilities and a host of special studies.

(ix) Accomplishes all the preceding item with great speed.

Question 9

Briefly explain the principles to guide the design of measures and indicators to be included in EIS. *(Final Nov. 2007)*

Answer

Various principles to be followed while designing EIS are:

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

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

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

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

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

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

Question 10

Briefly discuss four basic components of Decision Support System. *(Final May. 2008)*

Answer

A decision support system has the following components:

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

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

(iii) A planning language: Two types of planning languages that are commonly used in decision support system are (1) general purpose planning languages and (2) special

purpose planning languages. General purpose planning languages allow users to perform many routine tasks like-retrieving various data from a database or performing statistical analysis. The languages in most electronic spreadsheets are good example of general purpose planning languages. These languages enable the user to tackle a broad range of budgeting, forecasting and other worksheet oriented problems. Special purpose planning languages are more limited. Some statistical languages, such as SAS, SPSS and Minitab are examples of special purpose planning languages.

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

6

ENABLING TECHNOLOGIES

Question 1

Explain the major categories of risks involved in transition from the mainframe computers to client servers? *(Final Nov. 2002 & Nov. 2004)*

Answer

The four categories of risks involved in the transition from mainframe to client server are explained below:

(1) The Technological risk is quite simple. How long will the system work without becoming obsolete? It will become obsolete is inevitable thus the question becomes – how soon will it become obsolete? To resolve this issue, the firm and the IT consultant/division should understand system standards and market trends and use them in their decision-making processes while deciding what system to incorporate into their organisation.

(2) Operational risks: These risks parallel the technological risks in both the short and long run. The questions that arise are - Will you achieve the performance you need from the new technology and will the software that you chose be able to grow or adapt to the changing needs of the business? Only sound planning and keeping an eye to the future are the remedies for these risks.

(3) Economic risks: In the short run, firms are susceptible to hidden costs associated with the initial implementation of the new client/server system. Cost will rise in the short term since one need to maintain the old system (main frame) and the new client server architecture development. In the long run, the concern centres around the support cost of the new system.

(4) Political risks: Political risks involved in this transition are based on short-term and long-term concerns. The short- term concern is-will end users and management be satisfied? The answer is negative if the system is difficult to use or is plagued with problems.

The long run question concerns costs. Unless the mainframe is completely replaced, the total cost of transaction processing goes up. When one division goes off the mainframe, the organization may reduce the local cost of transaction processing for that division but

the cost of processing for other divisions may have increased by remaining on the mainframe, and this creates political problems.

Question 2

What is client/server? Describe the various characteristics that reflect the features of a client/server system. (Final May 2003)

Answer

Client /Server (C/S) refers to computing technologies in which the hardware and software components (i.e. clients and servers) are distributed across a network. The client/server software architecture is a versatile, message - based and modular infrastructure that is intended to improve usability, flexibility, scalability and inter-operatability as compared to centralized, mainframe, time sharing computing. This technology includes both the traditional data base-oriented C/S technology, as well as more recent general distributed computing technologies. The use of LANs has made the client/server model even more attractive to organizations.

Characteristics that reflect the key features of a client / server system are as follows:

(i) Client/Server architecture consists of a client process and a server process that can be distinguished from each other.

(ii) The client portion and the server portions can operate on separate computer platforms.

(iii) Either the client platform or the server platform can be upgraded without having to upgrade the other platform.

(iv) The server is able to service multiple clients concurrently. In some client/ server systems, clients can access multiple servers.

(v) The client / server (c/s) system includes some sort of networking capability.

(vi) A significant portion of the application logic resides at the client end.

(vii) Action is usually initiated at the client end, not at the server end.

(viii) A user friendly graphical user interface generally resides at the client end.

(ix) A structured query language capability is characteristic of the majority of client/server systems.

(x) The database server should provide data protection and security.

Question 3

Describe the various components of Client-Server Architecture. (Final Nov. 2003, May 2006)

Answer

Various components of client server architecture are briefly described below:

(i) Clients: Clients, which are typically PCs, are the "users" of the services offered by the servers. There are three types of clients (a) Non-Graphical User Interface (NGUI) clients, (b) GUI-clients, (c) Object –Oriented User Interface (OOUI) clients.

   (a) Non-GUI clients include ATMs, Cell phones, fax machines and robots that require minimum amount of human interaction.

   (b) GUI-clients are human interaction models usually involving object / action models like the pull-down menus in Windows operating system.

   (c) OOUI clients take GUI clients even further with expanded visual formats, multiple work places, and object interaction rather than application interaction.

   Windows 95 is a common OOUI-client.

(ii) Servers: Servers await requests from the clients and regulate access to shared resources. There are four types of servers:

   (a) *File server*: It shares files across a network by maintaining a shared library of documents, data and images.

   (b) *Database server:* This has processing power to execute Structured Query Language (SQL) requests from clients.

   (c) *Transaction server:* It executes a series of SQL commands, an online transaction processing program (OLTP) as opposed to database servers, which respond to a single client command.

   (d) *Web server:* This allows clients and servers to communicate with a universal language called HTTP.

(iii) Middleware: The network system implemented within the client/server technology is commonly called by the computer industry as middleware. It is the distributed software that is needed to allow clients and servers to interact. The middleware is typically composed of four layers which are service, back-end processing, network operating system and transport stacks. The service layer carries coded instructions and data from software applications to the back-end processing layer for encapsulating network-routing instructions. Next, the network operating system adds additional instructions to ensure that the transport layer transfers data packets to its designated receiver efficiently and correctly.

(iv) Fat-client or Fat-server: Fat client or fat-server are popular terms which serve as vivid description of the type of client/server system in place. In a fat-client system, more of the processing takes place on the client, like with a file server or database server. Fat-servers place more emphasis on the server and try to minimize the processing done by

clients. Examples of fat –server are groupware and web server. Visually fat-clients are referred to as 2-tier system and fat-servers referred to as 3-tier systems.

(v) Network: The network hardware is the cabling, the communication cords and the device that link the server and the clients. The communication and data flow over the network is managed and maintained by network software.

Question 4

What is client-server technology? Enumerate any six of its benefits. *(Final May 2004)*

Answer

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

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

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

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

- The expenses of hardware and network in the client/server environment are less than those in the mainframe environment
- Users are more productive today because they have easy access to data and because applications can be divided among many different users so efficiency is at its highest.
- Client/server applications make organisations more effective by allowing them to port applications simply and efficiently.
- Reduces the cost of the client's computer: The server stores data for the clients rather than clients needing large amounts of disk space. Therefore, the less expensive network computers can be used instead.
- Reduces the cost of purchasing, installing, and upgrading software programs and applications on each client's machine; delivery and maintenance would be from one central point, the server.

Easy to add new hardware to support new systems such as document imaging and video teleconferencing which would not be feasible or cost efficient in a mainframe environment.

Question 5

Define a 2-tier and a 3-tier architecture. *(Final Nov. 2004)*

Answer

2-tier and 3-tier Architecture: 2-tier refers to fat clients and 3-tier refers to fat servers in a client/server architecture. Fat client and fat-server serve as vivid descriptions of the type of client/server systems in place. In a fat-client system, more of the processing takes place on the client, like with a file server or database server. Fat-servers place more emphasis on the server and try to minimise the processing done by the clients. Examples of fat-servers are transaction, groupware, and the web servers.

Question 6

Write short note on client-server model. *(Final May 2005)*

Answer

Client-Server Model - It refers to computing technologies in which the hardware and software components are distributed across a network. Client-server (c/s) technology intelligently divides the processing work between the server and the workstation. The server handles all the global tasks while the workstation handles all the local tasks. The server only sends those records to the workstation that are needed to satisfy the information request. Network traffic is significantly reduced. The result of this system is that it is fast, secure, reliable, efficient, inexpensive and easy-to-use.

Client-server technology model has following characteristics:

(i) The client and server portion can operate on separate platform.

(ii) Client/server platform can be upgraded independently.

(iii) The server is able to serve multiple clients concurrently.

(iv) A significant portion of the application logic resides at the client end.

(v) Action is usually initiated at the client end, not the server end.

(vi) A user-friendly GUI resides at the client end. A structured query language capability is offered by majority of client/server systems.

(vii) The database server provides data protection and security.

Question 7.

Write short note on Server-centric model. *(Final Nov. 2005)*

Answer

Sever centric computing is a model in which applications are deployed, managed, supported and executed 100% on a server. The client handles data entry and information display. It uses a multi-user operating system and a method for distributing the presentation of an application's interface to a client device. With server-based computing, client devices, whether 'fat' or 'thin' have instant access to business critical applications via the server-without application rewrites or download. This means improved efficiency when deploying business-critical applications. In today's environment, this server-based computing model is very useful for growing enterprises because it provides them with the tools and capabilities they need to be successful.

Traditionally used for centralised business applications such as general ledger, payroll etc., this model now includes web-based applications where the user browse through data over the network.

Question 8

Briefly explain the risks associated with client / server model. *(Final May. 2008)*

Answer

The four categories of risks associated with client / server model are briefly discussed below:

(i) Technological Risks: The technological risk is quite simple. The first risk is – Will the new system work? But more important is the risk that in the long run the system may become obsolete. To resolve this issue, the firm and the IT consultant / division should understand system standards and market trends and use them in their decision making processes while deciding what system to incorporate into their organization.

(ii) Operational Risk: These risks parallel the technological risks in both the short and long run. Respectively, they are – Will you achieve the performance you need from the new technology and will the software that you chose be able to grow or adapt to the changing needs of the business.

(iii) Economic Risk: In the short run, firms are susceptible to hidden costs associated with the initial implementation of new client / server system. Cost will rise in the short term since one needs to maintain the old system (mainframe) and the new client server architecture development. In the long run, the concern centres around the support costs of the new system.

(iv) Political Risks: Finally, political (people) risks involved in this transition are addressed. Here, the short-term question is – will end users and management be satisfied? The answer to this is definitely not if the system is difficult to use or is plagued with problems.

Question 9

What control techniques can be utilized for increasing security in a client-server model?

(Final Nov 2004, May 2007 & Nov. 2008)

Answer

Client/Server Security:

Client/server technology utilise distributed techniques, thus there is an increased risk of unauthorised access to data and modification. To increase the security; following techniques can be utilised:

- Disabling the floppy disk drives, ports, and use of Diskless workstations to control unauthorized access and thus securing data and applications.
- Unauthorised users can be prevented to override login scripts and access by securing automatic boot or start up batch file.
- Monitoring of the client using detective control technique can help network security and aid later investigations.
- Various network-monitoring devices are used for this purpose. Since this is a detective control technique, the network administrator must continuously monitor the activities and maintain the devices, otherwise these tools become useless.
- Data encryption techniques can be used to protect data from unauthorized access.
- Authentication systems can be provided for a client so that they can enter into system only by entering login name and password.
- Use of smart cards i.e. intelligent hand held devices and encryption techniques can be used to decipher random codes provided by client-server based operating systems. A smart card displays a temporary password based on an algorithm and must be re-entered by the user during the login session for access onto the client – server system.
- Applications controls may be used and users should be limited to access only those functions in the system those are required to perform their duties.

NOTE

7

SYSTEM DEVELOPMENT PROCESS

Question 1

State and explain any five approaches to System Development. *(Final May 1996)*

Answer

Organisations 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 organisation. 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 organisations 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 organisational goals, objectives and strategies. Using the top-down approach, we begin by analysing organisational objectives and goals and end by specifying application programs and modules that need to be developed to support those goals. The various stages in top down approach are as follows:

(a) Analyse the objectives and goals of the organisation 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 organisation (for example, marketing, production, research and development) and explain how they support the entire organisation.

(c) Based on the functions identified above, ascertain the major activities, decisions and functions of the managers at various levels of hierarchy.

(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 organisation. As we come closer to the strategic planning level, we need to integrate more and more data and information processing activities.

Question 2

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

(Final Nov. 1996, May 1999 & May 2008)

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. *(Final May 2006)*

Answer

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

The following areas may be studied in depth:

1. Review historical aspects: A brief history of the organisation 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 organisation 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. Analyse inputs: A detailed analysis of present inputs is important since they are basic to the manipulation of data. Source documents are used to capture the originating data for

any type of system. The system analyst should be aware of the various sources from where the data can be initially captured, keeping in view the fact that outputs for one area may serve as an input for another area. The system analyst must understand the nature of each form, what is contained in it, who prepared it, from where the form is initiated, where it is completed, the distribution of the form and other similar considerations. 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 on–line and off –line files which are maintained in the organization as these will reveal information about data that are not contained in any output. The related cost of retrieving and processing the data is another important factor that should be considered by the systems analyst.
4. Review methods, procedures and data communications: Methods and procedures transform input data into useful output. A method is defined as a way of doing something; a procedure is a series of logical steps by which a job is accomplished. A procedure's review is an intensive survey of the methods by which each job is accomplished, the equipment utilized and the actual location of the operations. Its basic objective is to eliminate unnecessary tasks or to perceive improvement in opportunities in the present information system. 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 carry–over 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 3

What do you understand by "Requirement analysis"? What is the significance of analysing the present system and how is it carried out? Explain briefly. (Final May 2002 & Nov 2007)

Or

What are the facts finding techniques used by a system analyst? (Final Nov. 2005)

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 organisation in depth, and determining the features, which the new system should possess. Various fact-finding techniques and system development tools are used for requirement analysis.

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

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

resources are used to accomplish the activities of input, processing, output, storage and control.

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 analysing 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
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 analysing documents, questionnaires etc.

Question 4

(*a) Explain prototyping approaches to systems development. (Final May 2000)*

(b) What are the advantages of prototyping approaches? (Final May 2000)

Answer

(a) Prototyping approach: The traditional approach sometimes may take years to analyse, design and implement a system. In order to avoid such delays, organisations are increasingly using prototyping techniques to develop smaller systems such as decision support systems, management information systems and expert systems. The goal of prototyping approach is to develop a small or pilot version called a prototype of part or all of a system. A prototype is 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 scraped. 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.

(b) 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.

Question 5

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? *(Final Nov. 2002)*

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 6

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

(Final May 2003)

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 analyse the flow of dialogue between computers and people. They document the flows among different display screens generated by alternative end user responses to menus and prompts.

(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 7

Bring out the reasons as to why the organizations fail to achieve their Systems Development Objectives? *(Final Nov. 2003)*

Answer

Following are some of the reasons due to which the organisations 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.

(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 8

Write short notes on the following:

(a) Data Dictionary *(Final Nov. 2002 & May 2005)*

(b) System Development Life Cycle *(Final May 1998, May 2004, Nov. 2004 & Nov 2007)*

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 realise 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.

(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.

Question 9

Describe any five functional areas of a system which needs to be analysed by system analyst for detailed investigation of the present system. *(Final May 2005)*

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) Analyse 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 organisation 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) Analyse Outputs - The outputs or reports should be scrutinized carefully by the system analyst in order to determine how well they will meet the organisation'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 10

What are the various tangible and intangible benefits that can result from the development of a computerised system? *(Final Nov. 2005)*

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 11

Write short note on top down approach of system development. *(Final May 2006)*

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 organisational goals, objectives and strategies. The logic here is that, above all, an information system needs to be responsive to and supportive of an organisation's basic reasons for being. Hence the organisation's goals should be the driving force behind development of all the computer systems. Thus, using top down approach, we begin analysing objectives and goals of the organisation and end by specifying application programs and modules that are needed to be developed.

Various steps in top-down approach are as follows:

(a) Analyse the objectives and goals of the organisation in terms of profit, growth, diversification etc.

(b) Identify the functions of the organisation and explain how they support the entire organisation.

(c) Ascertain major activities, decisions and functions at various levels of hierarchy. It should be analysed 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 12

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. *(Final Nov. 2006)*

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.

(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 mange 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 13

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

(Final May 2007 & May 2008)

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 have inserted 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 14

What is prototyping approaches to systems development? Describe its advantages and disadvantages also. *(Final Nov. 2002, May 2004 & May 2007)*

Answer

Prototyping approaches: Prototyping technique is used to develop smaller systems such as decision support systems, management information systems and expert systems. The goal of prototyping approach is to develop a small or pilot version called a prototype of part or all of a system. A prototype is a usable system or system component that is built quickly and at a lesser cost, and with the intention of being modifying or replacing it by a full scale and fully operational system. 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 develop the real system.

Prototyping can be viewed as a series of four steps:

Step 1: Identify Information System Requirements: In traditional approach, the system requirements have to be identified before the development process start. However, under prototype, the process of determining them can be less formal and time-consuming than when performing traditional systems analysis.

Step 2: Develop the Initial Prototype: In this step, the designers create an initial base model-for example, using fourth-general programming languages or CASE tools. The main goal of this stage is 'rapid development' and 'low cost'.

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

Step 4: Obtain User Signoff of the Approved Prototype: At the end of Step 3, users formally approve the final version of the prototype, which commits them to the current design and establishes a contractual obligation about what the system will, and will not do or provide.

Advantages of Prototyping

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

Disadvantages of Prototyping

1. Prototyping can only be successful if the system users are willing to devote significant time in experimenting with the prototype and provide the system developers with change suggestions.
2. The interactive process of prototyping causes the prototype to be experimented with quite extensively. Because of this, the system developers are frequently tempted to minimize the testing and documentation process of the ultimately approved information system. Inadequate testing can make the approved system error-prone, and inadequate documentation make this system difficult to maintain.
3. Prototyping may cause behavioral problems with system users. These problems include dissatisfaction by users if system developers are unable to meet all user demands for improvements as well as dissatisfaction and impatience by user when they have to go through too many interactions of the prototype.

Question 15

Write short notes on the following:

(a) End user development approach in system development *(Final Nov 2007)*

(b) Program documentation *(Final May 2008)*

Answer

(a) End User development approach: With the increasing availability of low-cost technology, end user development is becoming popular. Here it is the end user and not the computer professional who is responsible for systems development activities. The number and nature of systems development activities followed by the end user often differ from those found in formal approaches. There are some risks involved. Enforcing standards and policies is unlikely to be carried out to the same degree as in other approaches. The end-user will not have the experience of an analyst in completing an accurate specification of system requirements. Hence, there would be a reduction in the quality assurance and stability of the system. As departments would choose their own software and hardware, an increase in unrelated and incompatible systems would result. Also difficulties in accessing could arise for users trying to access a central system.

(b) Program documentation: The writing of narrative procedures and instructions for people who will use software is done throughout the program life cycle. User documentation should also be reviewed for understandability. Program design and a set of technical design specifications must include the following:

   1. A brief narrative description of what the program should do.
   2. A description of the outputs, inputs and processing to be performed by the program.
   3. A deadline for finishing the program.
   4. The identity of the programming language to use and the coding standards to follow.
   5. A description of the system environment into which the program should fit.

6. A description of the testing required to certify the program for use.
7. A description of documentation that must be generated for users, maintenance programmers and operational personnel.

Question 16

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. *(Final Nov. 2008)*

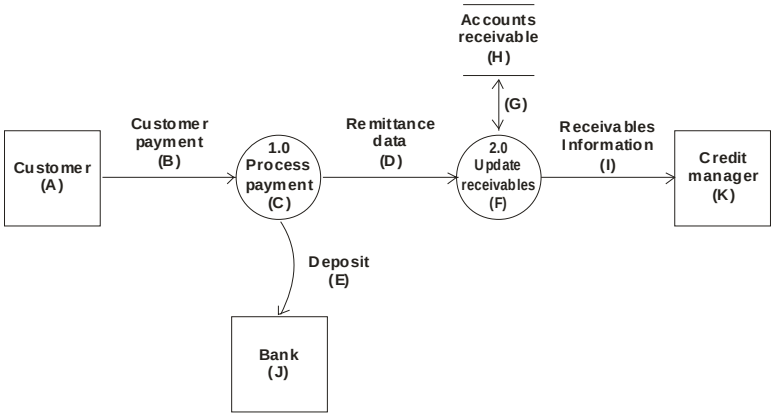
Answer

System development tools are used to help end users and systems analysts to improve current information systems and to develop new ones. Their main purposes are

- To conceptualize, clarify, document and communicate the activities and resources involved in the organisation and its information systems.
- To analyze present business operations, management decision making and information processing activities of the organisation.
- To propose and design new or improved information systems to solve business problems or pursue business opportunities that have been identified.

The major tools used for system development can be divided under four categories based on the systems features documentation as discussed below:

1. System Components and Flows: These tools help the system analysts to document the data flow among the major resources and activities of an information system. They show the flow of data as they are processed by the hardware devices and manual activities. A Data Flow Diagram (DFD) uses a few simple symbols to illustrate the flow of data among entities (such as people or organisations etc.), processing activities and data storage elements. A system component matrix provides a matrix framework to document the resources used, the activities performed and the information produced by the information system. A DFD is drawn below:

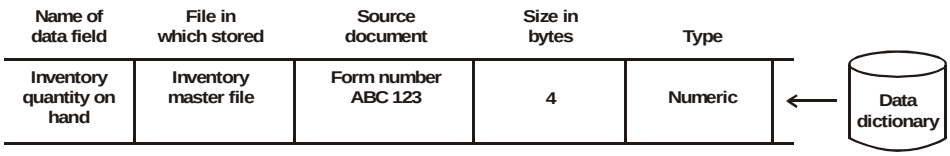


2. User Interface: A friendly interface between end users and the computer system is a major consideration. Layout forms and screens are used to construct the formats and contents of input/output media and methods. Data flow diagrams analyze the flow of dialogue through an Information system. They document the flows among different display screens generated by alternative end user responses to menus and prompts.

   Figure below illustrates a layout screen for the design of a customer order form.

CUSTOMER ORDER FORM				
DATE MM/DD/YY				
ORDER NUMBER	9999			
CUSTOMER NAME	XXXXXXXXXXXXXXXXXXXXXXX			
CATALOG NUMBER	AVAILABLE	LOCATION	COST	DELMODE
XXXXXXXXXXXXX	X	XXXXXXX	999.99	XXXX
XXXXXXXXXXXXX	X	XXXXXXX	999.99	XXXX

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



4. Detailed system process: These tools are used to help the programmer to develop detailed procedures and processes required in the design of a computer program. Decision trees and decision tables are drawn in a network or tabular form to document the complex conditional logic involved to select from alternatives. Structure charts document the purpose, structure and hierarchical relationships of the modules in a program. A decision table is represented below:

	Granting Credit Facility	R1	R2	R3	
Part 1C1	Credit limit Okay	Y	N	N	Part 3
C2	Pay experience Favourable	-	Y	N	
Part 2A1	Allow Credit Facility		X	X	
A2	Reject Order			X	Part 4

NOTE

8
SYSTEMS DESIGN

Question 1

Discuss with examples, the commonly used coding schemes for data processing.

(Final May 1997, Nov 2006)

Answer

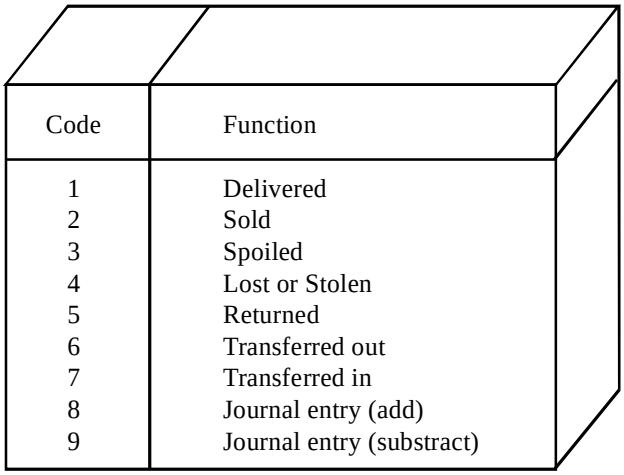
The commonly used coding schemes for data processing are briefly discussed below:

1. Classification codes : Classification codes place separate entities, such as events, people, or objects into distinct groups called classes. A code is used to distinguish one class from another. The code is recorded on the source document by the user. In an online system, it can be keyed directly into the system through a terminal. The user classifies the event into one of the several possible categories and records the code.

   For example, on a toll bridge, the number of each type of vehicles travelling on the bridge is counted to monitor its use. Toll charges are based on the type of vehicle. Since many types of vehicles travel the bridge, using common attributes of size, weight and the state to which it belongs would make its description difficult. Therefore, classification codes are established to group the vehicles in various classes. For example, a passenger car travelling the bridge is categorized as class 1 vehicle and charged the lowest rate. However, a passenger car towing a two wheeler trailer-is coded as class 2 and the one towing a four wheeler trailer is classified as class 3.

   Classification codes vastly simplify the input process because only a single digit code is required. The need for writing lengthy descriptions or making judgements is eliminated and hence the process is made simpler.

2. Function codes: Function codes state the activities or work to be performed without spelling out all of the details in narrative statements. Analysts use this type of code frequently. The figure below shows a list of function codes for updating inventory. Data required for input vary depending on what function is needed. For example, appending or updating a record in a transaction processing system would require only the identification key of the record and the function code. On the other hand, adding a new record would require all data elements to be input, including the function code.



Code	Function
1	Delivered
2	Sold
3	Spoiled
4	Lost or Stolen
5	Returned
6	Transferred out
7	Transferred in
8	Journal entry (add)
9	Journal entry (substract)

Function codes compactly capture functions that the computer must perform

3. Significant-digit subset codes : A well-conceived coding scheme, using significant-digit subset codes, can provide a wealth of information to users and management. Suppose item numbers are to be assigned to the different materials and products that a firm stocks or sells. One way to accomplish this is to assign numbers in sequence, starting with the first and going through to the last. Or a prefix can be added to the identification numbers to further describe the type of item: steel has an S-prefix, plastic a P, and so on.

   Codes can be divided into subsets or subcodes, characters that are part of the identification number and that have special meaning. The subcodes give the user additional information about the item. In the inventory example, the most important information is the class of product, the item within that class, and the supplier. Therefore, the analyst develops an identification number carrying this information through significant digits in several subsets of the overall item.

123	456	78
Product Class	Item number	Vendor number

   If management wants to know how sales are in the waterwheel line, #323, the data can be sorted on that subset and a report produced. Similarly, if information is wanted about all products supplied by vendor 28, a quick examination of this subset of products will provide the information.

   Using digits in an identification number to convey additional information does not add to the length of the data or, to processing time. However, the extra information sub codes provide can be invaluable to management.

4. Mnemonic codes: These are suitable where the codes have to be remembered by people e.g., BL. may stand for bolts. Universities frequently use mnemonics to code

information: MBA for Master of Business Administrator or CS for computer science, mnemonic coding is particularly suited to tool stores since tools can be divided into four categories and each category may be assigned a mnemonic code e.g.

DR for drills

SW for saw blades

GR for grinding wheels etc.

The prefix (e.g. DR) may he followed by size e.g., 0.2 meaning 2 centimeter drill.

Question 2

Explain in detail, the guidelines that should be observed for "form design".

(Final May 1999 & May 2006)

Answer

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

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

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

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

   Ideally, these sections should appear on a page grouped as they are shown in the figure given below. Notice that the seven sections cover basic information required on most forms. The top quarter of the form is devoted to three sections: the heading, the identification and access section and the instruction section. The heading section includes the name and address of the business originating the form. The identification and access section includes codes that may be used to fill the report and gain access to it at a later date. The middle of the form is its body, which composes approximately half of the form. This is the part of the form that requires the most details and development from the person completing it. The bottom quarter of the form is composed of three sections: signature and verification, totals and comments.

   (c) *Captioning:* Clear captioning is yet another technique that can make the work of filing up the form easy. Captions tell the persons completing the forms what to put

on a blank line, space or box.

HEADING		IDENTIFICATION AND ACCESS
INSTRUCTIONS		
BODY		
SIGNATURE AND VERIFICATION		TOTALS
COMMENTS		

2. Meeting the intended purpose: Forms are created to serve one or more purposes in the recording, processing, storing and retrieving of information for various businesses. Sometimes, it is desirable to provide different information to different departments or users while still sharing some basic information. This is where specialty forms are useful. The analyst can use his imagination to design such forms which can provide the information required by different departments while avoiding duplication of information.
3. Ensuring accurate completion: Error rates typically associated with collecting data can drop sharply when forms are designed to assure accurate completion. Design is important in making people to do the right thing with the form. Various controls can be embedded in the form design. For example, the form design can provide an internal double check with column totals and row totals, summing to the same number. If the row and column totals do not sum to the same number, the employee filling out the form knows that there is a problem and can correct it on the spot.
4. Keeping forms attractive: An aesthetic form draws people into it and encourages proper completion. This means that people who fill out the forms will be more satisfied and that the forms will be completed. Thus, forms should look uncluttered, organised and logical even after they are filled in. Providing enough space for typewriter or for underlining responses will help in this regard. To be attractive, forms should elicit information in the expected order: convention dictates asking for name, address, city, state and pin–code in this order. Proper lay–out and flow contribute to a form's attractiveness. Using different fonts for type within the same form can help in making it attractive for the user. Separate categories and sub–categories with thick and thin lines can also encourage interest in the form. Type fonts and lines weights are useful design elements for capturing attention and forcing people to fill in the form correctly.

Question 3

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

(Final Nov. 2002, May 2006 & May 2008)

Answer

Various issues that should be considered while designing systems input are briefly discussed below:

Input design consists of developing specifications and procedures for data preparation, developing steps which are necessary to put transactions data into a usable form for processing, and data-entry, i.e., the activity of putting the data into the computer for processing.

A starting point for the input design process is a review of the information compiled during the requirement analysis phase. The analyst must review facts related to the current system such as what data are entered, who enters them, where they are entered, and when they are entered. This review highlights basic problems and difficulties with the present system. An understanding of the present system's input directs attention to those areas needing improvement for more efficient data entry.

Important factors to be considered in the input design:

(i) Content: The analyst is required to consider the types of data that are needed to be gathered to generate the desired user outputs. This can be quite complicated because new systems often mean new information and new information often requires new sources of data. Sometimes, the data needed for a new system are not available within the organization. Hence, the system designer has to prepare new documents for collecting such information.

(ii) Timeliness: In data processing, it is very important that data is inputted to computer in time because outputs cannot be produced until certain inputs are available. Hence, a plan must be established regarding when different types of inputs will enter the system. In transaction data processing, the people needing output are not the same who input most of the data. Hence, timeliness of input becomes more relevant for such systems.

(iii) Media: Another important input consideration includes the choice of input media and subsequently the devices on which to enter the data. Various user input alternatives available in the market include display work stations, magnetic tapes, magnetic disks, key-boards, optical character recognition, pen-based computers and voice input etc. A suitable medium may be selected depending on the application to be computerized.

(iv) Format: After the data contents and media requirements are determined, input formats are considered. While specifying the record formats, for instance, the type and length of each data field as well as any other special characteristics (number decimal places etc.) must be defined. However, designing input formats in mainframe and mini-computer database environments often requires the assistance of a professional programmer or database administrator.

(v) Input volume: Input volume refers to the amount of data that has to be entered in the computer system at any one time. In some decision-support systems and many real-time transaction processing systems, input volume is light. In batch-oriented transaction processing systems, input volume could be heavy which involves thousands of records that are handled by a centralized data entry department using key-to-tape or key-to-disk systems.

Question 4

What are the six important factors which should be considered while designing the user outputs? (Final May 2001 & May 2004)

Answer

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

(i) Content : Content refers to the actual pieces of data included among the outputs provided to users. For example, the contents of a weekly report to a sales manager might consist of sales person's name, sales calls made by each sales person during the week, and the amount of each product sold by each salesperson to each major client category. It is to be noted here that systems designers generally put too much content into managerial reports instead of too little. Too much content can cause managers to waste time in isolating the information that they need; it also diminishes the impact of truly important information. Hence, only the required information should be included in various outputs.

(ii) Form : Form refers to the way that content is presented to users. Content can be presented in various forms; quantitative, non-quantitative, text, graphics, video and audio. For example, information on distribution channels may be more understandable to the concerned manager if it is presented in the form of a map, with dots representing individual outlets for stores. Various department managers often prefer both summary and detailed information to be presented in relative terms or in chart form such as a pie chart, line chart or bar chart rather than information in absolute terms. Sometimes, converting absolute values to relative values such as percentages often help managers to comprehend the data easily and make better decisions. Hence, the form of the output should be decided keeping in view the requirements for the concerned user.

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

(iv) Timeliness : Timeliness refer to when users need outputs. Some outputs are required on a regular, periodic basis - perhaps daily, weekly, monthly, at the end of a quarter or annually. Other types of outputs are generated on request. A sales manager, for example, may be requiring a weekly sales report. Other users, such as airline agents, require both real- time information and rapid response times in order to render better client service. Hence, the system designer might require that display information be provided to the airline agents within a few seconds at least 95% of the time. Communication-oriented and real-time systems are often the solution for such situations.

(v) Media: Input-output medium refers to the physical device used for input, storage or output. A variety of output media are available in the market these days which include

paper, video display, microfilm, magnetic tape/disk and voice output. Many of these media are available in different forms. The system designer can select a medium, which is best suited to the user requirements.

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

Question 5

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

(Final May 2005)

Answer

A printed output format is nothing but the arrangement of data items. While designing the printed output, the systems analyst builds the mock of actual report or document as planned to appear during actual operation. It should display the location, position of all information such as item details as well as summaries, control breaks with headings, names, addresses, instructions notes and comments etc. To start the designing, one has to determine the data items to be included in the output. The systems analyst can use layout screens, with a CASE Tools to design the report besides the manual process.

There are few guidelines to design the output, which should be followed while preparing the layout form. It will make the job much easier for the analyst, and also ensure that users will receive an understandable report. Some of these guidelines are as stated below:

1. Reports and documents should be so designed that it is to be read from left to right and top to bottom.
2. It should be easiest to find the most important items/highlights of the report.
3. Each page of the report should include the title and heading of the report along with the page no., date of report generation and column headings. The title should be descriptive but yet concise. Each page should be numbered. Date of generation helps the users in determining the utility of the report at the time of reference and makes the complete review process a very effective one. Column headings serve to orient the user to the report contents.
4. Each data item should have a heading, a very short and descriptive. Similar items should be grouped together on the report with the description printed only once at the change or in case it spills over to the next page.
5. Control breaks should be used in the report for better readability. They should be clearly separated from rest of data with additional lines. In order to draw the attention of the user, either the boxes or bold letters or both should be used at control breaks. One can

use special characters also to highlight the control breaks. This makes it easier to find critical information.

6. There should be sufficient margin at left and right as well as at top and bottom for better concentration of the user. It also helps in getting the report bound for permanent records storage without any information being hidden in binding.
7. The detail line for variable data should be defined by indicating whether each space is to be used for an alphabetic, special or numeric character.
8. Finally the mock reports should be thoroughly reviewed by the users and programmers for feasibility, readability, usefulness, understandability as well as aesthetic appeal. This not only helps in generating the quality reports but also saves significant development efforts, which go into re-development of modified reports later.

Question 6

Discuss the desired characteristics of a good coding system. (Final May 2005 & May 2008)

Answer

Characteristics of a Good Coding Scheme

(i) Individuality – The code must identify each object in a set uniquely and with absolute precision. To use one code number for several objects in a set would obviously cause a great deal of confusion. The code should be universally used over the entire organisation.

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

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

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

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

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

Question 7

What is system manual? What information is included in it? (Final Nov. 2003 & May 2007)

Answer

A system manual or job specification manual is an output of the system design that describes the task to be performed by the system with complete layouts and flow charts. It contains:

(i) General description of the existing system: It describes the general structure of the existing system from top management to the bottom management.

(ii) Flow of the existing system: It describes the input, processing and output of the data to be flow at various levels of organisation's structure.

(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 purpose and functions and also major differences from the existing system are stated together with a brief justification for the changes.

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

(vi) Output Layouts: It describes the user interface or layouts for the user that is used for better communication in near future.

(vii) Output distribution: 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 as well as a complete layouts of the input documents, input disks or tapes are described.

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

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

(xi) Files to be maintained: The specifications will contain a listing of the tape, disk or other permanent record files to be maintained, and the items of information to be included in each file.

(xii) List of programs: A list of 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.

Question 8

State the standards that should be followed while designing graphical output. (Final Nov 2007)

Answer

The system analyst must determine the purpose of the graph, the kind of data that need to be analysed, its audience and the effects on the audience of different kinds of graphical outputs.

- Graphic output also contains text, the design of which is an important aspect. Each graphic report should include a title and the date of preparation.
- For a series, page numbers should also be included. Labels can increase the accuracy with which people read data in the graphic form. However, placement of the label affects readability.
- Consistent spacing in all labels and using a common family of type styles maximizes readability.
- All vertical and horizontal axes should be proportional. The use of all capital letters in long words, titles or footnotes impedes readability and should be avoided. Abbreviations should not be used.

9

SYSTEM'S ACQUISITION, SOFTWARE DEVELOPMENT AND TESTING

Question 1

What factors should be considered while selecting a computer system ? (Final May 1996)

Answer

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

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

(ii) Computer performance for commercial work is mainly determiend by the speeds and capabilities of input/output and storage peripherals. Scientific, engineering and operations problems require good computational facilities. Thus, the efficiency of a computer in handling such problems will depend on the main storage available and the instrution execution speed, and repertoire. A comparison along these lines can be made quickly and quite effectively.

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

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

(v) The selection of a computer does not end within the choice of a manufacturer and a model. It continues to the selection of a configuration and a plan for its gradual expansion.

In view of the above observations, following factors may govern the selection of a computer system:

Economic Factors

1. Cost comparisons
2. Return on investment
3. Acquisition methods

Hardware Factors

1. Hardware performance, reliability, capacity and price
2. Presence or absence of modularity
3. Number and accessibility of backup facilities
4. Firmness of delivery date
5. Effective remaining life of proposed hardware
6. Compatibility with existing systems

Software Factors

1. Software performance and price
2. Efficiency and reliability of available software
3. Programming languages available
4. Availability of useful and well-documented packages
5. Ease of use and modification

Service Factors

1. Facilities provided by manufacturer for checking new programs.
2. Training facilities offered and quality of training provided.
3. Programming assistance and conversion assistance offered
4. Maintenance terms and quality

Reputation of manufacturer

1. Financial Stability
2. Record of keeping promises

Question 2

Discuss various testing procedures to be adopted by the programmer in order to make the program error-free. *(Final May 2002)*

Answer

In order to have an error free program, following test procedures must be performed:

1. Desk checking: The first step involves detailed review of the program. Desk checking consists of two parts:
   (i) The review of the general logic of completeness i.e. there are no logical flaws in the design.
   (ii) Dry run, in which some sample data is used and the programmer checks the manner in which the program handles the data, keeping track on paper, of the status of pertinent registers, counters and indicators in the program.

2 Program preparation and compilation: After the coding has been reviewed and desk checked, the program is ready for input, which is keyed in. Thereafter, the compilation phase starts. The compiler will validate the programming instructions from the point of view of syntax of a language used. If no errors are found, it is translated into machine language instructions.

3. Program testing: Once the compilation errors have been removed, the program is ready for testing phase. It is allowed to operate on fabricated test data designed to simulate a number of conditions of input. During this phase, numerous errors may be found due to many reasons. All of these errors must be traced and be removed from their point of occurrence.

4. Production or volume testing: If the program operates on fabricated test data correctly, then the program is put on "live data" testing. This test ensures that provisions have been correctly made for all conditions of input.

5. System testing: After completion of system testing, it can be assumed that the program is in operating condition. The entire system, of which the above program is only a small part, must be subjected to a rigid test. This test will determine if the linkage between programs has been correctly made i.e., whether the output of one program becomes the input of next program, the assumption made in both programs must be valid.

6. Parallel operation: After the system testing, the new system is made to run in parallel with the old system. It means that both the systems must produce output on a daily or regular basis. Both the output generated by new system and the old system should match. It is assumed that old system produces correct output.

Question 3

Explain briefly the stages through which the program has to pass during its development.

(Final May 2005)

Answers

The system developer must instruct the computer how to do everything without error and in the required sequence. Hence, the development of application software has to go through a life cycle having following stages:

(i) Program Analysis: In this stage, for a particular application, the programmer ascertains the inputs available, the output required and to achieve that, what kind of processing is needed. Depending upon the complexity, the programmer then determines whether the proposed application can be or should be programmed at all. It is not unlikely that the proposal is shelved for modification on technical grounds.

(ii) Program Design: Depending upon the main function to be performed, the programmer develops the general organisation of the program. The input, output, file layouts, flowcharts, and program specification etc are provided to the programmer by the analyst.

(iii) Program Coding: The logic of the program expressed in the flowchart is converted into program instructions. While coding, the syntax of the language used is to be kept in mind. The coded instructions are then entered into the magnetic media through available sources such as key to diskette. The program is then compiled through compiler of the language. Several syntax errors may crop up at this stage. These errors are required to be removed after getting the printed listing etc.

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

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

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

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

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

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

Question 4

(i) What is an application software?

(ii) Discuss the factors upon which "Make or Buy" decision of an application software depends. (Final Nov. 1998 & May 2003)

(iii) Before purchasing the packaged software, on what features the software will be assessed? (Final Nov. 1998)

Answer

(i) Application software: Application software is aimed at a solution to a particular problem of the user of a computer system. It has direct interface with the computer system and provides standard processing utilities to solve the specific application problems of the user. For example, number of application software exists in the area of accounting and financial management.

Application software can be sub-divided into two categories viz. general-purpose and application-specific. General-purpose application software are programs that perform common information processing jobs for end users such as word processing programs, spreadsheet programs and database management programs etc. Application specific programs support specific applications of end users e.g. accounting package, inventory control, scientific analysis, computer assisted instruction programs in education etc.

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

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

- *Availability of sophisticated software*: In many instances, the programs available for purchase are more sophisticated than the organization would probably develop. For example, many of the applications programs are fully integrated with other application programs. This integration is a powerful incentive for purchasing rather than developing programs.

(iii) Before purchasing the packaged software, the following features of the software should be assessed:

(a) It is package really available, or is it just another example of vaporware product announced well in advance of the time when it will be actually ready use ?

(b) Is the output produced by the package suitable in form and content to the user ?

(c) Can the package accept the input data that the user needs to process in the form that he needs to use ?

(d) Does the package support an acceptable range of I/O devices ?

(e) Are the files created ad / or processed by the software acceptable in terms of such contents, storage media, record format, access restrictions, ad degree permanency?

(f) Does the package have an adequate response time, or the user must wait for lengthy periods while the program processes the last data entry ?

(g) Is the package "user friendly" – is it easy to learn and use ?

(h) What is the quality of the documentation ? Are the manuals and other documents in the package complete, clearly written and well organized ?

(i) Does the package have good error – handling controls ? Are system error reported to the users in clear messages or cryptic codes ?

(j) What is the warranty period for the package ? What is the level of support one expect to receive from the vendor ?

(k) Does the package represent a good value for money ? Can an attractive, acceptable, package be obtained for a significantly lower outlay ?

Question 5

Describe any five program design tools.

(Final May 1997 May 2004 & Nov. 2007)

Answer

Five program design tools are briefly discussed below:

1. Program flow chart: Program flow chart is among the most common program design tools that managers and users encounter when reviewing the design work of the system development project. These flow charts depict the logical steps through which a computer program must proceed when solving a problem. At one time, program flow

charts were considered the premier program design tool. Although they are still widely used, sometimes it is difficult for programmers to translate a program flow chart directly into a structured code.

A program flow chart depicts the logical processing steps followed by a program quite well. However, unlike some of the other program design tools, they often do not provide a broad view of how the program is organised. However, they are useful for problems involving mathematical or scientific formulae.

2. Pseudo code: When reviewing the work done by a program designer, users may also need to review narrative descriptions of a program logic. Pseudocode, like program flow charts, also represents program logic. However, instead of using graphical symbols and flow lines, pseudo code presents program logic in English - like statements. Pseudocode is generally preferred by programmers over flowcharts because it represents program code more closely. Many users also find pseudo code more understandable than program flow charts.

   Pseudocode is used in a variety of ways. For example many fourth - generation languages use pseudocode - like statements. Besides using pseudocode to design program code in a 3GL, it can be embedded into a completed 3GL program as non-executable 'comment' statements that serve as a documentation to indicate what the program is doing. Pseudocode is particularly useful when designing transaction processing and information- retrieval programs.

3. Structure chart: Another type of program design tool that a user may review is the program structure chart. Structure charts, which look similar to corporate organisation charts, are useful for organising problems. The structure chart organises each of the program tasks into well-defined modules. The higher-level modules represent control portions of the program; the lowest level modules do the actual task of the program. Unlike either flow charts or pseudocode, the structure chart does not give any detail of the actual program logic and the order in which various tasks are executed. Instead they show how all the logical functions of the program fit together as a whole.

4. 4GL Tools: The various tools described above were developed as manually applied methods for designing programs or systems. The main drawback of manually applied tools is that they take a lot of time to prepare. Also, when a program flow chart is prepared or a structure chart is drawn, the programmer is not sure if it is internally consistent. Fourth-generation languages provide a way out to remove these obstacles by automating many of these manual tasks by using 4GL tools. These tools ensure that the work done with them is consistent with the other work performed by the system team. The automation of manual task and internal consistency checks are two reasons due to which productivity gains result from using 4GL tools.

5. Object oriented programming and design tools: These tools provide a means of enhancing programmer productivity and of reducing the application backlogs common in many organisations. Object oriented software design results in a model that describes object, classes and their relationships to one another. The object-oriented design is often

taken from a data flow diagram (DFD). In fact, every input and output screen, every process and data store found in a fully decomposed DFD may be a candidate for an object in an object-oriented design. There is a wide variety of object oriented development tool kits available in the market.

By adopting 4GL and object-oriented programming tools, the organisations can decrease their application development time substantially.

Question 6

List the various sources of acquiring the software. *(Final Nov. 2004)*

Answer

Once the computer hardware is decided, the question of software acquisition becomes important for the management. Some system software is supplied by the manufacturer, which may make a significant difference if it contains a package of special applicability to the job envisaged. Different sources for software acquisition are explained below:

(i) At the time of selection of hardware, it should be identified which manufacturer supplies general/particular software.

It has been observed that all manufacturers supply general software packages for LP, PERT etc. and packages for such commercial applications as inventory control and production planning etc. A few manufacturers also offer packages specially designed for a particular industry such as airline reservation, banking and insurance.

(ii) After deciding user outputs and input designs, the system developer may decide to create the software in-house i.e. a 'make decision'.

(iii) At this stage, the decision may be taken to acquire the software from the vendor. This decision is often called the 'buy decision'. In market, several pre-packaged application software in many business functions, including accounting, general ledger etc. are available. Therefore, they could be directly purchased, and personnels be trained to start the work immediately.

(iv) Computer manufacturers, large and small software houses and computer retail stores are some of the sources from where software packages can be purchased.

(v) There are user groups or association of users of a particular computer system, which are the sources of packaged software. These softwares are developed by one member organisation and made available to other members.

Question 7

Discuss four most compelling advantages of using a pre-written application package

(Final Nov. 1998, May 2003 , Nov. 2004 & Nov 2005)

Answer

Advantages of Pre-written Application Packages: The four most compelling advantages of using pre-written application packages are summarized below:

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

(ii) Low risk: Since the application package is available in the finished form, the 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 specialized application field and hence can provide better software. In contrast, in-house programmers often have to work over a wide range of application areas; they may not be possessing expertise for undertaking proposed software development.

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

Question 8

Write short-notes on the following:

(a) Bench Marking Problem for Vendor's Proposals. *(Final May 2000* & Nov. 2006*)*

(b) System Testing *(Final May 2001 & May 2008)*

(c) Point-Scoring Analysis in Vendor Evaluation. *(Final Nov. 2003)*

Answer

(a) Bench marking problem for vendors' proposals: Benchmarking problems for vendors' proposals are sample programs that represent at least a part of the buyer's primary computer work load. They include software considerations and can be current applications programs or new programs that have been designed to represent planned processing needs i.e. benchmarking problems are oriented towards testing whether a computer offered by the vendor meets the requirements of the job on hand of the buyer. They are required to be representative of the job mix of the buyer. Obviously, benchmarking problems can be applied only if job mix has been clearly specified. The benchmarking problems would then comprise long jobs, short jobs, printing jobs, disk jobs, mathematical problems, input and output loads etc., in proportion typical of the job mix. If the job is truly represented by the selected benchmarking problems, then this

approach can provide a realistic and tangible basis for comparing all vendors' proposals. Tests should enable buyer to effectively evaluate cross performance of various systems in terms of hardware performance (CPU and input/output units), compiler language and operating system capabilities, diagnostic messages, ability to deal with certain types of data structures and effectiveness of software utilities.

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

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

System level testing is a very good time for training employees in the operation of the Information Systems as well as maintaining it.

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

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

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

(c) Point-Scoring Analysis in Vendor Evaluation: It is an approach for evaluating those accounting packages that meet most of a company's major requirements (This analysis can also be used to evaluate hardware as well.) To illustrate, assume that in the process of selecting an accounts payable system, an organisation finds three independent vendors whose packages appear to satisfy current needs. Table 1 shows the results of

the analysis. (Because the cost to purchase or lease each vendor's accounts payable software package is about the same, "cost" is not an issue in this selection process.)

Table-1

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

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

Although point-scoring analyses provide an objective means of selecting a final system, there are no absolute rules in the selection process, only guidelines for matching user needs with software capabilities. Thus, even for a small business, the evaluators must

consider such issues as the company's data processing needs, its in-house computer skills, vendor reputations, software costs, and so forth.

Question 9

What is Vendor evaluation? Define the process for the same. (Final May 2005)

Or

Briefly discuss about various factors which should be considered for evaluating the vendor proposal for supply of computer system. (Final May 2006)

Answer

Once the proposals are received from various vendors for the system, it is the responsibility of the IT Incharge or the committee to select the best product relevant to the requirements/needs of the organization. It is a very tedious and time consuming process and needs a very professional approach in order to safeguard the interests of the organization. The vendors would be offering various types of variations, configurations and options. In order to facilitate the process, following are the factors contributing to evaluation and validation process of vendors' proposals:

(i) Performance Rating of the proposed system in relation to its cost: It is imperative that besides fulfilling the information needs of the organization, the system should also have the capability to process the data within the stipulated time frame as determined by the users. There are quite a few measures of performance such as speed of processing, response time, number of users supported, system configuration etc. One can use the benchmark tests to study the operating efficiency of the system. In this approach, the vendors are provided with the sample data and the task is performed by each vendor. Subsequently representatives of the organization examine the outputs for accuracy, consistency as well as processing efficiency.

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

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

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

hardware and other computing environment like operating system, application software, procedural concerns etc.

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

Other factors worth considering are:

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

Question 10

Write short note on sources of packaged software. *(Final May 2006)*

Answer

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

Question 11

Describe various steps that should be taken for successful installation of the equipment during the implementation phase. *(Final May 2007)*

Answer

Following steps should be taken for successful installation of the equipment:

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

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

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

2. Equipment installation: The equipment must be physically installed by the manufacturer, connected-to the power source and wired to communication lines, if required.

3. Equipment check out: The equipment must be turned on for testing under normal operating conditions. Not only the routine 'diagnostic test' should be run by the vendor, but also the implementation team should devise and run extensive tests of its own to ensure that equipments are in proper working condition.

Question 12

What factors should be considered while selecting a computer system? *(Final Nov 2007)*

Answer

Steps involved in selection of a computer system:

- Prepare the design specifications.
- Prepare and distribute an RFP (Request for proposal) to selected computer vendors.
- On the basis of analysis of proposals, eliminate vendors whose proposals are inferior.
- Have vendors present their proposals.
- Conduct further analysis of the proposals.
- Contact present users of the proposed system.
- Conduct equipment benchmark tests.
- Select the equipment.

Question 13

Discuss in brief salient features of consideration while selecting a computer system. Also suggest contents in a point scoring table for evaluation of a ready to use software.

(Final May 2008)

Answer

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

- Today all computer systems available in the market have good hardware, competent software and roughly similar facilities. Due to rapid advances in computer technology, more recent computers are better in performance and the lower in cost. Hence as far as possible, the latest possible technology should be acquired in general.
- Commercial data processing involves mainly reading-in-data, printing data, storing and retrieving information from media. For commercial work computer performance is affected by the speed and capabilities of input/output and storage peripherals in contrast to scientific, engineering and operations problems which require good computational facilities, hence the efficiency of a computer system in handling such problems will depend on the main storage available. A comparison along these lines may be made.
- The software supplied by the manufacturer may make a significant difference if it contains a package of special applicability to the jobs envisaged. The selection of computer can also be made on software considerations. While all manufacturers supply general software packages for documentation and linear programming etc, a few manufacturers also offer packages specially designed for a particular industry such as Accounting applications in banking and insurance. Obviously, a manufacturer who has a package for users special needs will enjoy a significant advantage.
- Modern computers are marketed as series of compatible, increasingly powerful and interchangeable peripherals. After some period, work expands beyond to fit in the existing computer needing higher capacity machine. Also, in case of breakdown, compatibility allows a wider range of machines to be used as back-up. Thus, the choice

of a computer really becomes the choice of the model within the series, based on the long-range plan of expansion. But dependence on vendor/server is preferable to reprogramming which can be prohibitively expensive or time consuming. The selection of the computer configuration and a plan for its gradual expansion, as a properly considered model can save a great deal of money. The computer systems must be forward and backward compatible.

- Outside assistance in computer selection can be had from computer manufacturers, independent consultants specializing in computers, or management consulting firms. The distinction between vendor selection and machine selection is essentially a matter of business judgment. Once, however, the vendor is selected, he can be counted upon to provide useful guidance for machine also.

Point scoring Table for 'Ready to use' software:-

Software Evaluation Criteria	Possible points	Vendor A	Vendor B	Vendor C
Does the software's meet the mandatory specifications?	10	7	9	6
Will program modifications, if any, be minimal to meet company needs?	10	8	9	7
Does the software contain adequate controls?	10	9	9	8
Is the performance (speed, accuracy, reliability etc.) adequate?	10	7	9	6
Are other users satisfied with the software?	8	6	7	5
Is the software user-friendly?	10	7	8	6
Can the software be demonstrated and test-driven?	9	8	8	7
Does the software have an adequate warranty?	8	6	7	6
Is the software flexible and easily maintained?	8	5	7	6
Is online inquiry of files and records possible?	10	8	9	7
Will the vendor keep the software up to date?	10	8	8	7
Total	123	94	106	85

It may be noted that the data shown above are indicative only.

Question 14

State and briefly explain the various stages of developing an in-house program.

(Final May 2007 & May 2008)

Answer

An In-house development of programs commonly involves the following six stages:

(i) Program Analysis: In this state, the programmer ascertains the input, processing and output required for a particular application. The programmer then determines whether the proposed application can be programmed at all. It is not unlikely that the proposal is shelved for modifications on technical grounds.

(ii) Program design: In this stage the programmer develops the general organization of the program as it relates to the main functions to be performed. Out of several other tools available to him input, output, file layouts and flowcharts are quite useful at this stage. These are provided to the programmer by the systems analyst.

(iii) Program Coding: The logic of the program outlined in the flowchart is converted into program statements or instructions at this stage. For each language, there are specific rules concerning format and syntax. There are special sheets for writing the program instructions in each language. The format of these sheets facilitates writing error-free programs. The programmers broadly pursue three objectives: simplicity, efficient utilization of storage and least processing time. Future changes and development of the programs should be kept in mind.

(iv) Debug the program: The process of debugging a program refers to correcting the language syntax and diagnostic errors so that the program compiles cleanly. A clean compile means that the program can be successfully converted from the source code written by the program into machine language instructions. Debugging consists of four steps:

(a) Inputting the source program to the compiler,

(b) Letting the compiler find errors in the program,

(c) Correcting lines of codes that are in error; and

(d) Resubmitting the corrected source program as input to the compiler.

These are followed by use of structured walkthroughs, testing of the program and review of the program code for adherence to standards.

(v) Program documentation: The writing of narrative procedures and instructions for people who will use software is done throughout the program life cycle. The procedures and instructions should be reviewed and approved by the authorized persons. The documentation should be prepared in such a way that the user can clearly understand the instruction given in Program documentation.

(vi) Program maintenance: The requirements of business data processing applications are subject to continual change. This calls for modification of the various programs. There are usually separate categories of programmers called maintenance programmers who are entrusted with this task.

NOTE

10

SYSTEMS IMPLEMENTATION AND MAINTENANCE

Question 1

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

(May 1998, May 2000, Nov. 2003 & Nov 2007)

Answer

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

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

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

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

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

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

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

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

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

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

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

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

Disadvantages: Many times prototyping is not feasible and hence this conversion method can not be used for such systems. Further, under this approach, special attention must be paid to intefaces 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 2

Discuss briefly, various activities that are involved for successful conversion of an existing manual system to a computerized information system. (Final May 1999 & May 2005)

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

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

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

Question 3

Why is personnel training important for the successful implementation of information system? What type of training should be imparted to (i) systems operator and (ii) users?

(Final May 2003 & Nov. 2006*)*

Answer

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

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

familiarization with run procedures, which involve working through the sequence of activities needed to use a new system on an ongoing basis.

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

Question 4

"The final step of the system implementation is its evaluation." What functions are being served by the system evaluation? Discuss development, operation and information evaluations. *(Final Nov. 2004 & May 2008)*

Answer

Evaluation of the new system: The final step of the system implementation is evaluation. Evaluation provides the feedback necessary to assess the value of information and the performance of personnel and technology included in the newly designed system. This feedback serves two functions:

1. It provides information as to what adjustments to the information system may be necessary.
2. It provides information as to what adjustments should be made in approaching future information system development projects.

There are two basic dimensions of information systems that should be evaluated. The first dimension is concerned with whether the newly developed system is operating properly. The other dimension is concerned with whether the user is satisfied with the information system with regard to the reports supplied by it.

Development evaluation: Evaluation of the development process is primarily concerned with whether the system was developed on schedule and within budget. This is a rather straightforward evaluation. It requires schedules and budgets to be established in advance and that record of actual performance and cost be maintained. It may be noted that very few information systems have been developed on schedule and within budget. In fact, many information systems are developed without clearly defined schedules or budgets. Due to the uncertainty and mystique associated with system development, they are not subjected to traditional management control procedures.

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

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

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

Information evaluation: An information system should also be evaluated in terms of information it provides. This aspect of system evaluation is difficult and it cannot be conducted in a quantitative manner, as is the case with development and operation evaluations. The objective of an information system is to provide information to support the organizational decision system. Therefore, the extent to which information provided by the system is supportive to decision making is the area of concern in evaluating the system. However, it is practically impossible to directly evaluate an information system's support for decision-making in an organisation. It must be measured indirectly. User satisfaction can be used as a measure to evaluate the information provided by an information system. Measurement of user satisfaction can be accomplished using the interview and questionnaire technique. If management is generally satisfied with an information system, it is assumed that the system is meeting the requirements of the organization. If management is not satisfied, modifications ranging from minor adjustments to complete redesign may be required.

Question 5

Write a short note on System maintenance.

(Final May 2001, Nov. 2002, Nov. 2005 & May 2007)

Answer

System maintenance: System maintenance involves adding new data elements, modifying reports, adding new reports, changing calculations etc. to update systems. There are two categories of maintenance –

(i) Scheduled i.e. anticipated and planned maintenance.

(ii) Rescue maintenance for previously undetected malfunctions that were not anticipated but require immediate solution.

As systems increase and expand, systems maintenance places increasing demands on programmers' time. As information systems may remain in an operational and maintenance mode for several years, the system should be evaluated periodically to ensure that it is operating properly, changes may be incorporated to suit the changing needs of the users.

Question 6

Describe various strategies for change over from manual system to computerised system. *(Final May 2006)*

Answer

Strategies for change over from manual system to computerized system : The following strategies are adopted:

(i) *Direct change over:* Conversion by direct changeover means that on a specified date the old system is dropped and the new system is put into use. This can be successful only if extensive testing is done before hand.

It is risky approach and may cause long delays if error occurs. Users may resent being forced into using an unfamiliar system.

(ii) *Parallel conversion:* This refers to running the old system and the new system at the same time, in parallel. 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 stopped.

The advantage includes the possibility of checking new data against old data. It also offers a feeling of security to users who are not forced to make abrupt changes. However, cost of running two systems is high and at the same time workload also increases. With a given choice between two systems, employees will continue to use old system because of their familiarity with it.

(iii) *Gradual conversion:* In this plan, the volume of transactions is gradually increased as the system is phased in. It combines the best features of the earlier two plans. However, it takes too long time to get new system in place.

(iv) *Modular conversion:* This approach uses the building of modular, operational prototypes to change from old system to new in a gradual manner. As each module is modified and accepted, it is put into use. In this manner, each module is tested thoroughly and users also get familiarised. However, special attention is required to be paid to interfaces so that the modules being built actually work as a system.

(v) Distributed system: In this method, one entire conversion is done at one site. When that conversion is successfully completed, other conversions are done for other sites. It is most popular in banking industry or in franchises etc. This approach requires that peculiarities of each site should be handled properly.

Question 7

Define and differentiate between 'Scheduled maintenance' and 'Rescue maintenance' along with their respective benefits. *(Final Nov 2008)*

Answer

Most information systems need some modifications after development. This need arises from time to time, due to failures to anticipate all requirements during system design and/or due to changed organisational needs. The changing needs impact most information systems and thus regular systems maintenance involves adding new data elements, modifying reports, adding new reports, changing calculations etc.

Such maintenance can be categorised in the following two ways:

(1) Scheduled Maintenance is undertaken for tasks which can be anticipated and can be planned for in advance. An information system may remain in an operational and maintenance mode for several years. The system should be evaluated periodically to ensure that it is operating properly and is still workable for the organisation.

(2) Rescue maintenance refers to previously undetected malfunctions or such sudden changes that were not anticipated but require immediate solution. A system that is properly developed and tested should have few occasions of rescue maintenance. Rescue maintenance is unplanned and generally puts system stand still.

11

DESIGN OF COMPUTERISED COMMERCIAL APPLICATIONS

Question 1

Briefly explain Share Accounting System. *(Final May 1996 & May 2007)*

Answer

Share Accounting: Purchase of shares is an investment option used by many persons. A person may purchase shares either from the company (at the time of a public or a rights issue) or from the open share market. A share accounting system needs to maintain an updated list of shareholders. For each shareholder, the main information held is the name and address, names of joint holders (if any), the number of shares held, and the identification of the certificates through which these shares are held.

When a person purchases shares from a share holder, share transfer form along with the certificates is sent by the buyer to the company for incorporating the transfer. The system records a change in ownership for the shares from the seller to the buyer.

Periodically, the company declares a dividend. Dividend warrants (cheques) need to be mailed on a particular day to various shareholders who hold shares. Calculation of income tax to be deducted at source is also done before printing and mailing dividend warrants.

Other facilities usually provided in a share accounting system are:

- bank mandate facility, where the shareholder's dividend warrant is sent to a bank account at the shareholder's request
- splitting of share certificates, where a single certificate containing a large number of shares is replaced with a number of certificates containing a smaller number of shares
- consolidation of shares, where many certificates belonging to a single shareholder are combined into one share certificate
- mailing annual reports and invitations to various meetings

Main inputs in a share accounting system are:

- shareholding data from a fresh issue–this is usually supplied by the issue agency on electronic media
- share transfer request

- split request
- consolidation request
- request for bank mandate
- tax exemption forms
- request for duplicate certificates
- change in share holder's address

Processing involves:

- updating shareholders master file
- recording the transfer of shares
- handling splitting, consolidation and duplicate requests and printing new certificates
- calculation of dividend and income tax to be deducted.

Main outputs are:

- transferred share certificates
- new share certificates in case of consolidation, splitting and duplicates
- dividend warrants and counterfoils
- statement of tax deduction

Question 2

Explain inputs, processes and outputs of any three subsystems of an Accounting Information System. *(Final May 1996)*

Answer

The inputs, processes and outputs of accounts payable, pay-roll accounting system and inventory control system which are sub-systems of an accounting information system are stated below:

(i) Accounts Payable:

Inputs	*Processes*	*Outputs*
Batches of invoices	Verify and edit invoices	Print error list
Purchase orders	Prepare disbursement vouchers	Printer batch totals,
Packing slips	Assemble disbursement vouchers	Edit list
Bills of lading	Derive batch totals	Daily invoice register
Other related	Prepare control total slip	Cheques and remittance

records like receiving report	Prepare disbursement voucher record	statements Accounts payable update disk
	Sort out disbursement voucher records	Cash disbursement register Cash requirements
	Prepare transaction file	statements
	Edit and print runs	Trial balance
	Sort disbursement voucher disk	Accounts payable
	Accounts payable update run	distribution summary
		Vendor analysis report

(ii) Pay roll accounting system:

Inputs	*Processes*	*Outputs*
Master file containing Personnel data like record code, Employer no., Employee name, Address,Phone No., Department, Salary Details, Over time. Leave particulars Payment data Time records for transaction data	Execute payroll edit program Pay roll transaction file sorting Update master file to get current period payroll master Update old labour distribution file Consolidate master payroll file	Payroll register for Payment details - employee-wise with all particulars Labour analysis Journal report Quarterly/ annual reports Department wise totals Other required print outs for Internal accounting purposes

(iii) Inventory control system:

Inputs	*Processes*	*Outputs*
Inventory master file containing	Prepare receipts and issue notes	Inventory transactions

Cash items, location	Assemble in batch	Inventory ledger
of each item	Compute batch totals	Customers' report
Cost of the item, Reorder level	Prepare transaction file using above data	Back order file
Quantity currently on order		Excess stock report
Name and address	Edit run	Under stock report
of vendor and	Sort transaction file	Slow moving items report
Historical data	Update inventory master file	Printout of customer reports
Sales transactions	Print desired reports	ABC classifications
Misc. transactions		Items to be ordered file
for adjustments for		
lost or damaged		
data		
Back order file		

Question 3

For an online real time sales order processing system, draw a system flow chart and explain the following:

(i) Transactions

(ii) Files

(iii) Processing

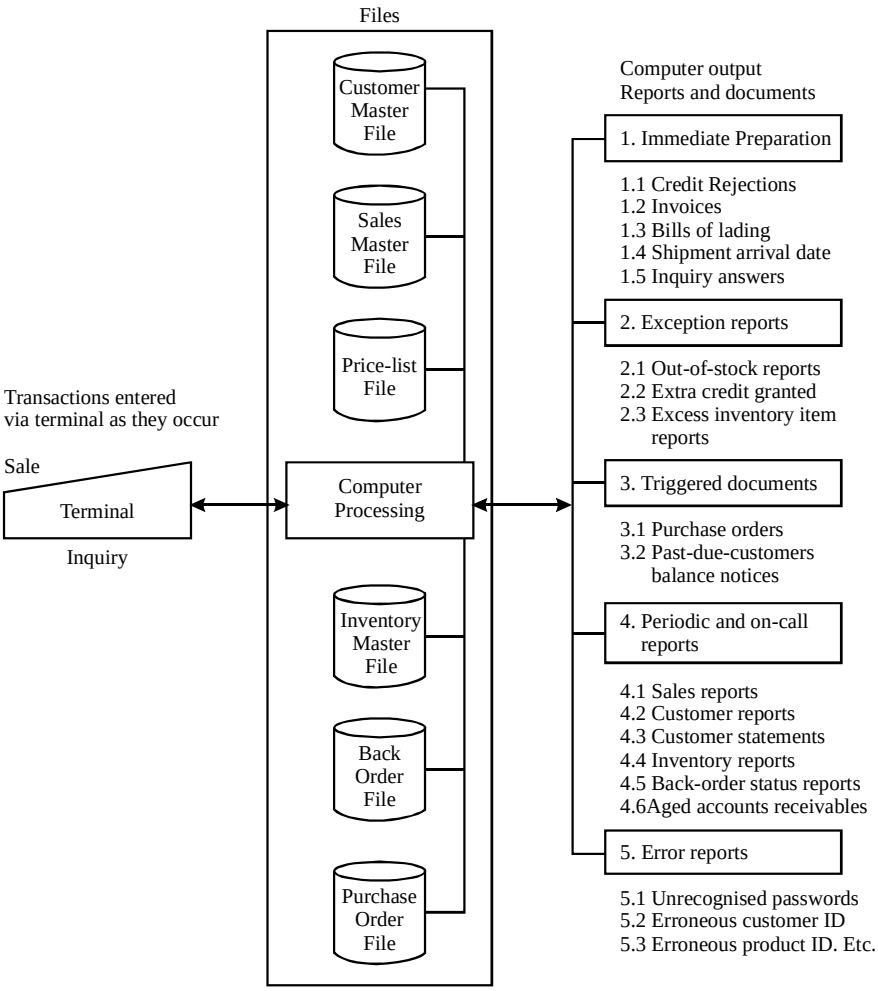
(iv) Output reports and documents *(Final May 2002 & Nov 2004)*

Answer

Online Real-time Sales Order Processing

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

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



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

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

insufficient quantity of a product, either the order is cancelled, or the salesman changes the order to the quantity available and backorders the addition items desired, according to the customer's wishes.

The communication is sent to the customer.

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

5. All necessary reports etc. are then printed.

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

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

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

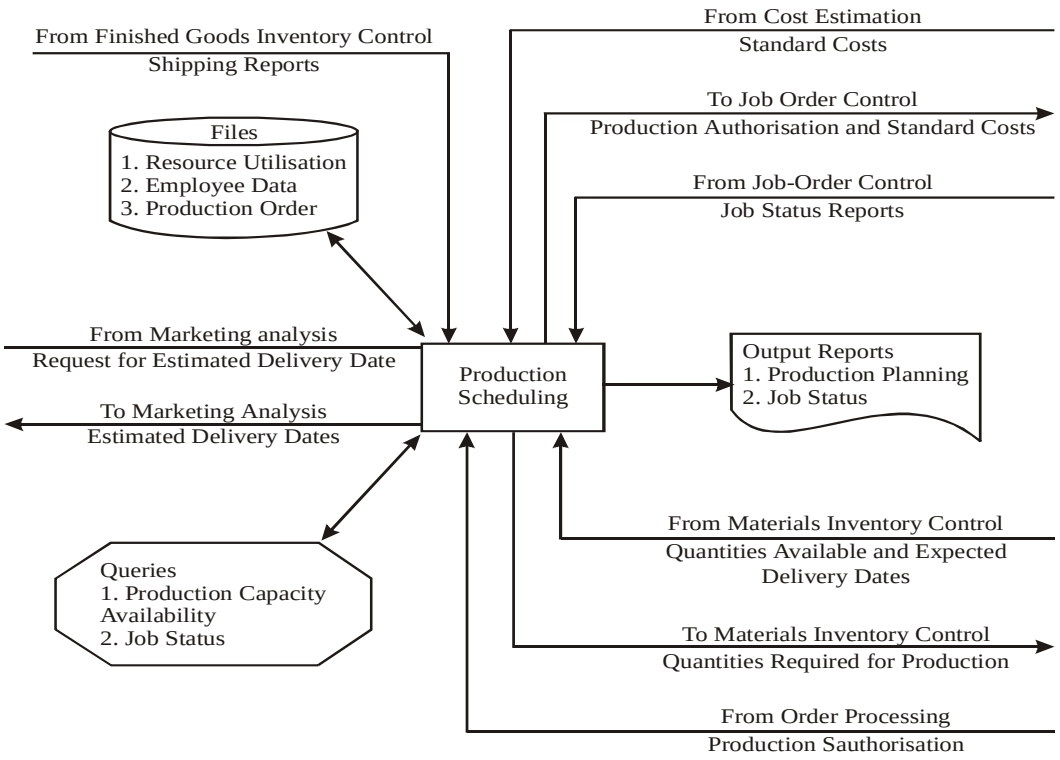
Report: Each of the reports shown in the figure can be produced at any location desired. Typically the credit rejection report, the inquiry answers, and the error reports are displayed or printed at the terminal from where the transaction is entered. Triggered reports occur when an internal condition automates a programmed algorithm. For example, when the quantity of an item on hand drops below a reorder level, a purchase order may be printed.

Question 4

Draw a system flow chart for a Production Scheduling system. (Final Nov. 1998 & Nov. 2002)

Answer

Production scheduling is the nerve centre of the production management system. It schedules production and monitors all physical flows. The figure shows the information flow involving the production scheduling system is given below.



Production Scheduling System

Question 5

What systems interfaces are involved in Production Planning? *(Final Nov. 2002)*

Answer

System Interface in Production Planning: The Production Planning system interacts frequently with other systems of the organization. The sales order processing system authorises production scheduling to start work on a job. Production scheduling then provides with estimated delivery dates and receives shipping reports from the finished goods inventory control system. Thus, all job scheduling information is kept in one system.

Within the production management system, the production scheduling and materials inventory control system interface frequently. Production scheduling informs materials inventory control of the items and quantities required to schedule production and inventory control indicates the quantities available; work-in-process control receives production authorization from the

scheduling system. This authorization creates a new record for a job, and production costs can be charged to the job. The work in process control system receives the standard cost for the job and provides status reports to the scheduling system. Cost estimation provides production scheduling with budgeted standard costs for all job production.

Question 6

Draw a payroll flow chart explaining the processes involved. *(Final May 2003)*

Answer

The flow chart drawn on the next page shows the processing of payroll. Inputs to the system consists of keyed data for time cards, batch control information and the employee master file, updated by the preliminary master payroll file update. Outputs from the system include a completed employee master file, updated by time cards information and the reports and documents discussed below

In run # 1, the payroll edit program is executed. The first function of this program is to detect errors in the input data. If an error is detected, it is immediately printed to permit correction. If accumulated totals computed by the computer program from individual records do not balance control totals contained in the lead record, the difference is also printed. Processing is discontinued at this point so that errors can be corrected. Once this is done, the edit program is rerun to produce an error free input file. The input file produced by the payroll edit program is recorded on magnetic disk or tape.

In run # 2, the payroll transaction file is sorted by the employee number within department number.

In run # 3, the sorted transaction file is used to update the master file on magnetic disk. The type of cost code stored in master file indicates the nature of the account to which employee's gross pay is charged such as direct labour, indirect labour etc.

Gross and net pay are calculated in this run; year-to-date and current period data are accumulated and written on the payroll master file. The data necessary for printing pay slips and pay cheques for the current period are put on a magnetic disk constituting another output of this run. Payroll register is also printed during this run. Payroll register is a printed record of details in the computed employee master file.

In run #4, the current period payroll master disk is used to produce pay cheques and pay slips.

In run #5, the current period payroll disk is sorted by job number.

In run # 6, the output file of run # 5 is used to update the old labour distribution file.

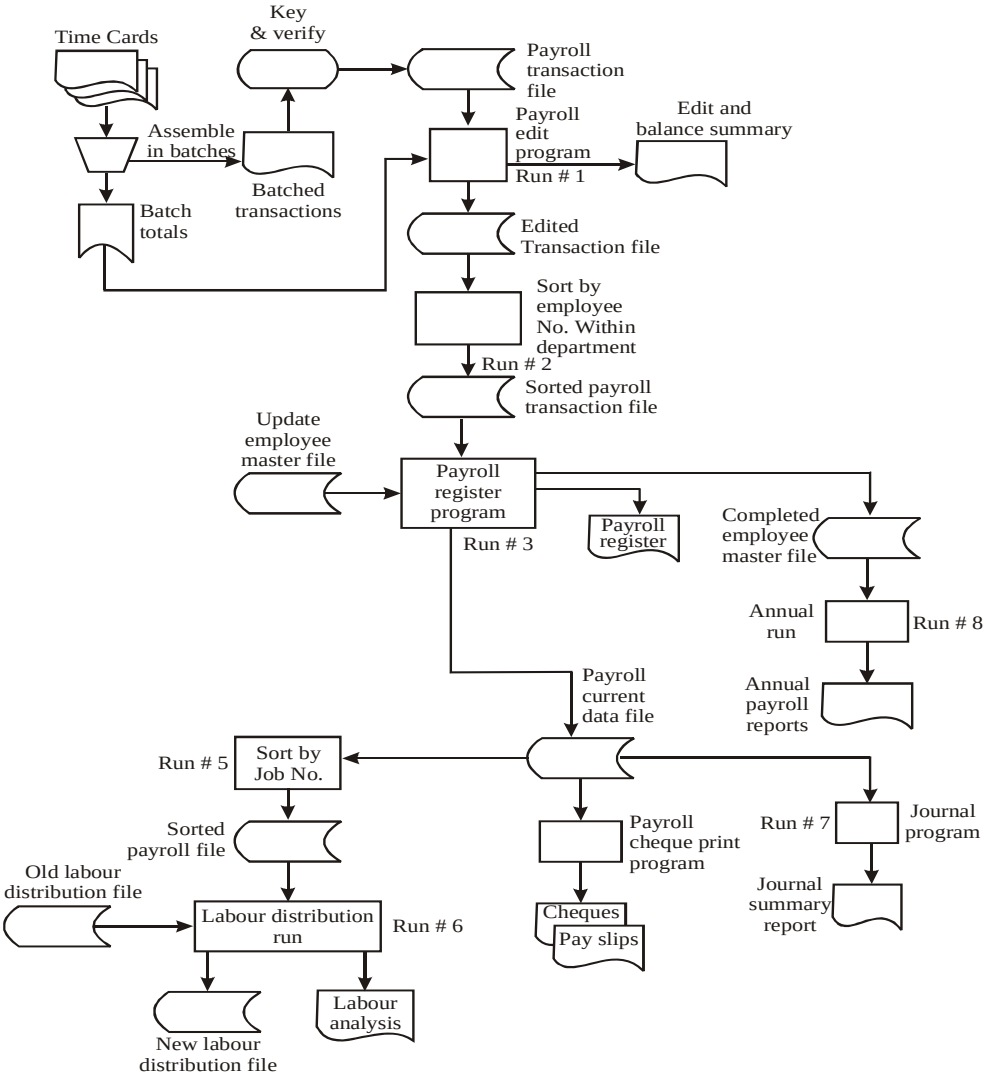
The cumulative values of various trades as *at the end of last month* are updated to as *at the end of this month* by means of the payroll file.

The labour analysis is printed for each job as another output of this run.

In run # 7, a journal report is printed. This report is used to supply current and year –to- date entries to the general ledger, which is the final consolidated accounting document. Journal

reports record total funds expended by source and by disposition. For example, total money amount for overtime and total amount for special advances etc, are summarized by separate account on the general ledger. Similarly, total insurance premium deductions, provident fund deductions, staff welfare fund, income tax deduction etc. make up other accounts.

In run #8, the completed master payroll file is used to print quarterly/ annual reports. Government regulations require quarterly/ annual reports on payroll activities. Such reports include provident fund deduction statement, income-tax deductions, insurance premium deductions etc. Many other reports for internal accounting purposes may also be printed on quarterly/ yearly basis.



Payroll Accounting Flowchart

Question 7

For a material inventory control system, draw the system flowchart and explain the following:

(i) System interfaces

(ii) Files and inputs

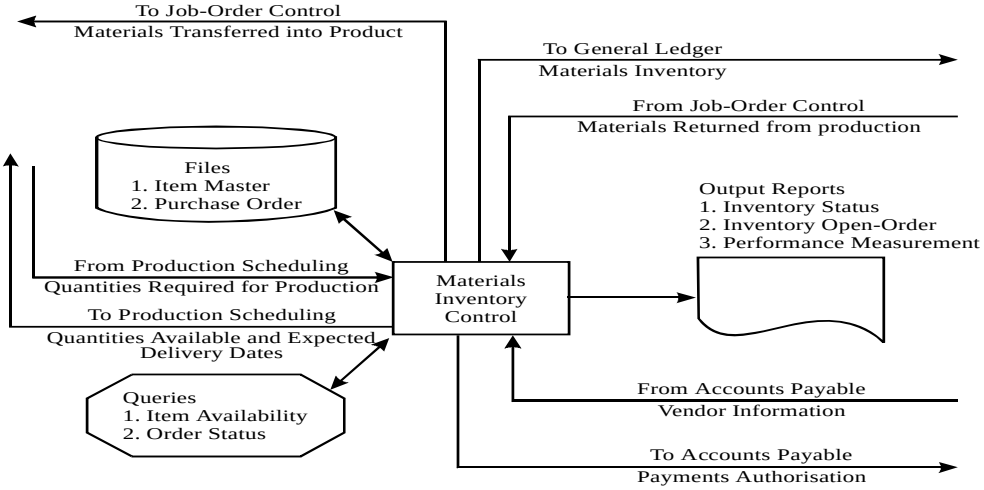
(iii) Reports. (Final Nov. 1996, May 1998, May 2000, May 2001, Nov. 2003 & Nov 2007)

Answer

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

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

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



Material Inventory Control System

The work-in-process control system contains the work-in-process accounts.

Direct and indirect materials are requisitioned from the inventory control system and transferred to work-in-process control. On occasion, materials are returned from the production department to materials inventory control.

Information concerning the quantities of items required for scheduled production is provided to materials inventory control systems from the production scheduling system. This information is used in determining order quantities and timing. Similarly, information about materials returned from the production department is recorded in materials inventory control. It also provides information concerning quantities available and expected delivery dates to the production scheduling system. This information is then used for scheduling production.

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

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

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

(iii) Reports: The materials inventory control system generally produces following reports on periodic basis:

- An inventory status report contains the quantity of each item available on a particular date. The report provides the unit cost of an item and any costing technique such as FIFO, LIFO and average cost etc. can be used. The report also includes the beginning balance, transfers, receipts, adjustments and ending balance of each item.
- An open purchase order report contains information concerning the status of open purchase orders. It includes the item number, vendor identification, date of order, unit cost, quantity ordered, promised shipping date, and other status information.

- Performance measurement reports contain information concerning turnover, stock-outs, shrinkage, investment and other appropriate measurements related to management performance in inventory control.
- The material inventory control system provides the facility of frequently answering the queries. The system is designed to respond instantaneously to these queries so that constant monitoring and control can be exercised on material inventory.

Question 8

What do you understand by ON-LINE, REAL-TIME SYSTEMS ? *(Final Nov. 2004)*

Answer

An on-line real time (OLRT) system processes a transaction as soon as it is entered. Practically, no delays occur during computer processing. The transaction recording and entry system may be created at the point of sale (POS) in the machine-readable form and entered directly into the computer. A system can be fully automated, and even the delay in entering the transaction could be eliminated.

In an OLRT system, all files of the sub-systems related with a particular type of transaction processing must be electronically connected to the computer when a transaction of that type is entered into the machine. Generally, the files of an OLRT system reside on magnetic disks.

The OLRT systems operate (processing) entirely in a different manner compared to BATCH systems. In Batch systems, the transactions for a pre-defined period say a day, a week or a month are collected and then processed in one go. Whereas in OLRT systems, transactions are processed as and when they are created. These days, even the transactions can be created on telephone lines; e-mails, faxes etc. and the processing takes place without losing any time.

OLRT systems are very useful for enquiries. In Bank applications, the customer may be interested to know about the balance of his account, which may be either known through a telephone or directly by a machine, after entering few details.

In an OLRT system, there may be few user-input controls. Extensively programmed edit and logging controls are required to protect the computer files from erroneous or unauthorized transactions. It is also essential for important printed reports, such as control reports, exemption reports, or summaries, to be carefully reviewed by a user department employee who is not responsible for entering transactions.

Question 9

What do you mean by Production scheduling? Draw the information flow diagram for design of computerized production scheduling system. Also explain:

(i) System interface

(ii) File inputs and

(iii) Reports required for the above system. *(Final May 2006)*

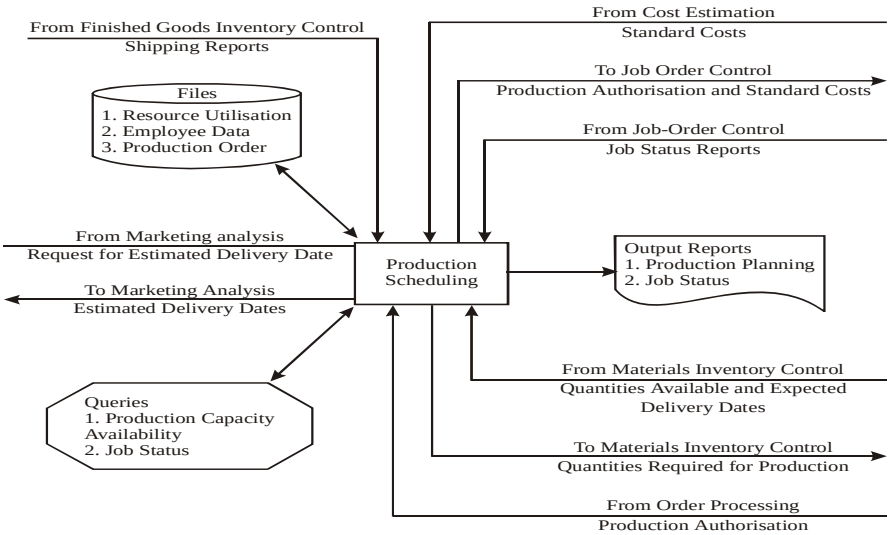
Answer

Production scheduling: It schedules production of components and monitors their progress throughout. It is the nerve centre of the production management system. The information flow involving the production scheduling is given on the next page.

System Interfaces: The production scheduling system interacts with various other systems of the organisation. The sales order processing system authorizes production scheduling to start work on a job. Production scheduling then provides with estimated delivery dates and receives shipping reports from the finished goods inventory control system. Production scheduling informs material inventory control of the items and quantity required to schedule production and inventory control indicates the quantities available. Work in progress (WIP) control receives production authorization from the scheduling system. This authorization creates a new record for a job and production costs can be charged on the job. At the same time, the work-in-process control system receives the standard cost for the job and provides status reports to the scheduling system. Cost estimation provides production scheduling with budgeted standard costs for all jobs production.

Files and Inputs: Three files are required in the production scheduling system. The resource utilization file contains a record for each machine and production process in the factory and maintains work schedules for them. The employee data file contains data concerning employee skills and scheduled work assignments. The production order file maintains completion date and schedule information for each job.

Reports: The scheduling system produces periodic production planning reports. They include the available capacity and scheduled future utilisation of labour and machinery. Job status reports concern the status of jobs in the production process. They compare scheduled and actual completion time in the production process.



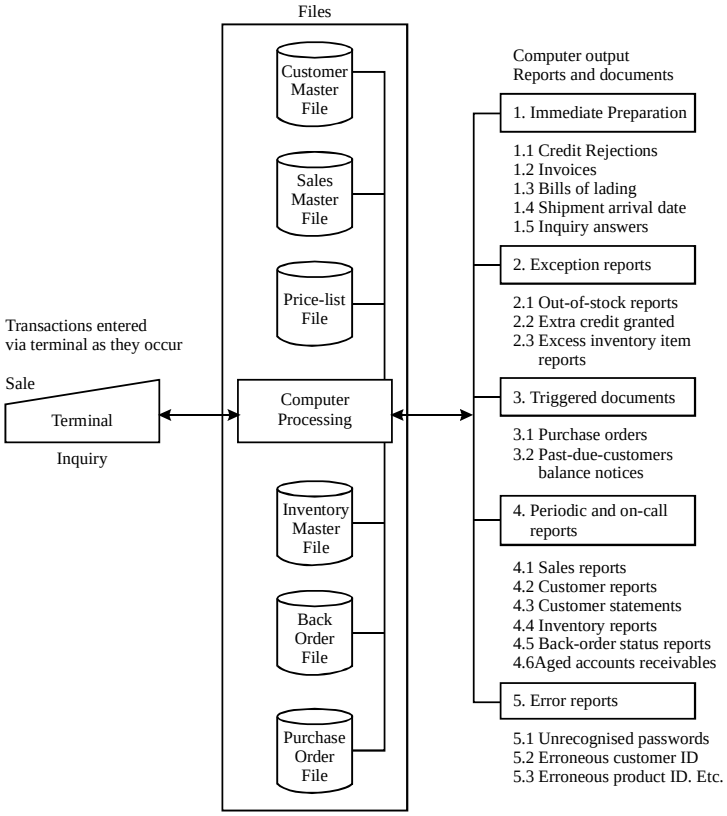
Question 10

Describe the sequence of events which occur immediately for each transaction when controlled by the sales order entry computer programs in an OLRT system.

(Final May 1997 & Nov. 2006)

Answer

Sales order processing system: Controlled by the sales order entry computer programs in an OLRT systems, the following events occur immediately for each transaction in the sequence given below :



1. The sales person tells the computer the nature of the transaction by entering a transaction code identifying it as a credit sales transaction; this activates the sales order processing computer program. The customer number, the item number and quantity are then entered.
2. The computer program checks the customer's account in the customer file to "validate" the customer number (to establish that a credit customer exists with that number) and to see how much additional credit the customer can be granted; the up-to-date credit status of the customer is contained in the customer's account. If

the customer cannot be extended further credit, the salesperson is notified by the computer and the credit transaction is cancelled.

3. The product number of the product ordered is checked for validity in the inventory file, and the stock level of that item shown by the inventory file is compared with the number of items ordered. If there is an insufficient quantity of a product, the program examines the purchasing file to establish when the next shipment is due. The system conveys this information to the terminal of the salesperson and awaits further instructions. The salesperson consults with the customer and then cancels the order for that item or changes the order to the quantity available and back-orders the additional items desired, according to the customer's wishes.
4. The computer program then seeks product pricing and quantity discount information from the price list file and special "preferred customer" discount information, if any, from the customer file. The total cost of the item to the customer including tax is calculated by the computer.
5. The details of the transaction, including the cost details, may appear on a display device at the salesperson's terminal so that they can be told to the customer. Changes may be made in the order by the customer and entered into the computer. The salesperson signals the computer when the customer approves the transaction.
6. An invoice is printed out for mailing, either at the salesperson's terminal or on a printer at a central location.
7. On a printer at the warehouse location of the merchandise, the computer system prepares a multipart-shipping document, which is the authorisation for shipping personnel to select, pack, and ship the merchandise ordered. One copy of the document, known as the "bill of lading" is enclosed and shipped with the merchandise.
8. Product records in the inventory file are adjusted to reflect the decrease in inventory caused by the sale.
9. The customer's account is updated to reflect the details of the transaction, and a new customer balance is calculated and placed in the account.
10. The record for each item in the sales file is updated with details of the transaction. This updating may include all details necessary for sales analysis based on customer type and territory, as well as other factors. A separate transaction listing that records all details of the entire transaction in one transaction file (not shown) may also be made for control and backup purpose.

Question 11

What is work-in-process control system? Describe briefly the system interfaces, files and inputs, and reports involved in this system. *(Final May 2008)*

Answer

The work-in-process control system assigns materials, labour and overhead costs to production jobs or products. In a job order system, each cost is assigned to a specific job. In a process costing system, costs are assigned to departments and then to products. The objectives of a work-in-progress system are to cost jobs through the manufacturing process and provide management with information to assist in controlling cost and measuring the performance of departments or other units within the factory. Therefore, to function properly, the system needs information concerning materials requisitioned for each job, labour employed on each job, overhead costs allocated to each job and the production status of each job. The figure given below depicts the flow of information to and from the job-order control system:

System Interfaces

The work-in-process control system interfaces directly with the payroll, general ledger, finished goods inventory control, production scheduling and materials inventory control systems. Labour cost distribution and factory overhed allocation are inputs from pay-roll and the general ledger systems respectively. Aggregate work-in-process inventory transferred to finished goods is sent from work-in-process control to the general ledger. Once manufacturing is complete, jobs are transferred from work-in-process control to finished goods inventory control.

Authorization to start production along with a bill of materials, specifications, production schedule, and budgeted standard costs are transferred from the production scheduling system. Job status reports are available to this system. Direct and indirect materials are requisitioned from the materials inventory control system.

Files and Inputs

A typical work-in-process system in a manufacturing firm contains a job file that has one record for each job in the manufacturing process. The record contains information regarding job identification number, customer identification, promised completion date, estimated shipping date, promised shipping date, total estimated material cost, total standard labour cost and total standard overhead cost etc.

The job detail file contains in-depth information about each job. When authorization to start a job is received from production scheduling, a record is created for the job. A bill of materials, a machine schedule and a labour schedule are entered into the file.

Reports

The work-in-process control system produces job cost, job status and department performance reports periodically. A job cost report contains a detailed summary of the costs incurred to date, the budgeted cost, and estimated completion dates for each job in this system. Reports are helpful in saving time because we get all the information in summarized form.

Question 12

What is Payroll accounting? Describe in brief the inputs and master file, output and system flow diagram required for it. *(Final Nov. 2008)*

Answer

A payroll system is intended to basically produce pay slips and pay cheques for the employees every month. Preparing a payroll requires collecting employee work hours through their attendance cards, converting hours to gross earnings and computing deductions and net pay. Other activities to be performed as by products of payroll include accumulating summary data for general ledger reports, printing quarterly and year-end reporting statements and making labour distribution job costing or job performance measurements and reporting them. In addition to accounting activities, a payroll system also maintains record of sick leave, earned accruals and usage, and other details of the employees.

Inputs and Master File:

Master file: The payroll computer application uses a combination of current and year-to-date master computer file having records for the current period as well as for yearly reporting. The master file contains permanent as well as current data.

Information such as employee's rate of pay, accumulated earned leave, change in status code etc. are used as inputs to transform gross salary into net pay. Therefore, prior to actual processing of payroll, a preliminary master file update must be completed. The payroll master file may consist of following field:

Personnel Data:

Record code	Employee number	Employee name	Address	Phone number	Sex	Date of birth	Date started employment

Payroll computation Data:

Job number	Department number	Type of cost code	Basic pay	Exempt status (exempt employees do not get extra pay for overtime)	Overtime rate

Leave Data:

Earned leave accumulation rate	Sick leave accumulation rate	Accumulated Earned leave	Accumulated Sick leave	Earned leave used in this year	Sick leave used in this year

Payment data for the payroll:

Current gross pay	Current dearness allowance	Current housing allowance	Special allowance	Current regular hours	Current overtime hours	Current provident fund	Current insurance premium	Current voluntary deductions	Current net pay	YTD gross pay	YTD income tax	YTD provident fund	YTD Insurance Premium	YTD Voluntary deductions	YTD hours

Transaction File:

Employee number	Regular hours	Overtime hours	Earned leave	Sick leave	Special deductions

The permanent portion of the master file must be updated before current transactions are entered into the system. The accounting department also obtains data in new employees and recent changes to existing employees for updation of payroll master file. Inputs to the system consist of keyed data for time cards, batch control information and the employee master file updated by the preliminary master file update.

Outputs: The payroll accounting system produces following Outputs:

- Cheques, pay slips of employees
- Labour analysis – Job No. wise and trade wise
- Payroll Budget Report – Amount v/s Description head (i.e. salary, income tax etc.)
- Payroll Journal summary – quarterly, annual basis.
- The system flow chart is given below:

Refer Question 6 for answer to system flow diagram of payroll accounting

12

ENTERPRISE RESOURCE PLANNING : REDESIGNING BUSINESS

Question 1

What is an ERP system? Bring out the major challenges involved in its implementation.
(Final Nov. 2002 & Nov. 2003)

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.

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 2

Explain the process of evaluation of various ERP packages. (Final May 2003 & May 2006)

Answer

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

(i) Flexibility: It should enable organizations to respond quickly by leveraging changes to their advantage, letting them concentrate on strategically expanding to address new products and markets.

(ii) Comprehensive: It should be applicable across all sizes, functions and industries. It should have in depth features in accounting and controlling, production and materials management, quality management and plant maintenance, sales and distribution, human resources management and plant maintenance, human resources management and project management. It should also have information and early warning systems for each function and enterprise – wide business intelligence system for informed decision making at all levels.

It should be open and modular. It should embrace an architecture that supports components or modules, which can be used individually, expandable in stages to meet the specific requirements of the business including industry specific functionality. It should be technology independent and mesh smoothly with in house / third party applications, solutions and services including the web.

(iii) Integrated: It should overcome the limitations of traditional hierarchical and function oriented structures. Functions like sales and materials planning, production planning, ware house management, financial accounting, and human resources management should be integrated into a work flow of business events and processes across departments and functional areas, enabling knowledge workers to receive the right information and documents at the right time at their desktops across organizational and geographical boundaries.

(iv) Beyond the Company: It should support and enable inter-enterprise business processes with customers, suppliers, banks, government and business partners and create complete logistical chains covering the entire route from supply to delivery, across multiple geographic, currencies and country specific business rules.

(v) Best Business Practices: The software should enable integration of all business operation in an overall system for planning, controlling and monitoring. It should offer a choice of multiple ready-made business processes including best business practices that reflect the experience and requirements of leading companies across industries. It should intrinsically have a rich wealth of business and organizational knowledge base.

(vi) New Technologies: It should incorporate cutting edge and future proof technologies such as object orientation into product development and ensure inter- operability with the Internet and other emerging technologies.

(vii) Other factors to be considered are :

- Global presence of the package
- Local presence
- Market targeted by the package
- Price of the package
- Obsolescence of package
- Ease of implementation of package
- Cost of implementation
- Post –implementation support availability.

Question 3

Write down the general guidelines which are to be followed before starting the implementation of an ERP package. *(Final Nov. 2003)*

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 organisation 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 organisation.

(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.

(vii) Selecting a good implementation methodology with minimum customisation.

(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 4

Write a detailed note on the expectations, fears and the ground realities that a corporate management faces during the post-implementation phase of ERP. (Final Nov. 2004)

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.

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.
- 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 5

Write short notes on the following:

(a) Benefits of Enterprise Resource Planning

(b) Business Process Reengineering (BPR). *(Final Nov. 2004)*

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
- 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 6

What are the characteristics and features of an ERP? (Final May 2005 & May 2008)

Answer

An ERP (Enterprise Resource Planning) system is not only the integration of various functional systems / processes in the organization, but has few more characteristics as stated below to qualify as a full-fledged ERP solution:

(i) Flexibility: An ERP system is flexible enough to respond fast to the changing needs of the organization. The Client Server technology enables ERP to run across various databases at the back-end using Open Data Base Connectivity.

(ii) Modular and Open: ERP system has the open architecture i.e. any modules can be interfaced or detached without affecting the use of rest of the modules. It should support multiple hardware platforms as well as third party add-on solutions.

(iii) Comprehensive: It supports various organizational functions and is suitable for wide range of business organizations.

(iv) Beyond the company: It is not confined to the organizational boundaries rather it is extended to the external business entities connected to the organization with online connectivity.

(v) Best Business Practice: It has inbuilt best business practices applicable worldwide and imposes its own strategies and logics over existing culture and processes of the organization.

Some of the major features of an ERP are:

- It provides multi-platform, multi-facility, multi-mode of manufacturing, multi-currency and multi-lingual facilities.
- It supports strategic and business planning activities, operational planning and execution activities, material and resource planning.
- It has end-to-end Supply Chain Management to optimize the overall demand and supply.

- It facilitates integrated Information Systems covering all functional areas like manufacturing, procurement, sales and distribution, payables, receivables, human resources, inventory and finance etc.
- It enhances customer services through increased efficiency in core activities thus augmenting the corporate image.
- It bridges the information gap across organization.
- ERP is the solution for better project management.
- It allows introduction of latest technologies like Electronic Funds Transfer, Electronic Data Interchange, Internet, Intranet, E-commerce etc.
- It eliminates business problems like material shortages, productivity, customer service, cash management, quality and prompt delivery; and
- It provides intelligent business tools like Decision Support System, Executive Information System, Data Mining etc.

Question 7

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

(Final May 2005)

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 8

Write short notes on Business Engineering. *(Final Nov. 2005)*

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 9

Write short note on Enterprise Controlling. *(Final Nov. 2006)*

Answer

Enterprise Controlling: Enterprise can be managed by using an integrated enterprise management. This consists of getting accounting data prepared by subsidiaries for corporate reporting which will be automatically prepared simultaneously within the local books of each subsidiary. This data is transferred to a module called enterprise controlling (EC).

It is easy to transfer the data to the EC module to automatically set up consolidated financial statements including elimination of inter-company transactions currency translations etc. Enterprise controlling consist of 3 modules. EC-CS component is used for financial statutory and management consolidation. 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. It is also possible to take data directly from EC-PCA to ES-CS consolidation.

EC-EIS (Executive Information System) allows to take financial data from EC-PCA, EC-CS or any other application and combines with any external data such as market data, industry benchmark and / or data from non-SAP applications to build a company specific comprehensive enterprise information system.

EC allows to control the whole enterprise from a corporate and a business unit perspective within one common infrastructure. From EC-EIS top-level2 reports, end users can drill down to more detailed information within EC or any other R/3 application.

Question 10

How will you establish and implement Critical Success Factors (CSFs) and Key Performance Indicators (KPIs) is an organization for achieving the benefits of implementation of ERP?

(Final May. 2007)

Answer

Effective use of ERP is a direct result of steps taken at the time of implementation toward preparing the organization. Change integration has to be necessarily embedded in the task list for any ERP implementation. The main tool for this is the process of communication in all forms-written, oral, workshops, meetings and follow up activities. The process should start quite early by educating all layers of the management on the particular ERP product, its relevant functionality, limitations and benefits.

Also at the start of the project, the Critical Success Factors (CSFs) for the company as whole should be listed. These should be drilled down to CSFs for respective departments like Finance, Marketing, Purchase, Stores, Production, Quality, Maintenance and HRD or Personnel. From these CSFs, performance measures required to address these CSFs should be culled out. The numeric figures against these performance measures can be classified as the Key Performance Indicators (KPIs). The process of firming up the above is usually done through workshops. This has to be completed before the processes to be configured on the ERP are drawn up. The important end users should be involved in evolving the process keeping ERP in mind. The KPIs derived from organisational goals and CSFs should be kept in mind.

The post implementation tasks are:

- Develop the new job descriptions and organization structure to suit the post ERP scenario.
- Determine the skill gap between existing jobs and envisioned jobs.
- Assessing training requirements, and create and implement a training plan.
- Develop and amend HR, financial and operational policies to suit the future ERP environment.
- Develop a plan for workforce logistic adjustment.

Then the major task is to monitor KPIs and take correct business decisions to improve them. Hence, the immediate task is to set attainable goals. Certain KPIs, though existing in the system, are better monitored and controlled after ERP System attains maturity. There will be resistance to change, but the management should be strong to continue implementation.

Question 11

What is Enterprise Resource Planning? Briefly describe its benefits.

(Final Nov. 2005 & Nov 2007)

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.

Enterprise resource planning promises one database, one application, and one user interface for the entire enterprise, where once disparate systems ruled manufacturing, distribution, finance and sales. Taking information from every function, it is a tool that assists employees and managers to plan, monitor and control the entire business.

The following are some of the benefits they achieved by implementing the ERP packages:

- Gives Accounts Payable personnel increased control of invoicing and payment processing and thereby boosting their productivity and eliminating their reliance on computer personnel for these operations.
- Reduces paper documents by providing on-line formats for quickly entering and retrieving information.
- Improves timeliness of information by permitting posting daily instead of monthly.
- Provides greater accuracy of information with detailed content, better presentation, satisfactory for the auditors.
- Improved cost control.
- Faster response and follow-up on customers.
- More efficient cash collection, say, material reduction in delay in payments by customers.
- Better monitoring and quicker resolution of queries.
- Enables quick response to change in business operations and market conditions.
- Helps to achieve competitive advantage by improving its business processes.
- Improves supply-demand linkage with remote locations and branches in different countries.
- Provides a unified customer database usable by all applications.
- Improves International operations by supporting a variety of tax structures, invoicing schemes, multiple currencies, multiple period accounting and languages.
- Improves information access and management throughout the enterprise.
- Provides solution for problems like Y2K and Single Monetary Unit (SMU) or Euro Currency.

Question 12

Discuss the functions and facilities provided by Treasury Cash Management module of an ERP package. *(Final Nov. 2008)*

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.

Management Information and Control Systems

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.

(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.

13

CONTROLS IN EDP SET-UP : GENERAL CONTROLS

Question 1

Explain the various general components of Disaster Recovery Plan.

(Final Nov. 1996, & May 2005)

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 off–site, 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 organisation and the importance of their loss must be evaluated. An indication must be given of the efforts and cost involved in restoring the various application systems.

(iii) An application systems hierarchy must be spelt out.

(iv) Selection of a disaster recovery site must be made. A reciprocal agreement with another organisation having compatible hardware and software could be made.

(v) A formal back agreement with another company must be made. This should cover the periodical exchange of information between the two sites regarding changes to hardware/software, the time and duration of systems availability, modalities of testing the plan etc.

Back–up Plan: Organisations no matter how physically secure, their systems are always vulnerable to the disaster. Therefore, an effective safeguard is to have a backup of anything that could be destroyed, be it hardware or software. As regards hardware, 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 2

What are the two major categories of exposures in the Communication subsystems including Internet and Intranet? What control mechanisms could be used to deal with them?

(Final Nov. 2002)

Answer

There are two major exposures in the communication sub -system including Internet and Intranet.

Data may be lost or corrupted through Component failure.

An intruder may subvert data being transmitted through the sub-system.

(i) Component Failure: The primary components in the communication sub-systems are –

(a) Communication lines viz. twisted pair, coaxial cables, fibre optics, microwave and satellite etc.

(b) Hardware – ports, modems, multiplexers, switches and concentrators etc.

(c) Software – Packet switching software, polling software, data compression software etc.

Due to component failure, transmission between sender and receiver can be disrupted, destroyed or corrupted in the communication system. There may be loss of databases and programs stored on the network server due to equipment failure.

(ii) Subversive threats : An intruder attempts to violate the integrity of some components in the sub-system.

(a) *Invasive tap:* By installing it on communication line, he can read and modify data.

(b) *Inductive tap:* It monitors electromagnetic transmissions and allows the data to be read only.

Subversive attacks can provide intruders with important information about messages being transmitted and the intruder can manipulate these messages in many ways.

Following mechanism can be used to control risks:

(i) Fire wall: Organizations connected to the Internet and Intranet often implement an electronic firewall to insulate their network from outside intruder. A firewall is a system that enforces access control between two networks. To accomplish this:

All traffic between the outside network and the organisation's Intranet must pass through the firewall.

Only authorised traffic between the organisation and the outside is allowed to pass through the firewall.

The firewall must be immune to penetration from both outside and inside the organisation.

In addition to insulating the organisation's network from external networks, firewalls can be used to insulate portions of the organisation's Intranet from internal access also.

(ii) Controlling Denial of Service Attacks: When a user establishes a connection on the Internet through TCP/IP, a three way handshake takes place between SYN packets, ACK packets and ACD packets. Computer hacker transmits hundreds of SYN packets to the receiver but never responds with an ACD to complete the connection. As a result, the ports of the receiver's server are clogged with incomplete communication requests and legitimate transactions are prevented from processing. Organisations under attack have been prevented from receiving Internet messages for days in the past. If target organisation could identify the server that is launching the attack, the firewall could be programmed to ignore all communication from that site.

(iii) Encryption: Encryption is the conversion of data into a secret code for storage in databases and transmission over networks. The sender uses an encryption algorithm and the original message called the clear text is converted into cipher text. This is decoded at the receiving end. The encryption algorithm uses a key which is of 56 to 128 bits in length. The more bits in the key, the stronger is the encryption method. Two general approaches to encryption are use of private key and public key encryption.

(iv) Message Transaction Log: An intruder may penetrate the system by trying different passwords and user ID combinations. All incoming and outgoing message along with attempted access should be recorded in a message transaction log. The log should record the user ID, the time of the access and the terminal location and telephone number from which the request originated.

(v) Call Back Devices: It is based on the principle that the key to network security is to keep the intruder off the LAN rather than imposing security measure after the criminal has connected to the LAN server. The call- back device requires the user to enter a password and then the system breaks the connection. If the caller is authorized, the call

back device dials the caller's number to establish a new connection. This limits access only from authorised terminals or telephone numbers and prevents an intruder masquerading as a legitimate user.

Question 3

What are the different types of securities required for the computer system? Explain briefly the different components of physical security of a computer installation.

(Final Nov. 1996, May 1998 & Nov. 2003)

Answer

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

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

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

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

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

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

(iii) Energy Variation: Voltage regulators and circuit breakers protect the hardware from temporary increase or decrease of power. Battery back-up can be provided in case a temporary loss of power occurs. A generation plant is needed for sustained losses in power.

(iv) Pollution damage: The major pollutant in a computer installation is dust. Dust caught between the surfaces of magnetic tape / disk and the reading and writing heads may cause either permanent damage to data or read/ write errors. Due consideration should be given for dust free environment in the computer room. Regular cleaning of walls, floors and equipment etc. is essential. Only such materials and finishing may be used inside the room which enables it to remain dust free.

(v) Unauthorized intrusion: Unauthorised intrusion takes two forms. First, the intruder by physically entering the room may steal assets or carry out sabotage. Alternatively, the intruder may eavesdrop on the installation by wire tapping, installing an electronic bug or using a receiver that picks up electro-magnetic signals. Physical entry may be prevented by restricting the entry to the computer room by various means. A badge system may be used to identify the status of personnel in the computer room. Eavesdropping breaches the privacy of data. It may be used by an intruder to obtain a password or sensitive information of the organization. Various devices are available to detect the presence of bugs by the intruder.

Question 4

Discuss the activities dealing with system development controls in EDP setup.

(Final May 2004)

Answer

Controlling new system development activities: The six activities discussed below deal with system development controls in EDP setup.

(i) System Authorization Activities : All systems must be properly authorized to ensure their economic justification and feasibility. As with any transaction, system's authorization should be formal. This requires that each new system request be submitted in written form by users to systems professionals who have both the expertise and authority to evaluate and approve (or reject) the request.

(ii) User Specification Activities : Users must be actively involved in the systems

development process. User involvement should not be ignored because of a high degree of technical complexity in the system. Regardless of the technology involved, the user can create a detailed written description of the logical needs that must be satisfied by the system. The creation of a user specification document often involves the joint efforts of the user and systems professionals. However, it is most important that this document remains a statement of user needs. It should describe the user's view of the problem, not that of the systems professionals.

(iii) Technical Design Activities : The technical design activities in the SDLC translate the user specifications into a set of detailed technical specifications of a system that meets the user's needs. The scope of these activities includes systems analysis, general systems design, feasibility analysis, and detailed systems design. The adequacy of these activities is measured by the quality of the documentation that emerges from each phase. Documentation is both a control and evidence of control and is critical to the system's long term success.

(iv) Internal Auditor's Participation : The internal auditor plays an important role in the control of systems development activities, particularly in organisations whose users lack technical expertise. The auditor should become involved at the inception of the SDLC process to make conceptual suggestions regarding system requirements and controls. Auditor's involvement should continue throughout all phases of the development process and into the maintenance phase.

(v) Program Testing : All program modules must be thoroughly tested before they are implemented. The results of the tests are then compared against predetermined results to identify programming and logic errors.

Program testing is time-consuming, the principal task being the creation of meaningful test data. To facilitate the efficient implementation of audit objectives, test data prepared during the implementation phase must be preserved for future use. This will give the auditor a frame of reference for designing and evaluating future audit tests. For example, if a program has undergone no maintenance changes since its implementation, the test results from the audit should be identical to the original test results. Having a basis for comparison, the auditor can thus quickly verify the integrity of the program code. On the other hand, if changes have occurred, the original test data can provide evidence regarding these changes. The auditor can thus focus attention upon those areas.

(vi) User Test and Acceptance Procedures : Just before implementation, the individual modules of the system must be tested as a unified whole. A test team comprising user personnel, systems professionals, and internal audit personnel subjects the system to rigorous testing. Once the test team is satisfied that the system meets its stated requirements, the system is formally accepted by the user department(s).

The formal test and acceptance of the system are considered by many to be the most important control over the SDLC. It is imperative that user acceptance be documented. Before implementation, this is the last point at which the user can determine the system's adequacy and acceptability. Although discovering a major flaw at this juncture is costly, discovering the flaw during the production operations can be devastating.

Question 5

Write short notes on the following:

(a) Security risks associated with Personal Computers (Final Nov. 1998)

(b) Personal Computer Controls (Final May 2003)

(c) Firewalls (Final May 2004, May 2006 & May 2008)

Answer

(a) Security risks associated with Personal Computers:

1. Personal computers are small in size and easy to connect and disconnect, they are likely to be shifted from one location to another or even taken outside the organization for theft, or for theft of information, leaving no trace.
2. Decentralized purchasing of PCs can result in hardware/software incompatibility in the long run. There is also the risk of multiple purchases of same hardware and software.
3. Floppies can be very conveniently transported from one place to another, as a result of which data corruption and theft of information may occur. Even hard disks can be ported easily these days.
4. PC is basically a single user oriented machine and hence, does not provide inherent data safeguards. Problems can be caused by computer viruses and pirated software, namely, data corruption, slow operations and system break down etc.
5. Segregation of duty is not possible, owing to limited number of staff.
6. Due to vast number of installations, the staff mobility is higher and hence becomes a source of leakage of information.
7. The operating staff may not be adequately trained.

(b) Personal Computer Controls: The capabilities, adaptability and user friendliness of personal computers are posing a serious challenge to auditors. PCs have the following special characteristics, which give rise to new risks that need to be controlled.

They are small, fast and powerful, some of them even approach the power of minis and mainframes.

They are available in many makes and models.

Floppies provide a convenient way of data storage.

Their user-friendliness has resulted in end-user computing.

They act as inexpensive front-ends to large computers.

There is a tendency to buy off-the shelf application packages.

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

(i) *Weak access control*: Security software that provides log-on procedures is available for PCs. Most of these programmes, however, become active only when the

computer is booted from the hard drive. Disc locks are devices that prevent unauthorised individuals from accessing the floppy disk drive of a computer.

(ii) *Multi-level password control* : To preserve the integrity of mission-critical data and programmes, organizations need formal back up procedures.

(iii) *Floppy disc backup :* Dual internal hard drives, external hard drives and tape back up devices are also used.

(iv) *Dual internal hard drives* : PC can be configured with two physical internal hard drives. One disk can be used to store production data while the other stores the back-up file.

(v) *External hard drive* with removable disk cartridge can be used. This can provide an effective and simple back-up technique.

(c) Firewalls: Organizations connected to the Internet or other public networks often implement an electronic "firewall" to insulate their Intranet from outside intruders. A firewall is a system that enforces access control between two networks. To accomplish this:

All traffic between the outside network and the orgnaisation's Intranet must pass through the firewall.

Only authorized traffic between the organization and the outside, as specified by formal security policy, is allowed to pass through the firewall.

The firewall must be immune to penetration from both outside and inside the organization.

Firewall can be used to authenticate an outside user of the network, verify his or her level of access authority, and then direct the user to the program, data, or service requested. In addition to insulating the organisation's network from external networks, firewalls can also be used to insulate portions of the organisation's Intranet from internal access. There are a number of firewall products on the market. Firewalls can be grouped into two general types: network-level firewalls, and application-level firewalls.

Network-level firewalls provide low cost and low security access control. This type of firewall consists of screening router that examines the source and destination addresses that are attached to incoming message packets. The firewall accepts or denies access requests based on filtering rules that have been programmed into it.

Application-level firewalls provide a high level of customizable network security, but can be extremely expensive. These systems are configured to run security applications called proxies that permit routine services such as e-mail to pass through the firewall, but can perform sophisticated functions such as logging or user authentication for specific tasks. If an outside user attempts to connect to an unauthorized service or file, the network administrator or security group can be notified immediately.

Question 6

Your client has recently switched over from manual accounting to computerised accounting. When you receive computerized accounts for the first quarter, you find the following types of error:

(i) Incomplete or unauthorized data input

(ii) Errors in the files or database during updating

(iii) Improper distribution or disclosure of output.

You, as an information system auditor, suggest the suitable test of controls for audit of computer processing so that the above-mentioned errors can be prevented. (Final May 2005)

Answer

Test of controls for Audit of Computer Processing: During computer processing, the system might fail to detect erroneous input, improperly correct input errors, process erroneous input into files or databases during updating. Auditors must periodically re-evaluate processing controls to ensure their reliability. The following test of controls may be used:

- Evaluate adequacy of processing control standards and procedures.
- Evaluate adequacy and completeness of data editing controls.
- Verify adherence to processing control procedures by observing computer operations and the data control function.
- Verify that selected application system output is properly distributed.
- Reconcile a sample of batch totals and follow up on discrepancies.
- Trace disposition of a sample of errors flagged by data edit routines to ensure proper handling.
- Verify processing accuracy for a sample of sensitive transactions.
- Verify processing accuracy for a selected computer generated transactions.
- Search for erroneous or unauthorized code via analysis of program logic.
- Check accuracy and completeness of processing controls using test data.
- Monitor online processing using concurrent audit techniques.
- Recreate selected reports to test for accuracy and completeness.

The auditor must periodically re-evaluate processing controls to ensure their continued reliability. If processing controls are unsatisfactory, user and source data controls may be strong enough to compensate.

Question 7

Describe various access control methods used for safety of the database. (Final May 2005)

Access Control Methods: In data base environment, access control risks include corruption, theft, misuse and destruction of data. These originate from both unauthorised intruders and

authorised users who exceed their access privileges. Several data base access control features are discussed below:

(i) User View – The user view or sub-scheme is a subset of the total database that defines the user's data domain and provides access to the database. Though the DBA has primary responsibility for user view design, he works closely with users and system designer in this task. Access privileges to the data, as defined in their view, should commensurate with the user's legitimate needs. User view can restrict user access to a limited set of data, they do not define task privileges such a read, delete or write. Often several users may share a single user view but have different authority levels.

(ii) Database Authorization Table - The database authorisation table contains rules that limit the actions a user can take. Each user is granted certain privileges that are coded in the authority table, which is used to verify the user's action requests.

(iii) User-defined Procedures - A user defined procedure allows the user to create a personal security program or routine to provide more positive user identification than a single password can. For example, the security procedure asks a series of personal questions, which only the legitimate user is likely to know.

(iv) Data Encryption - Many database systems use encryption procedures to pocket highly sensitive data, such as product formula, personnel pay rates, password files and certain financial data. Data encryption uses an algorithm to scramble selected data, thus making it unreadable to an intruder browsing the database. In addition to protecting stored data, encryption is used for protecting data that are transmitted across networks.

(v) Biometric Devices - Biometric devices measure various personal characteristics such as fingerprints, voiceprints, retina prints or signature characteristics. These user characteristics are digitised and stored permanently in a database security file or on an identification card that the user carries. When an individual attempts to access the database, a special scanning device captures his or her biometric characteristics, which are compared with the profile data stored internally or on the ID Card. If the data do not match, access is denied.

Question 8

Discuss various ways in which audit trail can be used to support security objectives?
(Final Nov. 2005)

Answer

Audit trails can be used to support security objectives in three ways:

(i) Detecting unauthorized access to the system: Detecting unauthroised access can occur in real time or after the fact. The primary objective of real-time detection is to protect the system from outsiders who are trying to breach system controls. A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by a virus or worm.

Depending upon how much activity is being logged and reviewed, real-time detection can impose a significant overhead on the operating system, which can degrade operational performance. After-the-fact detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthroised access was accomplished, or attempted and failed.

(ii) Facilitating the reconstruction of events: Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals or application processing errors. Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and avoid similar situations in the future. Audit trail analysis also plays an important role in accounting control. For example, by maintaining a record of all changes to account balances, the audit trail can be sued to reconstruct accounting data files that were corrupted by a system failure.

Promoting personal accountability: Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behaviour. Individuals are likely to violate an organisation's security policy if they know that their actions are recorded in an audit log.

Question 9

Describe the various security components available in a Secure Operating system.

(Final May 2006)

Answer

Operating System Security: Operating system security involves policy, procedures and controls that determine who can access the operating system, which resources they can access, and what actions they can take. The following security components are found in secure operating system:

(i) Log-on Procedure: A log-on procedure is the first line of defence against unauthorised access. When the user initiates the log-on process by entering user id and password, the system compares the ID and password to a database of valid users. If the system finds a match, then log-on attempt is authorised. If password or ID is entered incorrectly, then after a specified number of attempts, the system should lock out the user from the system.

(ii) Access token: If the log on attempt is successful, the OS creates an access token that contains key information about the user including user ID, password, user group and privileges granted to the user. The information in the access token is used to approve all actions attempted by the user during the session.

(iii) Access control list: This list contains information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compasses his or her ID and privileges contained in the access token with those contained in the access control list. If there is a match, the user is granted access.

(iv) Discretionary Access Control: The system administrator usually determines who is granted access to specific resources and maintains the access control list. However, in distributes system, resources may be controlled by the end-use. Resource owners in this setting may be granted discretionary access control, which allows them to grant access privileges to other users. For example, the controller who is owner of the general ledger grants read only privilege to the budgeting department while accounts payable manager is granted both read and write permission to the ledger.

Question 10

Write short note on source program library control. *(Final May 2006)*

Answer

Source Program library controls: In large computer systems, application program modules are stored in source code form on magnetic disks called the source program library (SPL).

To control the SPL, protective features and procedures must be explicitly addressed. This requires the implementation of SPL management system. This software is used to control four critical functions.

- Storing programs on the SPL.
- Retrieving program for maintenance purposes.
- Deleting obsolete programs from the library.
- Documenting program changes to provide an audit trail of the changes.

SPLMs may be supplied by the computer manufacturer as part of operating system or may be purchased through software vendors. An SPL requires specific planning and control techniques to ensure program integrity. The following control techniques may be used:

- Password control: One form of access control over the SPL is provided by assigning passwords. Every financially significant program stored in the SPL can be assigned a separate password. However, passwords have drawbacks. When more than one person is authorized to access a program, preserving the secrecy of a shared password is a problem.
- Separation of Test Libraries: Under this concept, a strict separation is maintained between the production programs that are subject to maintenance in the SPL and those being developed. Production programs are copied into the programmer's library for maintenance and testing purposes only. Direct access to the production SPL is limited to a specific librarian group that must approve all requests to modify, delete, and copy programs. Passwords for production programs can be changed regularly and disclosed only on a need-to-know basis.

Question 11

Why Computerised Information systems are more vulnerable to many more kinds of threats than manual systems? Name some of the key areas where large amounts of data stored in electronic form are most vulnerable. *(Final Nov. 2006)*

Answer

When large amounts of data are stored in electronic form they are vulnerable to many more kinds of threats than when they exist in manual form. Since the data is in electronic form and many procedures are invisible through automation, Computerized Information Systems (CIS) are vulnerable to destruction, misuse, error, fraud, hardware and software failures. Online systems and those utilizing the Internet are especially vulnerable because data and files can be immediately and directly accessed through computer terminals at many points in the network. Hackers can penetrate corporate networks and cause serious system disruptions. Computer viruses can spread rampantly from system to system, clogging computer memory or destroying programs and data. Software presents problems because of high costs of correcting errors and because software bugs may be impossible to eliminate. Data quality can also severely impact system quality and performance.

Following are the key areas due to which data stored in electronic form are most vulnerable:

(1)	Hardware failure,	(2)	Software failure,
(3)	Personnel actions,	(4)	Terminal access penetration
(5)	Theft of data, services, equipment,	(6)	Fire
(7)	Electrical problems,	(8)	User errors
(9)	Program changes,	(10)	Telecommunication problems

Question 12

Differentiate between General and Application controls. Also mention the broad categories into which the first can be subdivided. *(Final Nov.2006)*

Answer

General controls apply to a wide range of exposures that systematically threaten the integrity of all applications processed within CBIS environment. Application controls are focused on exposures associated with specific systems such as payroll, accounts receivable etc. These controls help to ensure the completeness and accuracy of transaction processing, authorization, and validity.

General controls can be subdivided under following headings:

(1) Operating system controls

(2) Data managements Controls

(3) Organizational structure controls

(4) Systems development controls

(5) Systems maintenance controls

(6) Computer Centre security controls

(7) Internet and intranet controls

(8) Personal computers control.

Question 13

What are the subversive threats? How do the intruders manipulate the messages being transmitted? (Final Nov. 2006)

Answer

Subversive threats refer to a situation where an intruder attempts to violate the integrity of some components in the subsystem. By installing an invasive tap on communication line, he can read and modify data or through inductive tap, he can monitor electromagnetic transmissions and allow the data to be read only. Subversive attacks can provide intruders with important information about messages being transmitted.

The intruders can manipulate messages in following ways:

(i) Intruders may insert a message in a message stream being transmitted e.g. EFTs add transfer of funds in an additional account.

(ii) They may delete a message being transmitted, e.g. remove a/c withdrawal message.

(iii) They may modify the contents of message e.g. increase the amount filled in a deposit transaction.

(iv) Intruders may alter the order of the message in a message stream.

(v) They may duplicate message in a message stream, or copy deposit transactions for their accounts.

(vi) They may deny message services between a sender and a receiver by discarding messages or delaying messages.

(vii) They may use techniques to establish spurious associations so that they are regarded as legitimate users of a system. They may play back a handshaking sequence previously used by a legitimate user of the system.

Question 14

What are five control objectives of an Operating system? (Final May 2007)

Answer

Five Control Objectives of an operating system are:

(i) The operating system must protect itself from users: User applications must not be able to gain control of, or damage in any way, the operating system, thus causing it to cease running or destroy data.

(ii) The operating system must protect users from each other: One user must not be able to access, destroy, or corrupt the data or programs of another user.

(iii) The operating system must protect users from themselves: A user's application may consist of several modules stored in separate memory locations, each with its own data. One module must not be allowed to destroy or corrupt another module.

(iv) The operating system must be protected from itself: The operating system is also made up of individual modules. No module should be allowed to destroy or corrupt another module.

(v) The operating system must be protected from its environment: In the event of a power failure or other disaster, the operating system should be able to achieve a controlled termination of activities from which it can later recover.

Question 15

State and explain the four back up and recovery features necessary in a DBMS

(Final Nov. 2007)

Answer

The four backup and recovery features necessary in a DBMS are discussed below:

(i) Database backup: The backup features makes a periodic backup of the entire database. This is an automatic procedure that should be performed at least once a day. The backup copy should be stored in a secure remote area.

(ii) Transaction log: This feature provides an audit trail of all processed transactions. It lists transactions in a transactions log file and records the resulting changes to the database in a separate database change log.

(iii) Checkpoint feature: The checkpoint facility suspends all data processing while the system reconciles the transaction log and the database change log against the database. At this point the system is in a "quiet state". Checkpoints occur automatically several times an hour. If a failure occurs, it is usually possible to restart the processing from the last check point. Thus, only a few minutes of transaction processing must be repeated.

(iv) Recovery Module: The recovery module uses the logs and backup files to restart the system after a failure.

Question 16

Briefly discuss any five database control features. *(Final May 2008)*

Answer

Database control features include the following:

(i) User View: The user view or subschema is a subset of the total database that defines the user's data domain and provides access to the database. Access privileges to the data, as defined in their views, should be commensurate with the users' legitimate needs. Several users may share a single user view but have different authority levels. Effective access control requires additional security measures.

(ii) Database Authorisation Table: The database authorization table contains rules that limit the actions that a user can take. This technique is similar to the access control list used in the operating system. Each user is granted certain privileges that are coded in the authority table, which is used to verify the user's action requests.

(iii) User-Defined Procedures: A user defined procedure allows the user to create a personal security program or routine to provide more positive user identification than a single password can.

(iv) Data Encryption: Many database systems use encryption procedures to protect highly sensitive data like password files, certain financial data, product formulae etc. Data encryption uses an algorithm to scramble selected data, thus making it unreadable to an intruder "browsing" the database. Encryption is used for protecting data that are transmitted across networks.

(v) Biometric Devices: User authentication procedures use biometric devices, which measure various personal characteristics, such as fingerprints, voice prints, retina prints, or signature characteristics. These user characteristics are digitized and stored permanently in a database security file or on an identification card that the user carries. When an individual attempts to access the database, a special scanning device captures his or her biometric characteristics, which is compared with the profile data stored internally or on the ID card. If the data do not match, access is denied.

Question 17

Discuss, how a controlled source program library environment can help to deter unauthorized changes to program. *(Final May 2008)*

Answer

A Controlled Source program library environment helps to deter unauthorized changes to program which are discussed below:

Password Control: One form of access control over the SPL (Source Program Library) is provided by assigning passwords. Every financially significant program stored in the SPL can be assigned a separate password.

Separation of Test Libraries: A strict separation is maintained between the production programs that are subject to maintenance in the SPL and those being developed. Production programs are copied into the programmer's library for maintenance and testing purposes only. Passwords for production programs can be changed regularly disclosed only on a need-to-know basis.

Audit trail and Management Report: Important feature of SPL Management software is the creation of reports that enhance management control and the audit function. Program modification reports, which describe in detail all program changes to each module are most useful. During an audit, these reports can be reconciled against program maintenance requests to verify that only the required changes were actually implemented. These reports can be produced as hard copy and also on disk.

Program Version Number: The SPLMS assigns a version number automatically to each program stored on the SPL. When programs are first placed in the libraries, they are assigned a version numbers of zero. With each modification to the program, the version number is

increased by one. This feature, when combined with audit trail reports, provides evidence for identifying unauthorized changes to program modules.

Controlling Access to Maintenance Commands: Powerful maintenance commands are available for most library systems that can be used to alter or eliminate program passwords, alter the program version number and temporarily modify a program without generating a record of the modification. Access to the maintenance commands themselves should be password controlled and the authority to use them should be controlled by management or the security group.

Message sequence numbering: An intruder in the communications channel may attempt to delete a message from a stream of messages, change the order of messages received, or duplicate a message. A sequence numbers is inserted in each message and any such attempt will become apparent at the receiving end.

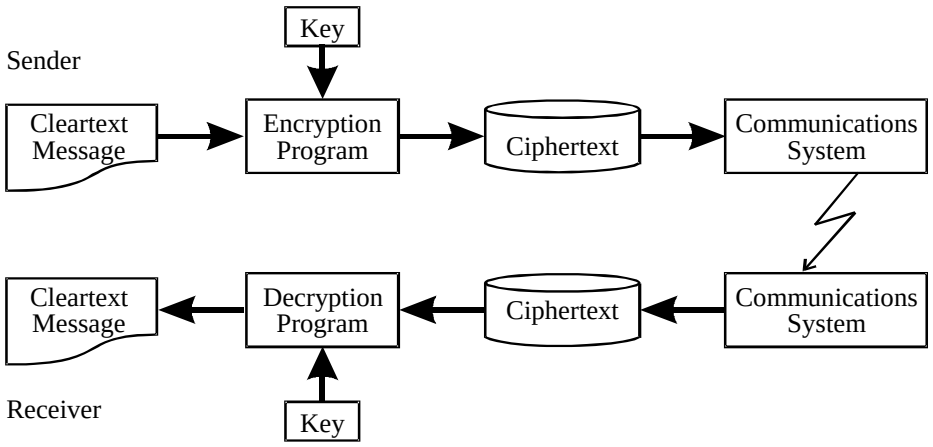
Question 18

Write short note on Encryption techniques *(Final Nov. 2008)*

Answer

Encryption Technique: It is the conversion of data into 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, cipher text is decoded back into clear text. The encryption algorithm uses a key, which is a binary number ranging typically from 56 to 128 bits in length. The more bits in the key, the stronger is the encryption method. Two general approaches used are private key and public key encryption.

Private Key Encryption: Data encryption standard (DES) 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, to produce a cipher text message. The encoded message is transmitted to the receiver, which decodes the message with a decryption program that uses the same key employed by the sender. Figure given below illustrates this technique.



In DES approach, a perpetrator may discover the key and intercept and decipher the message. The more individuals who know the key, the greater is the probability of it falling into wrong hands.

Public Key Encryption: It uses separate keys for encoding messages and for decoding them. Each recipient has a private key that is kept secret and a 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 they fall into the hands of a criminal.

14

CONTROLS IN EDP SET-UP : APPLICATION CONTROLS

Question 1

Briefly explain the various field checks used to ensure data integrity.

(Final Nov. 1996 & Nov. 1998)

Answer

The various field checks used to ensure data integrity have been described below:

Limit Check: This is a basic test for data processing accuracy and may be applied to both the input and output data. The field is checked by the program against predefined limits to ensure that no input/output error has occurred or at least no input error exceeding certain pre-established limits has occurred.

Picture Checks : These check against entry into processing of incorrect characters.

Valid Code Checks : Checks are made against predetermined transactions codes, tables or order data to ensure that input data are valid. The predetermined codes or tables may either be embedded in the programs or stored in (direct access) files.

Check Digit: One method for detecting data coding errors is a check digit. A check digit is a control digit (or digits) added to the code when it is originally assigned that allows the integrity of the code to be established during subsequent processing. The check digit can be located anywhere in the code, as a prefix, a suffix, or embedded someplace in the middle. Whenever the code is transcribed from one document to another this check is to be effected.

Arithmetic Checks : Arithmetic is performed in different ways to validate the result of other computations of the values of selected data fields.

Example : The discounted amount for Rs. 4,000 at 5% discounted may be computed twice by the following different ways :

$$4{,}000 - 4{,}000 \times \frac{5}{100} = 3{,}800 \text{ or}$$

$$4{,}000\left(\frac{100-5}{100}\right) = 3{,}800.$$

Valid Combinations of fields: In addition to each of the individual fields being tested, combinations of fields may be tested for validity.

Cross Checks: may be employed to verify fields appearing in different files to see that the result tally.

Valid Field Size, Sign and Composition: If the code number should be specified number of digits in length, the computer may be programmed to test that the field size is as specified. If the sign of the field must always be positive or always negative, a test may be made to determine that the field does indeed contain a proper composition of characters.

Question 2

What type of errors can corrupt a data code? *(Final May 2004)*

Answer

Two types of errors can corrupt a data code and cause processing errors. These are transcription and transposition errors as discussed below:

(i) Transcription errors fall into three classes:

- *Addition errors* occur when an extra digit or character is added to the code. For example, inventory item number 83276 is recorded as 832766.
- *Truncation errors* occur when a digit or character is removed from the end of a code. In this type of error, the inventory item above would be recorded as 8327.
- *Substitution errors* are the replacement of one digit in a code with another. For example, code number 83276 is recorded as 83266.

(ii) Transposition errors: There are two types of transposition errors.

- *Single transposition* errors occur when two adjacent digits are reversed. For instance, 83276 is recorded as 38276.
- Multiple transposition errors occur when nonadjacent digits are transposed. For example, 83276 is recorded as 87236.

Any of these errors can cause serious problems in data processing if they go undetected. For example, a sales order for customer 732519 that is transposed into 735219 will be posted to the wrong customer's account. A similar error in an inventory item code on a purchase order could result in ordering unneeded inventory and failing to order inventory that is needed. These simple errors can severely disrupt operations.

Question 3

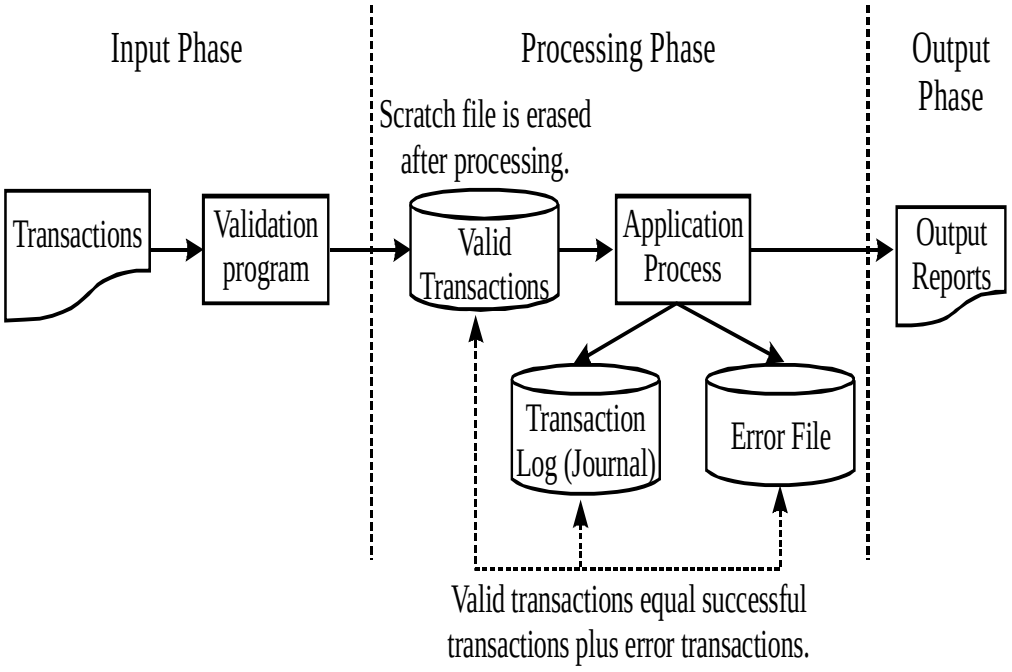
Write a short note on Transaction Logs *(Final Nov. 2003, May 2005)*

Answer

Transaction Logs: Every transaction successfully processed by the system should be recorded on a transaction log, which serves as a journal. Figure given on next page shows this arrangement.

There are two reasons for creating a transaction log. First, the transaction log is a permanent record of transactions. The validated transaction file produced at the data input phase is usually a temporary file. Once processed, the records on this file are erased (scratched) to make room for the next batch of transactions. Second, not all of the records in the validated transaction file may be successfully processed. Some of these records may fail tests in the subsequent processing stages. A transaction log should contain only successful transactions – those that have changed account balances. Unsuccessful transactions should be placed in an error file. The transaction log and error files combined should account for all the transactions in the batch. The validated transaction file may then be scratched with no loss of data.

Transaction Log to Preserve the Audit Trail



Question 4

Explain the importance of source documents and associated control techniques.

(Final Nov. 2005)

Answer

In systems that use physical source documents to initiate transactions, careful control must be exercised over these instruments. Source document fraud can be used to remove assets from the organization. For example, an individual with access to purchase orders and receiving reports could fabricate a purchase transaction to a non-existent supplier. If these documents were entered into the data processing stream along with a fabricated vendor's invoice, the system could process these documents as if a legitimate transaction had taken place. In the absence of other compensating controls to detect this type of fraud, the system would create an account payable and subsequently write a cheque for payment.

To control against this type of exposure, the organization must implement control procedures over source documents to account for each document, as described below:

(i) Use pre-numbered source documents: Source documents should come pre-numbered from the printer with a unique sequential number on each document. Source document numbers permit accurate accounting of document usage and provide an audit trail for tracing transactions through accounting records.

(ii) Use source documents in sequence: Source documents should be distributed to the users and used in sequence. This requires the adequate physical security be maintained over the source document inventory at the user site. When not in use, documents should be locked away. At all times, access to source documents should be limited to authorized persons.

(iii) Periodically audit source documents: Missing source documents should be identified by reconciling document sequence numbers. Periodically, the auditor should compare the numbers of documents used to date with those remaining in inventory plus those voided due to errors. Documents not accounted for should be reported to management.

Question 5

What is the significance of input validation control? Describe briefly three different levels of input validation controls used in computerized information system. (Final May 2006)

Answer

Input Validation Controls: These controls are intended to detect errors in transaction data before the data are processed. Validation procedures are most effective when they are performed as close to the source of the transactions as possible. However, depending on the type of Computer Based Information Systems (CBISs) in use, input validation may occur at various points in the system. For example, some validation procedures require making references against the current master file. Computer Based Information Systems (CBISs) using real-time processing or batch processing with direct access master files can validate data at the input stage. Some validation procedures are performed by each processing module prior to updating the master file record.

There are three levels of input validation controls:

(i) Field Interrogation: It involves programmed procedures that examine the characters of the data in the field.

The following are some common types of field interrogation:

(1) Limit Check: It may be applied to both the input data and the output data. The field is checked by the program to ensure that its value lies within certain predefined limits. For example, no pay where there is sick leave, physical balance can never go below zero etc.

(2) Picture checks: These check against entry into processing of incorrect characters. For example, all rooms are numbered by numeric. An incorrect room number 4D3 would be filtered.

(3) Valid Code checks: These checks are made against predetermined transactions codes, tables or order data to ensure that input data are valid. The predetermined codes or tables may either be embedded in the programs or stored in direct access files.

(4) Check digits: A customers' account number or any other numeric digits are checked for transcription and transposition errors.

(5) Arithmetic check: Arithmetic check is performed in different ways to validate the results of other computations of the values of selected data fields.

(6) Cross checks: These may be employed to verify fields appearing in different files to see that the results tally. For example, the quantity received, quantity invoiced by the supplier and quantity ordered may be compared. It may also be necessary to put check on the units of quantity.

(ii) Record Interrogation:

(1) Sequence checks are exercised to detect any missing transactions, off serially numbered vouchers or erroneous sorting.

(2) Format completeness checks are used to check the presence and position of all the fields in a transaction. This check is particularly useful for variable data field records.

(3) Redundant data checks are used in sequential processing. Matching keys of the transaction record and its master record may not be deemed enough. One may want to compare, say first five characters of the customer's name.

(4) Password: It is used to authorize users to access, read and write information.

(iii) File Interrogation: The purpose of file interrogation is to ensure that the correct file is being processed by the system. These controls are particularly important for master files, which contain permanent records of the firm and which, if destroyed or corrupted are difficult to replace. Various types of checks employed are:

(1) Internal label checks: These checks verify that the file processed is the one the program is actually calling for. To ensure that the correct file is processed, the system matches the file name and serial number in the header label with the

programme's file requirements. If the wrong file has been loaded, the system will send a message and suspend operation.

(2) Version checks are used to verify that the version of the file being processed is correct as per the programme's requirement.

(3) Expiration date check prevents a file from being deleted before it expires. To protect against destroying an active file by mistake, the system first checks the retention period contained in the header label. If the retention period has not yet expired, the system will generate error message.

Question 6

Discuss some common types of field interrogation as a validation control procedure in an EDP set up. *(Final Nov. 2006)*

Answer

Some common types of field interrogation as a validation control procedure in an EDP set up are discussed below:

(1) *Limit Checks*: The field is checked by the program to ensure that its value lies within certain predefined limits.

(2) *Picture checks*: These check against entry of incorrect characters into processing.

(3) *Valid Code Checks*: Checks are made against predetermined transactions codes, tables or other data to ensure that input data are valid. They may either be embedded in the programs or stored in files.

(4) *Check digit*: It is an extra digit that is added to the code when it is originally assigned. It allows the integrity of the code to be established during subsequent processing.

(5) *Arithmetic Checks*: Arithmetic is performed in different ways to validate the result of other computations of the values of selected data fields.

(6) *Cross Checks*: It may be employed to verify fields appearing in different files to check that the results tally.

Question 7

Write short notes on Audit trail controls in Computer Based Information System (CBIS)

(Final Nov. 2008)

Answer

Audit Trail Controls in CBIS: Every transaction must be traceable through each stage of processing from its economic source to its presentation in financial statements. In CBIS environment, the audit trail can become fragmented and difficult to follow. The following techniques can be used to preserve audit trails in a CBIS:

(a) *Transactions Logs*: Every successful transaction should be recorded on a transaction log, which serves as a journal. Thus the transaction log becomes permanent record of validated transactions etc. those that have changed account balances. Unsuccessful

transactions are placed in error file. The consolidation of transaction log and error files accounts for all transactions.

(b) *Transaction Listing*: The system should produce a hard-copy transaction listing of all successful transactions which may be reconciled by users.

(c) *Log and Listing of Automatic Transactions*: Some transactions are triggered internally by the system. All internally generated transactions must be placed in transaction log to maintain an audit trail. The responsible end user should receive detailed listing.

(d) *Unique Transaction Identifiers*: Each transaction processed by the system must be uniquely identified with a transaction number among thousands of records. In real-time systems, each validated transaction is assigned a unique number by the system.

(e) *Error Listing*: A listing of all error records should go to the appropriate user to support error correction and resubmission.

NOTE

15

DETECTION OF COMPUTER FRAUDS

Question 1

What measures can be adopted to detect Computer Frauds?

(Final Nov. 2002 & May 2007)

Answer

Following measures can be adopted to detect computer frauds as soon as possible:

(i) Conduct Frequent Audits: One way to increase the likelihood of detecting fraud and computer abuses is to conduct periodic external and internal audits as well as special network security audits. Auditors should regularly test system controls and periodically browse data files looking for suspicious activities. However, care must be exercised to make sure employees' privacy rights are not violated.

(ii) Use a Computer Security Officer: Most frauds are not detected by internal or external auditors. The study shows that assigning responsibility for fraud deterrence and detection to a computer security officer has a significant deterrent effect. This person should be independent of the information system function. The security officer can monitor the system and disseminate information about improper system uses and their consequences.

(iii) Use Computer Consultants: Many companies use outside computer consultants or in-house teams to test and evaluate their security procedures. The security weakness is detected by them is closely evaluated, and corresponding protective measures are implemented. Some companies dislike this approach, because neither they want their weaknesses to be exposed nor do they want their employees to know that the system can indeed be broken into.

(iv) Monitor System Activities: All system transactions and activities should be recorded in a log. The log should indicate who accessed what data, when, and from which terminal. These logs should be reviewed frequently to monitor system activity and trace any problems to their source.

There are a number of risk analysis and management software packages that can review computer system and networks. These systems evaluate security measures already in place and test for weaknesses and vulnerabilities. A series of reports is then generated that explain the weaknesses found and suggest improvements.

(v) Use Fraud Detection Software: People who commit fraud tend to follow certain patterns and leave behind telltale clues, such as things that do not make sense. Software has been developed to search out these fraud symptoms.

(vi) Use Computer Forensic Tools like Disk Imaging and Analysis which enable the fraud investigator to discover evidence of transactions that the fraudster might take as having been destroyed or might deem to be inaccessible.

(vii) Outside the normal file structure, i.e. where live files are stored, information can be recovered for investigation and detection of frauds from the unallocated space for data storage, slack space, deleted files undetected by processing software, Windows SWAP file, or Internet cache files.

Question 2

Why should businesses take Computer Frauds seriously? *(Final Nov. 2003)*

Answer

All businesses should take computer frauds seriously and need to assess the adequacy of their protection against computer frauds. Care should be taken even by those that do not currently do business on the Internet, since

(i) all businesses are now dependent on networked or stand alone computers;

(ii) individual businesses are increasingly linked through computer networks or by electronic payment systems;

(iii) the growth of electronic commerce means more businesses connected to the Internet and more risk of hacking;

(iv) the predicted growth of electronic cash means a real risk of interception, theft or destruction of electronic payments during transmission.

It may be stated that computer fraud is very different from conventional fraud in a number of important respects:

(i) It is easily hidden and hard to detect. Unlike conventional frauds, there may be no easily recognisable audit trail and the fraud is likely to be hidden in enormous volumes of data.

(ii) Evidence of computer crime may be not only hard to find, but also difficult to present to a court in a way which is effective or legally admissible. Anyone who has prosecuted or defended computer crime cases will be well aware of the problems of obtaining evidence in the first place, ensuring that it complies with the relevant statutes and trying to explain it to an inexperienced judge or jury.

(iii) It is easily committed in ways that may not be obvious:

- It involves the manipulation of "invisible" data;
- A few key strokes are all that may be needed;
- A business's computer can be remotely accessed, both by employees and outsiders;

- Huge amounts of data can be transported on a single floppy disk or CD-ROM, which can be written to in a matter of seconds.

Whilst this is not universally true, there is still a general lack of knowledge about how computers work and how systems can be protected which enables fraudsters to take advantage. The damage caused by interference with computer systems can be out of all proportion to the effort required to cause the damage. For example, the insertion of a virus may take a matter of minutes but wipes out all the data that the business has collected from its inception.

Question 3

What are the computer frauds committed through input? (Final May 2004& Nov 2006)

Answer

The simplest and most common way to commit a fraud is to alter computer input, it requires little, if any, computer skills. Instead, perpetrators need only to understand how the system operates so that they can cover their tracks. Some of the frauds that can be committed through input alteration are briefly discussed below:

(i) In collusive fraud, the perpetrator can use fraudulent input forms. For example, one perpetrator opened an account at a bank, and then prepared blank deposit slips. The slips were similar to those available in bank lobby, except that his account number was encoded on them. One morning he replaced all the deposit slips in the bank lobby with his forged ones, for three days all bank deposits using the forged slips went directly into his account. After three days the perpetrator withdrew the money and disappeared. He used an alias: his identity was never uncovered nor was he ever found.

(ii) In disbursement frauds, the perpetrator causes a company to either pay too much for ordered goods or to pay for goods that were never ordered. One perpetrator used a DTP package to prepare fraudulent bills for office supplies that were never ordered, then mailed those bills to companies across the country. The perpetrator kept the amount low enough so that most companies did not bother to enquire about purchase orders or approvals. An amazingly high percentage of the companies paid the bills without question.

(iii) To commit payroll frauds, perpetrators can enter data to increase their salary, create a fictitious employee, or retain a terminated employee on the records. Under the latter two approaches, the perpetrator proceeds to intercept and cash the illegal cheques.

(iv) In a cash receipts fraud, the perpetrator hides the theft by falsifying system input. For example, an employee at the Arizona Veteran's Memorial Coliseum sold customers full-price tickets, entered the sales as half-price tickets, and pocketed the difference.

Question 4

Substantiate with reasons to the view that there is a steep rise in the Internet Computer fraud. Why many institutions are unable to contain it? (Final Nov. 2004)

Answer

(a) There is no doubt that there has been a steep rise in the Internet computer frauds. This is mainly due to a number of characteristics of Internet, which are likely to attract fraudsters to commit frauds.

(i) It is unregulated in so far as who may set up a site. No license fees are payable to any central authority and no form of vetting is, or in practical terms ever could be, carried out on those persons or entities setting up sites.

(ii) An Internet site can be set up anywhere in the world at very low cost and can be reached from anywhere else in the world at low cost.

(iii) An impressive site with links to established companies or financial institutions may be more than an empty shell designed to attract and trap the unwary. There is no easy way of separating the genuine from the false.

(iv) The glamour and novelty of the Internet and the spurious credibility claimed by a site may cause otherwise prudent investors to become involved in fraudulent schemes.

(v) A site may, and probably will, operate outside the legal jurisdiction of the country in which the victim of the fraud resides.

The above factors make it extremely difficult to discover, in sufficient time to effect recovery or at all, the identity of the WWW Site operator.

Frauds on the Internet are proliferating as is evident by the examples released in the press.

(i) The offices of a small Illions company created the Agency for Inter-American Finance on the WWW in late 1995. The WWW site boasted impressive graphics and was linked to the Internet by a Swiss Internet Service provider. AIF claimed to be based in Antigua and that it was a provider of investment capital for Latin American businesses. Later investigation revealed that AIR was a Panamanian shell company, and that the bond and guarantor were fake.

(ii) “Fortuna Alliance” offered investors a return of $5,000 per month for an investment of $250. The USFTC began an investigation against this company for this improbable scheme. But then the investors had already lost $6 million before FTC blocked access to the site.

(iii) European Union Bank, which traded over the Internet, collapsed.

These are some common examples of Internet frauds:

- Overpayment Scam: In this very common scam type, a buyer will contact the seller and negotiate a deal on the merchandise. Many times, this buyer is located outside the country, and may be acting as a "broker" or a "third party" on behalf of another interested party. The buyer will send a cashier's cheque (or money order) for more than the asking price of the merchandise. The buyer will instruct the seller to send the difference for the overpayment. Unfortunately, the cashier's cheque or money

order used to originally pay the buyer is counterfeit and will be returned to the seller with insufficient funds. The seller is then cheated out of his or her own cash, plus any merchandise that was sent.

- Wire Fraud: In this scam, the buyer will request permission to wire transfer money directly into the seller's bank account. By providing confidential bank account information to the buyer, seller's account may be compromised by unscrupulous parties. Companies should always use caution when providing any form of personal information.
- Customs Scams: There are recent reports from the IFCC involving Eastern European countries and high incidences of fraud. Many of the fraudulent buyers of items are located in these countries and often ask that the seller to ship in a manner that will avoid customs or taxes. Sellers should be wary of this type of behavior.

Even though there is an increase in Internet computer frauds, not many are reported for various reasons and many companies are unable to contain it due to following reasons:

(i) Not everyone agrees on what constitutes computer fraud.

(ii) Many computer frauds go undetected.

(iii) 80-90% of the frauds data that are uncovered are not reported. Only the banking industry is required by law to report all frauds.

(iv) Most networks have a low level of security. It is estimated that two out of three sites have serious vulnerabilities, and most firewalls and other protective measures at the sites are ineffective.

(v) Many Internet pages give step-by-step instructions on how to perpetrate computer frauds and abuses. There are also thousands of pages on how to break into routers and disable web servers.

(vi) Law enforcement is unable to keep up with the growing number of computer frauds.

Question 5

Write short notes on the following:

(a) Internet Frauds *(Final May 2004 & Nov 2006)*

Answer

(a) Internet Frauds: Internet has become an integral part of our life today. Just as the Internet can be used for legitimate commerce, so can its power be harnessed for criminal and fraudulent purposes. The characteristics, which attract fraudsters, are as follows:

- It is unregulated in so far as who may set up a site. No license fees are payable to any central authority and no form of vetting is, or in practical terms ever could be, carried out on those persons or entities setting up sites.
- An Internet site can be set up anywhere in the world at very low cost and can reach anywhere else in the world at low cost. This means that fraudsters now have "global

reach" and can access a far larger market of potential victims than ever before. As fraudsters are always looking for new victims, this is a very attractive feature.

- An impressive site with links to established companies or financial institutions might be no more than an empty shell designed to attract and trap the unwary. There is no easy way of separating the genuine from the false.
- The glamour and novelty of the Internet and the spurious credibility claimed by a site may cause otherwise prudent investors to become involved in fraudulent schemes.
- A site may, and probably will, operate outside the legal jurisdiction of the country in which the victim of the fraud resides. A company, which gives itself a UK Internet address, need have absolutely no legal or commercial connection with the jurisdiction.

The above factors make it extremely difficult to discover, in sufficient time to effect recovery or at all the identity of the www site operator.

Question 6

Why is Computer fraud a serious threat to any business organisation? (Final May 2005)

Answer

In the modern business scenario, most of the businesses are dependent on networked or stand-alone computers. Even so, the individual businesses are also linked through computer networks or by electronic payments over the Internet. Hence, with the growth of electronic commerce and electronic cash, there are major threats of hacking, risk of interception and thefts, as well as destruction of electronic payments during transmissions.

It is very evident that the computer fraud is very different from the conventional frauds as:

- It is easily hidden and hard to detect. There may not be any easily recognizable audit trail and the fraud is likely to be hidden in enormous volumes of data.
- Evidence of computer crime, besides being hard to be found out, is difficult to present to a court in a manner, which is legally admissible and effective. It is not only extremely difficult to prosecute or defend the computer crimes; it is very hard to ensure that the evidence complies with the relevant statutes. It is also difficult to explain to the judge or jury having insufficient exposure to computers especially in India.
- There are various ways, which may not be obvious, to commit the computer frauds e.g.:
  - A few keystrokes are needed to manipulate the invisible data.
  - Employees as well as outsiders can access any computer remotely.
  - Huge volume of data can be transported on a floppy or CD which can be written in a very short time.

Lack of knowledge about the functioning of computers and protection of systems enables the fraudster to take advantage and commit the computer frauds/crimes. The extent of damage caused by the unauthorized interference with computer system may be totally disproportionate with the effort involved to cause the damage e.g. the insertion of virus takes few seconds whereas the

loss/damage of data may be enormous as it may have been collected and created in the organisation since the inception of the computer.

"Using a computer to cause prejudice, in the sense of financial and / or reputational damage, to a business" may be called a Computer Fraud. This statement describes precisely the damages caused by any computer fraud. Hence, the computer fraud, committed in any manner, is a serious threat to the business and appropriate measures must be taken to prevent the computer frauds.

Question 7

What kind of controls can be incorporated in the system to make frauds difficult to perpetrate? *(Final Nov. 2005)*

Answer

Various controls can be designed to make fraud difficult to perpetrate. These controls help to ensure the accuracy, integrity and safety of system resources. Some of these controls are briefly discussed below:

(i) Develop a strong system of internal controls: The overall responsibility for a secure and adequately controlled system lies with top management. Manager typically delegate the design of adequate control systems to systems analysts, designers and end users. The corporate information security officer and the operations staff are responsible for ensuring that control procedures are followed.

(ii) Segregate duties: There must be an adequate segregation of duties to prevent individuals from stealing assets and covering up their tracks.

(iii) Require vacations and rotate duties: Many fraud schemes require the ongoing attention of the perpetrator. If mandatory vacations were coupled with a temporary rotation of duties, such ongoing fraud schemes would fall apart.

(iv) Restrict access to computer equipment and data files: Computer frauds can be reduced significantly if access to computer equipment and data files is restricted. Only authroised users should be allowed to use the computer system, and legitimate users should be authenticated before they are allowed to use the system.

(v) Encrypt data and programmes: Another way to protect data is to translate it into a secret code, thereby making it meaningless to anyone without the means to decipher it.

(vi) Protect telephone lines: Computer hackers generally use telephone lines to transmit viruses and to access, steal and destroy data. One effective method to protect telephone lines is to attach an electronic lock and key to them. When new telephone system is installed, default password should be changed.

(vii) Protect the system from viruses: Some good virus protection programs are available. These programs are designed to remain in computer memory and search for viruses trying to infiltrate the system. The intrusion is detected when there is an unauthorized attempt to access an executable program. Virus detection program which spots an infection soon after it starts is more reliable than virus protection programs.

(viii) Control sensitive data: To protect its sensitive data, an organization should classify all of its data according to importance and confidentiality and then apply and enforce appropriate access restrictions. Controls can be placed over data files to prevent or discourage copying. Sensitive and confidential information, backup tapes and systems documentation should be locked up at night and should not be left out on desks. Servers and PCs should be locked when not in use. Companies should never store all of their data in one place or give an employee access to all of it. Closed circuit televisions can be used to monitor areas where sensitive data or easily stolen assets are handled.

(ix) Control laptop Computers: Special care should be given to laptops because thieves are increasingly breaking into cars and hotel rooms to steal laptops for the confidential information they contain. One of the control methods is to install software that makes it impossible for the computer to boot up without password. Laptops should be password protect and data on hard disk should be encrypted so that if a laptop is stolen, then data cannot be used.

Question 8

Define the following computer Fraud and Abuse technique:

(i) Hacking

(ii) Logic time bomb

(iii) Piggy backing

(iv) Spamming

(v) Data diddling. *(Final May, 2006)*

Answer

(i) Hacking: It refers to unauthorised access to and use of computer system usually by means of a personal computer and telecommunication network.

(ii) Logic time Bomb: It refers to the program that lies idle until some specified circumstance or a particular time triggers it. Once triggered, the bomb sabotages the system by destroying programs, data or both.

(iii) Piggy Backing: It refers to tapping into a telecommunications line and latching on to a legitimate user before he logs into the system; legitimate user unknowingly carries perpetrator into the system.

(iv) Spamming: It refers to a situation where the same message is e-mailed to everyone on one or more Usenet news groups or LISTSERV lists.

(v) Data diddling: Changing data before, during or after it is entered into the system in order to delete alter or add key system data is known as data diddling.

Question 9

Briefly explain five categories of Computer frauds based on the data processing model.

(Final Nov. 2007)

Answer

Various studies have examined frauds to determine the type of assets stolen and the approaches used by employees to commit computer frauds. One way to categorise computer fraud is to use the data processing model. Based on this model, five categories of computer frauds are:

(i) Input: The simplest and most common way to commit a fraud is to alter computer input, it requires little, if any, computer skills. Instead, perpetrators need only to understand how the system operates so that they can cover their tracks. Collusive fraud, disbursement frauds, payroll and receipt frauds are examples of computer frauds committed through computer input.

(ii) Processor: Computer fraud can be committed through unauthorized system use, including the theft of computer time and services. For example, some companies do not allow their employees to use company computers to keep personal or outside business records. Violating this policy would constitute a fraud. Similarly, employee goofing is also considered to be computer fraud.

(iii) Computer instructions: Computer fraud can be accomplished by tampering with the software that processes company data. This may involve modifying the software, making illegal copies of software or using it in an unauthorized manner. It might also involve developing a software program or module to carry out an unauthorized activity. This approach to computer fraud used to be one of the least common, because it requires a specialized knowledge of computer programming that is beyond the scope of most users.

(iv) Data: Computer fraud can be perpetrated by altering or damaging a company's data file or by copying, using them without authorization. There have been numerous instances of data files being scrambled, altered or destroyed by some selfish employees.

(v) Output: Computer fraud can be carried out by stealing or misusing system output. System output is usually displayed on monitors or printed on paper. Unless properly safeguarded, monitor and printer output is subject to pry eyes and unauthorized copying.

Question 10

Briefly explain various kinds of controls that can be incorporated in the system to make frauds difficult to perpetrate. *(Final May. 2008)*

Answer

One way to deter fraud is to design a system with sufficient controls to make fraud difficult to perpetrate. These controls help to ensure the accuracy, integrity and safety of system resources.

(i) Develop a strong system of Internal Controls: The overall responsibility for a secure and adequately controlled system lies with top management. Managers typically delegate the design of adequate control systems to systems analysts, designers, and end users. The corporate information security officer and the operations staff are typically responsible for ensuring that control procedures are followed.

(ii) Segregate Duties: There must be an adequate segregation of duties to prevent individuals from stealing assets and covering up their tracks.

(iii) Require vacations and Rotate Duties: Many fraud schemes, such as lapping and kiting, require the ongoing attention of the perpetrator. If mandatory vacations were coupled with a temporary rotation of duties, such ongoing fraud schemes would fall apart.

(iv) Restrict Access to Computer Equipment and Data Files: Computer frauds can be reduced significantly if access to computer equipment and data files is restricted. Physical access to computer equipment should be restricted, and legitimate users should be authenticated before they are allowed to use the system.

(v) Encrypt Data and Programs: Another way to protect data is to translate it into a secret code, thereby making it meaningless to anyone without the means to decipher it.

(vi) Protect Telephone Lines: Computer hackers use telephone lines to transmit viruses and to access, steal, and destroy data. One effective method to protect telephone lines is to attach an electronic lock and key to them.

(vii) Protect the System from Viruses: There are hundreds of thousands of virus attacks every year, and estimated 90% of the PCs that suffer a virus attack are re-infected within 30 days by the same virus or some other virus. A system can be protected from viruses by ensuring that the latest versions of the anti-virus programs are used.

(viii) Control Sensitive Data: Controls can be placed over data files to prevent or discourage copying. Employees should be informed of the consequences of using illegal copies of software, and the company should institute controls to see that illegal copies are not in use. Backup tapes, and system documentation should be locked up. Servers and PCs should also be locked when not in use. Companies should never store all of their data in one place or give an employee access to all of it. Closed-circuit televisions can be used to monitor areas where sensitive data or easily stolen assets are handled.

(ix) Control Laptop Computers: To control laptops, companies should take following measures:

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

Question 11

Define the following computer fraud and abuse technique:

(i) War dialing

(ii) Scavenging

(iii) Cracking

(iv) Internet terrorism

(v) Masquerading. *(Final May. 2008)*

Answer

(i) War dialing: It relates to programming a computer search for an idle modem by dialing thousands of phone lines. Perpetrator enters the system through idle modem, captures the personal computer attached to the modem, and gain access to the network to which the personal computer is attached.

(ii) Scavenging: Gaining access to confidential information by searching corporate records is termed as scavenging. Scavenging methods range from searching for printouts or carbon copies of confidential information to scanning the contents of computer memory.

(iii) Cracking: Unauthorized access to and use of computer systems, usually by means of a personal computer and a telecommunications network is called cracking. Crackers are hackers with malicious intentions.

(iv) Internet terrorism: Using internet to disrupt electronic commerce and to destroy company and individual communications is referred as internet terrorism.

(v) Masquerading: Under this technique, perpetrator gains access to the system by pretending to be an authorized user and enjoys same privileges as the legitimate user. Fraud messages can be sent to the receiver by using legitimate users identity and thus can prove to be harmful.

Question 12

Recently you have received a report from your bank client that money from one account has been unauthorisedly transferred to another account by stealing the login information of a client through Internet. How will you stop the recurrence of such events? *(Final Nov. 2008)*

Answer

Most of the attacks on online banking used today are based on deceiving the user to steal login data and valid PINs. Two well known examples for those attacks are phishing and pharming. Cross-site scripting and key logger/Trojan horses can also be used to steal login information.

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as user names, passwords and credit card details by masquerading as trust worthy entity in an electronic communication.

Pharming is hackers attack aiming to redirect websites traffic to another, bogus website. Pharming can be conducted either by changing the hosts file on a victims computer or by exploitation of a vulnerability in DNS server software.

Under such circumstances, all the customers must be informed about possible traps that they may fall into if they reveal their login and passwords. Continuous update and awareness should be created by the bank about various methods that are followed by fraudsters. The company should

have constant watch and vigil over such happenings and inform the customers immediately. To be more secure:

(1) The Company should have a policy which states very clearly that no login information will be sought by the bank either in email, or over phone. This should be communicated to all customers.

(2) There should be more than just two co-ordinates of login and password to make the transaction more secure. It can ask for additional details which are known only to the customer.

(3) The company should educate the customers about the use of strong passwords and the benefits of changing the passwords.

Question 13

Persian Paints is a small but highly regarded paint manufacturing company. The company has a network in place linking many of its business operations. Though the firm believes that its security is adequate, the recent addition of a Web site has become an open invitation to hackers. Management requested a risk assessment. The risk assessment identified a number of potential exposures. These exposures, their associated probabilities and average losses are summarized in the following table:

Persian Paints Risk Assessment

	Exposure	*Probability of Occurrence (%)*	*Annual Average Loss (Rs.)*
1.	*Virus attack*	*60*	*75,000*
2.	*Data Loss*	*12*	*70,000*
3.	*Embezzlement*	*3*	*30,000*
4.	*User Errors*	*95*	*25,000*
5.	*Threats from Hackers*	*95*	*90,000*
6.	*Improper use by Employees*	*5*	*5,000*
7.	*Power Failure*	*15*	*3,00,000*

Using the above risk assessment data, calculate the expected annual loss for each exposure. Which control points have the greatest vulnerability and Least vulnerability? Prepare a written report that summarises your findings and recommendations.

(Final Nov. 2008)

Answer

Persian Points Company has recently added a website and this has opened up invitation to hackers and the management is in the process of assessing its risk management. Various risk assessment factors are identified. The annual average losses and the associated problems are provided. We can calculate the expected monetary losses for each of the potential exposure.

	Exposure	Expected Monetary Loss		Rs.
1.	Virus Attack	0.60 × 75,000	=	45,000
2.	Data loss	0.12 × 70,000	=	8,400
3.	Embezzlement	0.03 × 30,000	=	900
4.	User Errors	0.95 × 25,000	=	23,750
5.	Threats from Hackers	0.95 × 90,000	=	85,500
6.	Improper use by Employees	0.05 × 5,000	=	250
7.	Power Failure	0.15 × 3,00,000	=	45,000

Amongst all the expected monetary losses listed in the above table, Item No. 5 results in the highest expected loss. Hence, "threats from hackers" has the highest vulnerability. Item No. 6, "improper use by employees" has the least vulnerability since it results in the least expected loss.

A careful analysis of the last column in the above table would show that the top management should exercise control by having a careful watch on the following factors in the following order of priority as listed below:

(i) Threats from Hackers (Item 5)

(ii) Virus Attack (Item 1) and power failure (Item 7)

(iii) User errors (Item 4)

(iv) Data Loss (Item 2)

(v) Embezzlement (Item 3)

(vi) Improper use by employees (Item 6).

NOTE

16

CYBER LAWS AND INFORMATION TECHNOLOGY ACT 2000

Question 1

Explain briefly the scope of the Information Technology Act, 2000 along with the relevant definitions that are used. *(Final May 2003 & Nov. 2004)*

Answer

Scope of the Information Technology Act, 2000: 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.

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) "A*ddressee*" – a person who is intended by the originator to receive the electronic record but does not include any intermediary.

(c) "A*ffixing 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) "A*ppropriate 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 programmes, 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 programmes, software and databases or micro film or computer generated micro fiche.

(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

What are the powers of the Central Government to make rules, as given in Section 87, Chapter XIII of Information Technology Act, 2000? (Final May 2004)

Answer

Powers of Central Government to make rules: Section 87 of the Information Technology Act, 2000 confers on the Central Government the power to make rules by notifying in the Official Gazette and the Electronic Gazette, in respect of certain matters, some of which are:

- Manner in which
  - any information or matter may be authenticated by means of digital signature under section 5;
  - electronic records shall be filed, created or issued and the method of payment;
  - digital signature may be affixed under section 10;
  - the adjudicating officer shall hold enquiry under section 46.
- (Electronic) Form in which
  - electronic records shall be filed, created or issued;
  - Digital signature may be affixed under section 10;
  - an application for licence may be made;
  - application is made for renewal of licence under section 23;
  - application for issue of a digital signature certificate may be made;
  - appeal may be filed .
- Prescribing fee
  - payable along with application for license;
  - for renewal of a licence under section 23;
  - (late) payable under proviso to section 23;
  - to be paid to certifying authority for issue of digital signature certificate;
  - for filing an appeal.

- Prescribing salary, allowances and other conditions of service of the
  - Presiding Officer under section 52;
  - officers and employees.
- Prescribing procedure
  - for security, for the purpose of creating secure electronic record and secure digital signature under section 16;
  - for investigation of misbehaviour or incapacity of the Presiding Officer .
- Prescribing
  - standards to be observed by the Controller ;
  - requirements which an applicant must fulfil ;
  - period of validity of licence granted ;
  - documents which shall accompany an application for licence;
  - qualification and experience which the adjudicating officer shall possess;
  - any other power of the civil court;
- Matters relating to the
  - type of digital signature under section 10;
  - any other.

Every notification made by the Central Government shall be laid, as soon as possible after it is made, before each House of Parliament, while it is in session, for a total period of thirty days. This period may be comprised in one session or in two or more successive sessions. If before the expiry of the session immediately following the above period, both Houses agree in making any modification, the rule will thereafter have effect only in the modified form. Similarly, if both Houses agree that the rule should not be made, the notification shall have no effect, thereafter.

Question 3

What is a Digital Signature? How is it used? What are the duties of certifying authorities in regard to its usage? *(Final Nov. 2002, Nov. 2005 & Nov. 2007)*

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 Act, 2000, Certifying Authority shall follow certain procedures in respect of Digital Signatures as given below:
    - Make use of hardware, software and procedures that are secure from intrusion and misuse.
    - Provide a reasonable level of reliability in its services, which are reasonably suited to the performance of intended functions.
    - Adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured and
    - Observe such other standards, as specified by the regulation.
2. Every Certifying Authority shall ensure that every person employed by him complies with the provisions of the Act, or rules, regulations or orders made thereunder.
3. A Certifying Authority must display its licence at a conspicuous place of the premises in which it carries on its business. A Certifying Authority whose licence is suspended or revoked shall immediately surrender the license to the Controller.
4. Every Certifying Authority shall display its Digital Signature Certificate, which contains the public key corresponding to the private key used by that Certifying Authority and other relevant facts.

Question 4

Write short notes on the following:

(a) Digital Signature Certificate *(Final Nov. 2003)*

(b) Encryption. *(Final Nov. 2004)*

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.

(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 5

State the objectives and scope of IT Act, 2000. *(Final May 2005 & Nov 2007)*

Answer

The IT Act 2000, passed by both the houses of Indian Parliament in May 2000 and subsequently received the assent of the President in August 2000, contains the Cyber Laws. It provides the legal infrastructure for e-commerce and it is important to understand the various perspectives of the Act.

The objectives of the Act are:

- To grant legal recognition to transactions carried out through electronic data interchange and other means of electronic communication commonly referred to as "electronic commerce" replacing the paper-based communication;
- To give legal recognition to Digital Signature for authentication of any information or matter which requires authentication under any law;
- To facilitate electronic filing of documents with Government Departments;
- To facilitate electronic data storage;
- To facilitate and give legal sanction to electronic funds transfers between banks and financial institutions;
- To give legal recognition for keeping of books of account by Bankers in electronic form;
- To amend the Indian Penal Code, the Indian Evidence Act, 1872; the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934.

Scope of the Act: This Act is applicable to whole of India, unless otherwise provided in the Act. It also applies to any offence or contravention there under committed outside India by any person.

Different provisions of this Act came into force on the different dates as notified by the Central Government.

The Act shall not be applicable 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.

Question 6

"No Company, big or small, can ignore the opportunity opened by the Internet." What are the various methods by which Internet can be accessed? What are the considerations for choosing the right alternative? *(Final Nov. 2005)*

Answer

The various methods by which Internet can be accessed are:

- Internet Service Provider (ISP)
- Online Services
- Direct communication through a gateway.
- Use of someone else's gateway

The following points are to be considered for choosing the right alternative:

- Whether accessing the Internet for the company or limited official use at distant location,
- Type of services needed,
- Monthly usage time,
- Budgeted spending,
- Data rate wanted.

Question 7

Describe the composition and powers of Cyber regulatory appellate tribunal.
(Final May, 2006, Nov 2006 & Nov 2008)

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 8

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? (Final Nov. 2006)

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.

Question 9

Describe some of the powers of controller under section 89 to make regulations consistent with Information Technology Act, 2000. *(Final May 2007)*

Answer

The controller has been given the following powers under Section 89 to make regulations consistent with the Information Technology Act, 2000:

- The particulars relating to maintenance of data base containing the disclosure record of every Certifying Authority
- The conditions and restrictions subject to which the Controller may recognize any foreign Certifying Authority
- The terms and conditions subject to which a license may be granted
- Other standards to be observed by a Certifying Authority
- The manner in which the Certifying Authority may make the disclosure Under Section 34
- The particulars of statement to be submitted along with an application for the issue of a Digital Signature Certificate
- The manner in which the subscriber should communicate the compromise of private key to the Certifying Authority.

Question 10

Discuss briefly the powers of Central Government under Section 87 to make rules in respect of Information Technology Act, 2000. *(Final May 2008)*

Answer

Section 87 of the Act confers on the Central Government the power to make rules. These are:

(1) The manner in which any matter may be authenticated by a digital signature.

(2) The manner and format in which electronic records shall be filed or issued.

(3) The type of digital signature, manner and format in which it may be affixed.

(4) The security procedure for the purpose of creating same electronic record and secure digital signature.

(5) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers.

(6) The requirements, manner and form in which application is to be made for a license to issue Digital Signature Certificates.

(7) The period of validity of the license.

(8) The qualification, experience of an adjudicating Officer, as well as other officers.

(9) The salary, allowances and terms and conditions of service of the Presiding Officer, etc.

Question 11

Discuss the main provisions provided in Information Technology Act, 2000 to facilitate E-governance. *(Final Nov. 2008)*

Answer

E-Governance sections of chapter III 6, 7 and 8 are the main sections for provisions related to E-governance provided in IT Act, 2000 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.

(iii) The details which will facilitate the identification of the origin, destinations, dates and time of despatch 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.

17

AUDIT OF INFORMATION SYSTEMS

Question 1

Discuss the various issues that are of primary concerns for an auditor involved in information system audit. *(Final May 2003 & Nov 2008)*

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 organisation's general ledger. Specifically, auditors must ensure that provisions are made for:

- An adequate audit trail so that transactions can be traced forward and backward through the system.
- Controls over the accounting for all data (i.e. transactions) entered into the system and controls to ensure the integrity of those transactions throughout the computerized segment of the system.
- Handling exceptions to and rejections from the computer system.
- Testing to determine whether the systems perform as stated.
- Control over changes to the computer system to determine whether the proper authorization has been given.
- Authorisation procedures for system overrides.
- Determining whether organization and Government policies and procedures are adhered to in system implementation.
- Training user personnel in the operation of the system.
- Developing detailed evaluation criteria so that it is possible to determine whether the implemented system has met predetermined specifications.
- Adequate controls between interconnected computer systems.
- Adequate security procedures to protect the user's data.
- Backup and recovery procedures for the operation of the system.

- Technology provided by different vendors (i.e. operational platforms) is compatible and controlled.
- Databases are adequately designed and controlled to ensure that common definitions of data are used throughout the organization, that redundancy is eliminated or controlled and that data existing in multiple databases is updated concurrently.

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

Question 2

What is the sole purpose of an Information System (IS) Audit? *(Final Nov. 2003)*

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.

Question 3

What is the role of an IS Auditor? *(Final Nov. 2003)*

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 4

While performing an IS Audit, the Auditor should make sure that various objectives are met. Briefly describe them. *(Final Nov. 2003 & Nov 2007)*

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 5

Describe the major techniques of Concurrent Audit of Information systems. Bring out the relevance of such Audit. *(Final Nov. 2002; May 2003 & May 2004)*

Answer

Commonly used concurrent audit techniques for information systems are discussed below:

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

   In a batch processing system, the ITF technique eliminates the need to reverse test transactions and is easily concealed from operating employees. ITF is well suited to testing on-line processing systems because test transactions can be submitted on a frequent basis, processed with actual transactions, and traced throughout every processing stage. All this can be accomplished without disrupting regular processing operations. However, care must be taken not to combine dummy and actual records during the reporting process.

2. The Snapshot Technique examines the way transactions are processed. Selected transactions are marked with a special code that triggers the snapshot process. Audit modules in the program record these transactions and their master file records before and after processing. Snapshot data are recorded in a special file and reviewed by the auditor to verify that all processing steps have been properly executed.

3. System Control Audit Review File (SCARF) uses embedded audit modules to continuously monitor transaction activity and collect data on transactions with special audit significance. The data are recorded in a SCARF file. Transactions that are generally recorded in a SCARF file include those exceeding a specified limit, inactive accounts, deviating from company policy, or containing write- downs of asset values etc. Periodically the auditor examines the SCARF file to identify questionable transactions and performs the necessary follow- up investigations.

4. Audit hooks are audit routines that flag suspicious transactions. For example, internal auditors at Insurance Company determined that their policyholder system was vulnerable to fraud every time a policyholder changed his or her name or address and then subsequently withdrew funds from the policy. They devised a system of audit hooks to tag records with a name or address change. The internal audit department will

investigate these tagged records for fraud. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach of real-time notification displays a message on the auditor's terminal.

5. Continuous and Intermittent Simulation (CIS) module that is embedded in a data base management system, examines all transactions that update the DBMS using criteria similar to SCARF. If a transaction has special audit significance, the module independently processes the data, records the results and compares them with those obtained by DBMS. If any discrepancies exist, the details are written on to an audit log for subsequent investigation. In case of serious discrepancies, CIS may prevent the DBMS from executing the update process.

Relevance of Concurrent Audit Techniques for Information System

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

Question 6

Briefly discuss the framework on which the auditor should work for the audit of Computer Security. *(Final May 2004)*

Answer

A framework on which the auditor should work for the audit of computer security is given below:

(i) Types of Errors and Fraud

- Theft of or accidental or intentional damage to hardware and files.
- Loss or theft of or unauthorized access to programs, data files, and other system resources.
- Loss or theft of or unauthorized disclosure of confidential data.
- Unauthorized modification or use of programs and data files.
- Interruption of crucial business activities.

(ii) Control Procedures

- Information security/protection plan.
- Restrictions on physical access to computer equipment.

- Logical access controls based on password protection and other authentication procedures.
- Data storage and transmission controls such as encryption.
- Virus protection procedures.
- File backup and recovery procedures.
- Fault-tolerant systems design.
- Disaster recovery plan.
- Preventive maintenance.
- Firewalls.
- Information systems insurance.

(iii) Audit Procedures : System Review

- Inspect computer sites.
- Interview IS personnel about security procedures
- Review written documentation about physical access policies and procedures
- Review logical access policies and procedures.
- Review file backup and recovery policies and procedures
- Examine data storage and transmission policies and procedures.
- Review procedures employed to minimize system downtime.
- Examine system access logs.
- Examine disaster recovery plan.
- Examine casualty insurance policies.

(iv) Audit Procedures : Tests of Controls

- Observe computer site access procedures.
- Observe the preparation and off-site storage of backup files.
- Review records of password assignment and modification.
- Investigate how unauthorized access attempts were dealt with.
- Verify the extent of data encryption use.
- Verify the effective use of data transmission controls.
- Verify the effective use of firewalls.
- Verify the effective use of virus protection procedures.

- Verify the use of preventive maintenance and uninterruptible power.
- Verify amounts and limitations on insurance coverage.
- Examine the results of test simulations of disaster recovery plan.

(v) Compensating Controls

- Sound personnel policies.
- Effective user controls.
- Segregation of incompatible duties.

Question 7

"In On-line systems, conventional audit trail is difficult and almost impossible." Why? Explain the kind of audit techniques used in such system. (Final Nov. 2004)

Answer

Historically, auditors have placed substantial reliance in evidence-collection work on the paper trail that documents the sequence of events that have occurred within an information system. Paper based audit trails have been progressively disappearing as online computer-based systems have replaced manual systems and as source documents have given a way to screen based inputs and outputs. In a batch processing system, one can still expect to find a visible trail of "run-to-run " controls, which can be reconciled to the original input batch totals. In such systems, it is unusual to find any significant loss of audit trails regarding the control totals. In online systems, however, data are stored in device-oriented rather than human-oriented form. Moreover, data files belonging to more than one application may be updated simultaneously by each individual transaction. In such systems, traditional run-to-run controls do not exist and the potential for loss of audit trail is significant.

In a batch processing systems, the test data is prepared by an auditor for audit purposes and the results are obtained from the program under execution and copy of relevant files. The results are compared with the predetermined correct outputs. Any discrepancies indicating processing errors or control deficiencies etc. are thoroughly investigated. In on-line systems, such kind of audit trail is not desirable since millions of transactions can be processed in a short time. In such cases, evidence gathered after data processing is insufficient for audit purposes. In addition, since many on-line systems process transactions continuously, it is difficult or impossible to stop the system in order to perform audit tests. Hence, the auditor needs to identify problems that can occur in an information system on a more timely basis. For this reason, a set of audit techniques has been developed to collect evidence at the same time as an application system undertakes processing of its production data.

Following are some of the audit techniques, which are being used for on-line systems :

(A) Concurrent Audit Techniques: These techniques can be used to continually monitor the system and collect audit evidence while live data are processed during regular operating hours. As the name suggests, this type of audit technique uses embedded audit modules, which are segments of program codes that perform audit functions. They

also report test results to the auditors and store the evidence collected for the auditor's review. These techniques are often time consuming and difficult to use, but are less so, if incorporated when programs are developed.

There are five such techniques, which auditors commonly use. These are :

(i) Integrated Test Facility (ITF) : In this technique, a small set of fictitious records is placed in the master file. Processing test transactions to update these dummy records will not affect the actual records. Actual and fictitious records are concurrently processed together, without the knowledge of employees. Auditor compares the output of dummy records with expected results and its controls to verify the correctness of the system.

(ii) Snapshot Technique : This technique examines the way transactions are processed. Selected transactions are marked with special code that triggers the snapshot processes. Audit modules in the program record these transactions and their master file records before and after processing. Snapshot data are recorded in a special file and reviewed by the auditor to verify that all processing steps have been properly executed.

(iii) SCARF : System Control Audit Review File uses embedded audit modules to continuously monitor transaction activities and collect data on transactions with special audit significance. The data is recorded in a SCARF file, which may have been exceptional transactions. Periodically the auditor receives a print out of the SCARF file, examines the information to identify any questionable transactions, and performs any necessary follow up investigation.

(iv) Audit Hooks : These are audit routines that flag suspicious transactions. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach, known as "real-time notification", displays a message on the auditor's terminal.

(v) CIS : Continuous and intermittent simulation embeds an audit module in a DBMS. This module examines all transactions that update the DBMS using criterion similar to those of SCARF. If a transaction has special audit significance, the module independently processes the data, records the results and compares them with those obtained by the DBMS. Discrepancies are noted and details are investigated.

(B) Analysis of Program Logic: If a serious natured unauthorized code is found, the auditor goes for detailed analysis of the program logic. This is a difficult task and the auditor must be well versed with the programming language. These days following software packages serve as aids in this analysis.

- Automated flowcharting programs
- Automated decision table programs.
- Scanning Routine.

- Mapping Programs.
- Program tracing.

Question 8

Write short note on disc Imaging and Analysis Technique. (Final May 2003 & May 2005)

Answer

Disc Imaging and Analysis Technique – It enables the fraud investigator to discover evidence of transactions that the fraudster thought were inaccessible or had been destroyed. It works in the following stages:

(i) Using specialist hardware/software without the suspect necessarily being alerted. An exact copy of the computer hard disc is taken leaving the original completely intact and leaving no trace of the copying process. This preserves the integrity of the hard disc and confidentiality of the investigation. The image is written directly to an optical disc, which can be copied onto a CD ROM for investigative purpose.

(ii) The image copy of disc is processed and areas of storage containing partially overwritten files and files which have been marked as deleted but not overwritten are recorded. At the time the image is taken, it is probable that there will be a number of deleted files or file fragments that have not been overwritten and are therefore available to investigator.

(iii) The final stage is the analysis of the processed image. This is done by search software, which can be programmed to find references to suspect transactions. The search is across all the contents of disc. Information can be recovered from investigation of free space, lost chains, slack space, deleted files, temporary Internet files etc.

Question 9

Discuss various factors that render manual audit method ineffective in IS audit.

(Final Nov. 2005 & May 2008)

Answer

The audit methods that are effective for manual audits prove ineffective in many IS audits because of the following factors:

(i) Electronic evidence: Essential evidence is not physically retrievable by most auditors, and it is not readable in its original electronic form.

(ii) Terminology: The tools and techniques used in automated applications are described in terms that are difficult for the non-EDP auditor to understand.

(iii) Automated processes: The methods of processing are automated rather than manual, making it difficult for the non-EDP auditor to comprehend processing concepts and the logic of these concepts.

(iv) New risks and controls: Threats to computer systems and the countermeasures to those threats are new to non-EDP auditors, and the magnitude of the risks and the effectiveness of the controls are not understood.

(v) Reliance on controls: In manual systems, the auditor can place some reliance on hard-copy evidence regardless of the adequacy of the controls. Whereas, in automated systems, the electronic evidence is only as valid as the adequacy of controls.

Question 10

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

(Final Nov. 2005)

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 authroised is identified and handled according to prescribed managerial policies.

(vi) Computer data files are accurate, complete, and confidential.

Question 11

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?

(Final May, 2006)

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 12

How do MIS auditing enhance the control process? *(Final Nov. 2006)*

Answer

Comprehensive and systematic MIS auditing can help organizations to determine the effectiveness of the controls in their information systems. Regular data quality audits should be conducted to help organizations ensure a high level of completeness and accuracy of the data stored in their systems. Data cleansing should also be performed to create consistent and accurate data for company wide use in e-commerce and e-business.

An MIS audit identifies all of the controls that govern individual information systems and assesses their effectiveness. To accomplish this, the auditors must acquire a thorough understanding of operations, physical facilities, telecommunications, control system, data security objectives, organizational structure, manual procedures and individual applications.

The auditor usually interviews key individuals who use and operate specific information system concerning their activities and procedures. Applications controls, overall integrity controls and control discipline are examined. The auditor should trace the flow of sample transactions through the system and perform tests using, if appropriate, automated audit software.

The auditor lists and ranks all control weaknesses and estimates the probability of their occurrences. He then assesses the financial and organisational impact of each threat. Management is expected to device a plan for countering significant weaknesses in controls.

Question 13

Write short note on Integrated Test Facility. *(Final Nov. 2006)*

Answer

Integrated Test Facility: It is one of the five concurrent audit techniques. It places a small set of fictitious records in the master files. The records might represent a fictitious division, department, or branch office, or a customer or supplier. Processing test transactions to update these dummy records will not affect the actual records. Because fictitious and actual records are processed together, company employees usually remain unaware that this testing

is taking place. The system can distinguish ITF records from actual records, collect information on the effect of the test transactions and report the results. The auditor compares processing and expected results in order to verify that the system and its controls are operating correctly.

In a batch processing system, the ITF technique eliminates the need to reverse test transactions and is easily concealed from operating employees. ITF is well suited to testing on-line processing systems because test transactions can be submitted on a frequent basis. All this can be accomplished without disrupting regular processing operations. However, care must be taken not to combine dummy and actual records during the reporting process.

Question 14

Write short notes on the following:

(a) Snapshot technique. *(Final May 2007)*

(b) Review areas of an IS Auditor. *(Final Nov 2007*)

Answer

(a) Snapshot Technique: It examines the way transactions are processed. Selected transactions are marked with a special code that triggers the snapshot process. Audit modules in the program, records these transactions and their master file records before and after processing. Snapshot data are recorded in a special file and reviewed by the auditor to verify that all processing steps have been properly executed.

(b) The IS auditors may focus on following review areas:

(1) Computerised systems and applications: The auditor should verify that systems and applications are appropriate to the users' needs, efficient and adequately controlled to ensure valid, reliable, timely and secure input, processing and output at current and projected levels of system activity.

(2) Information Processing Facilities: This facility must be controlled to ensure timely, accurate and efficient processing of applications under normal and potentially disruptive conditions.

(3) Systems Development: An IS auditor should ensure that systems under development meet the objectives of the organization, satisfy user requirements and provide efficient, accurate and cost effective systems and applications. The auditor should also ensure that these systems are written, tested and installed in accordance with generally accepted standards for systems development.

(4) Management of Information Systems: MIS must develop an organizational structure and procedures to ensure a controlled and efficient environment for information processing. This plan should also specify the computers and peripheral equipments required to support all functions in an economic and timely manner.

(5) Client/Server, Telecommunications and Intranets: In a client/server environment, all applications that can be dedicated to a user are put on the client. All resources that need to be shared are put on the server. Auditors must ensure that controls are in place on the client as well as on the server and on the network.

Auditors must provide the same level of control assurance in an Internet/Intranet environment as in a client/server environment, with special emphasis on TCP/IP and HTTP.

Question 15

Briefly describe the techniques used to preserve audit trails in a Computer Based Information system. (Final May 2007)

Answer

(a) The following are examples of techniques used to preserve audit trials in a CBIS.

(i) Transaction Logs: Every transaction successfully processed by the system should be recorded on a transaction log, which serves as a journal. There are two reasons for creating a transaction log. First, the transaction log is a permanent record of transactions. Second, not all of the records in the validated transaction file may be successfully processed. Some of these records may fail tests in the subsequent processing stages. A transaction log should contain only successful transaction-those that have changed account balances. Unsuccessful transactions should be placed in an error file. The transaction log and error files combined should account for all the transactions in the batch. The validated transaction file may then be scratched with no loss of data.

(ii) Transaction Listings: The system should produce a (hard-copy) transaction listing of all successful transactions. These listings should go to the appropriate users to facilitate reconciliation with input.

(iii) Log of Automatic Transactions: Some transactions are triggered internally by the system. An example of this is when inventory drops below a preset reorder point, and the system automatically processes a purchase order. To maintain an audit trail of these activities, all internally generated transactions must be placed in a transaction log.

(iv) Listing of Automatic Transactions: To maintain control over automatic transaction processed by the system, the responsible end user should receive a details listing of all internally generated transactions.

(v) Unique Transaction Identifies: Each transaction processed by the system must be uniquely identified with a transaction number. This is the only practical means of tracing a particular transaction through a database of thousands or even millions of records. In systems that use physical source documents, the unique number printed on the documents can be transcribed during data input and used for this purpose. In real-time systems, which do not use source documents, each transaction should be assigned a unique number by the system.

(vi) Error Listing: A listing of all error records should go to the appropriate user to support error correction and resubmission.

(Students are required to discuss any five points)

18

INFORMATION SECURITY

Question 1

What are the core principles of Information Security?

(Final Nov. 2002, Nov. 2003 & May 2005)

Answer

The security objective is supported by many core principles-accountability, awareness, multidisciplinary, cost effectiveness, integration, reassessment, timeliness, and societal factors. The eight core principles of information security are briefly discussed below:

1. Accountability - Responsibility and accountability must be explicit.

   Security of information requires an express and timely apportionment of responsibility and accountability among data owners, process owners, technology providers, and users. This accountability should be formalized and communicated.

   Issues to consider include:

   - Specification of ownership of data and information;
   - Identification of users and others who access the system in a unique manner;
   - Recording of activities through the provision of management audit trails;
   - Assignment of responsibility for maintenance of data and information; and
   - Institution of investigative and remedial procedures when a breach or attempted Breach of the security objective occurs.

2. Awareness - Awareness of risks and security initiatives must be disseminated.

   In order to foster confidence in information, data owners, process owners, technology providers, users, and other parties, with a legitimate interest to learn or be informed, must be able to gain knowledge of the existence and general extent of the risks facing the organization and its systems and the organization's security initiatives and requirements. Security measures are only effective if all involved are aware of their proper functioning and of the risks they address.

   Issues to consider include:

   - Level of detail disclosed must not compromise security;
   - Appropriate knowledge is available to all parties, not just users, who have a legitimate right to be informed;

- Awareness is part of the induction program for new recruits to an organization so as to build security awareness as part of the corporate culture; and
- Recognition that maintaining awareness is an on-going process.

3. Multidisciplinary - Security must be addressed taking into consideration both technological and non-technological issues.

   Security is more than just technology. It also covers administrative, organizational, operational, and legal issues. Accordingly, technical standards should be developed with and, be reinforced by, codes of practice; audit; legislative, legal, and regulatory requirements; and awareness, *education, and training.*

   Issues to consider include:

   - Business value or sensitivity of the information asset;
   - Impact of the organizational and technological changes on the administration of security;
   - Technologies that are available to meet the security objectives;
   - Requirements of legislation and industry norms; and
   - Requirements to carefully manage advanced security techniques.

4. Cost Effectiveness - Security must be cost-effective.

   Different levels and types of security may be required to address the risks to information. Security levels and associated costs must be compatible with the value of the information.

   Issues to consider include:

   - Value to and dependence of the organization on particular information assets;
   - Value of the data or information itself, based on a pre-defined level of confidentiality or sensitivity;
   - Threats to the information, including the severity and probability of such threats;
   - Safeguards that will minimize or eliminate the threats, including the costs of implementing the safeguards;
   - Costs and benefits of incremental increases to the level of security;
   - Safeguards that will provide an optimum balance between the harm arising from a security breach and the costs associated with the safeguards; and
   - Where available and appropriate, the benefit of adopting established minimum security safeguards as a cost-effective alternative to balancing costs and risks.

5. Integration - Security must be coordinated and integrated.

   Measures, practices, and procedures for the security of information should be coordinated and integrated with each other and with other measures, practices, and procedures of the organization, and third parties on whom the organization's business processes depend, so as to create a coherent system of security. This requires that all

levels of the information cycle-gathering, recording, processing, storing, sharing, transmitting, retrieving, and deleting-are covered.

Issues to be considered include:

- Security policy and management included as an integral part of the overall management of the organization;
- Concurrent development of security systems with information systems or, at least, harmonization of all security processes to provide a consistent security framework;
- Review of inter-related systems to ensure that the level of security is compatible; and

Risks relating to third parties on whom the organization's business processes depend.

6. Reassessment: The security of information system should be reassessed periodically, as information systems and the requirements for their security vary over time.
7. Timeliness: Security procedures must provide for monitoring and timely response to real or attempted breaches in security in proportion with the risk. Following issues must be considered:
   - Instantaneous and irrevocable character of business transactions.
   - Volume of information generated from the increasingly interconnected and complex information systems.
   - Automated tools to support real-time and after-the-fact monitoring and
   - Expediency of escalating breaches to the appropriate decision making level.
8. Societal factors: Information and the security of information should be provided and used in such a manner that the rights and interests of others are respected. Level of security must be consistent with the use and flow of information.

Question 2

Explain the role played by an information security administrator. (Final May 2003 & May 2008)

Answer

Role of an Information Security Administrator

An information security administrator is a person who is solely responsible for controlling and coordinating the activities pertaining to all security aspects of the organization.

(i) A security administrator attempts to ensure that the facilities in which systems are developed, implemented, maintained and operated are safe from threats that affect the continuity of installation and or result in loss of security.

(ii) The security administrator sets policy, subject to board approval.

(iii) He also investigates, monitors, advises employees, counsels management on matters pertaining to security.

(iv) The security administrator is responsible for establishing the minimal fixed requirements for classification of information based on the physical, procedural and logical security elements. The need to protect these securities is also stressed. He assigns responsibilities to job classification and formulates what is to be done in case of exceptions.

(v) The security administrator guides other information security administrators and users on the selection and application of security measures. He trains them on how to mark and handle processes, train security coordinators, select software security packages and solve problems.

(vi) Investigates all security violations.

(vii) Advises senior management on matters of information resource control.

(viii) Consults on matters of information security.

(ix) He is responsible of conducting security program, which is a series of ongoing, regular periodic evaluations of the facilities available.

(x) He has to consider an extensive list of possible threats to the organization. Also he prepares an inventory of assets, evaluates the existing controls and implements new controls.

The Information Security Administrator requires assistance from many experts in that particular field. He should see that whether these steps are performed on a regular basis. The results of the reviews are analyzed and documented by him and advices the management on appropriate action in the light of the results.

Question 3

Explain in brief information security and its importance.

(Final May 2004, May 2005 & Nov 2007)

Answer

Information security: Security relates to the protection of valuable assets against loss, disclosure, or damage. Securing valuable assets from threats, sabotage, or natural disaster with physical safeguards such as locks, perimeter fences, and insurance is commonly understood and implemented by most organizations. However, security must be expanded to include logical and other technical safeguards such as user identifiers, passwords, firewalls, etc. which is not understood nearly as well by organizations as physical safeguards. In organizations where a security breach has been experienced, the effectiveness of security policies and procedures has to be reassessed.

This concept of security applies to all information. In this context, the valuable assets are the data or information recorded, processed, stored, shared, transmitted, or retrieved from an electronic medium. The data or information is protected against harm from threats that will lead to its loss, inaccessibility, alteration, or wrongful disclosure. The protection is achieved through a layered series of technological and non-technological safeguards such as physical security measures, user identifiers, passwords, smart cards, biometrics, firewalls, etc.

The objective of information security is "the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity".

For any organization, the security objective is met when

- information systems are available and usable when required (availability),
- data and information are disclosed only to those who have a right to know it (confidentiality),
- data and information are protected against unauthorized modification (integrity).

Importance of Information Security: In a global information society, where information travels through cyberspace on a routine basis, the significance of information is widely accepted. Organizations depend on timely, accurate, complete, valid, consistent, relevant and reliable information. Accordingly, executive management has a responsibility to ensure that the organization provides all users with a secure information systems environment.

Today, there are many direct and indirect risks relating to the information systems. These risks have led to gap between the need to protect systems and the degree of protection applied. This gap is caused by:

- Widespread use of technology;
- Interconnectivity of systems;
- Elimination of distance, time and space as constraints;
- Unevenness of technological changes;
- Devolution of management and control;
- Attractiveness of conducting unconventional electronic attacks over more conventional physical attacks against organizations; and
- External factors such as legislative, legal, and regulatory requirements or technological developments;

Security failures may result in both financial losses and / or intangible losses such as unauthorized disclosure of competitive or sensitive information.

Threats to information system may arise from intentional or unintentional acts and may come from internal or external sources. The threats may emanate from, among others, technical conditions (program bugs, disk crashes), natural disasters (fires, floods), environmental conditions(electrical surges), human factors (lack of training, errors, and omissions), unauthorized access (hacking), or viruses. In addition to these, other threats, such as business dependencies (reliance on third party communications carriers, outsourced operations, etc.) that can potentially result in a loss of management control and oversight are increasing in significance.

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

Question 4

Give an example of an Information Security Policy Statement. *(Final Nov. 2004)*

Answer

The purpose of the information security policy is to protect the organization's information assets from all types of threats, whether internal or external, deliberate or accidental. Information system security is critical to the organisation's survival.

A typical Information Security Policy Statement should ensure that

- Assets will be classified as to the level of protection required;
- Information will be protected against unauthorized access;
- Confidentiality of information will be assured;
- Integrity of information will be maintained;
- Personnel security requirements will be met;
- Physical, logical and environmental security (including communications security) will be maintained;
- Legal, regulatory, and contractual requirements will be met;
- Systems development and maintenance will be performed using a life cycle methodology;
- Business continuity plans will be produced, maintained, and tested;
- Information security awareness training will be provided to all staff;
- All breaches of information system security, actual or suspected, will be reported to, and promptly investigated by Information Systems Security;
- Violations of Information Security Policy will result in penalties or sanctions;
- Standards, practices, and procedures will be produced, and measures implemented to support the Information Security Policy. These may include, but are not limited to, virus protection, passwords, and encryption;
- Business requirements for the availability of information and information systems will be met;
- The roles and responsibilities regarding information security are defined for:
  - Executive management;
  - Information systems security professionals;
  - Data owners;
  - Technology providers;
  - Users;
  - Information systems auditors.
- The Information Systems Security function has direct responsibility for maintaining the Information Security Policy and providing guidance and advice on its implementation;

- All managers are directly responsible for implementing the Information Security Policy within their areas of responsibility, and for adherence by their staff; and
- It is the responsibility of each employee to adhere to the Information Security Policy.

Question 5

Mention any five security management steps an Internet user should take to protect from Cyber crime and computer security threats. *(Final Nov. 2005)*

Answer

The following security management steps may be taken by an Internet user to protect from cyber crimes and other computer security threats:

(i) Use antivirus and firewall software and update it often to keep destructive programmes off the computer.

(ii) Don't allow online merchants to store the credit card information for further purchases.

(iii) Use a hard-to-guess password that contains a mix of numbers and letters and change it frequently.

(iv) Use different passwords for different websites and applications to keep hackers guessing.

(v) Use the most up-to-date version of the web browsers, e-mail software and other programmes.

(vi) Send credit card numbers only to secure sites; look for a padlock or key icon at the bottom of the browser.

(vii) Confirm that the site through which you are doing business is a secure site.

(viii) Use a security programe that gives you control over "cookies" that send information back to website.

(ix) Install firewall software to screen traffic if you use digital subscriber line (DSL) or a cable modem to connect to the Internet.

(x) Don't open e-mail attachments unless you know that the source of the incoming message is trustworthy.

Question 6

What do you mean by Information Security policy? Explain the salient features of the Information Security Policy. *(Final May 2006)*

Answer

Information Security Policy : Security policy defines acceptable behaviours and the reaction of the organisation when such behaviours are violated. The electronic trading, viruses affecting organisation's security documents and the misuse of credit cards have increased and this has augmented the need for security management. Also, legislation relating to information technology is becoming more prolific, with many countries enacting laws on issues such as

copyright and software privacy, intellectual property and personal data. These commercial, competitive and legislative pressures require the implementation of proper security policies.

A good security policy should suggest procedures and policies that can prevent loses and also help in saving money and increasing productivity. The security policy defines ways in which resources in a computer system may be accessed and used. Security policies might differ depending upon the system under consideration.

Features of Information Security Policy: The security objectives and core principles provide a framework for the first critical step for any organization-developing a security policy. The security policy should support and complement existing organizational policies. The thrust of the policy statement must be to recognize the underlying value of, and dependence on, the information within an organization. The information security policy should describe:

- Importance of information security to the organisation
- A statement from the chief executive officer in support of goals and principles of effective information security.
- Specific statements indicating minimum standards and compliance requirements for specific areas.
- Asset classifications.
- Data security
- Personnel security
- Physical, logical and environment security
- Communications security
- Legal, regulatory and contractual security
- System development and maintenance life cycle requirements
- Business continuity planning
- Security awareness, training and education
- Security breach detection and reporting requirements
- Violation enforcement provision
- Definitions of responsibility, accountability for information security and proper separation of duties
- Reporting responsibilities and procedures.

Question 7

Write short note on Restorative Information Protection. *(Final Nov. 2006)*

Answer

Restorative Information Protection: Security events that damage information will happen. If an organization cannot recover or recreate critical information in an acceptable time period, the organization will suffer and possibly have to go out of business.

Planning and operating an effective and timely information backup and recovery program is vital to an operation. It does not simply involve backing up just the valuable information but it frequently also means backing up the system as well, since the information may need services that the system provides to make the information usable.

The key requirement of any restorative information protection plan is that the information can be recovered. There is a common belief that if the backup program has written the information to the backup media, it can be recovered from the backup media. However, there are many variables that can prove that belief wrong.

Some of the questions that any restoratives information protection program must address are:

(i) Has the recovery process been tested recently?

(ii) How long did it take?

(iii) How much productivity was lost?

(iv) Did everything go according to plan?

(v) How much extra time was needed to input the data changes since the last back up?

Question 8

Write short notes on Holistic protection *(Final May 2007)*

Answer

Holistic Protection: Protection must be done holistically and give the organization the appropriate level of security at a cost that is acceptable to the business. One must plan for the unexpected and unknown, expect the worst events to happen, and recover from these events if and when they occur, as though nothing ever happened. Such events cannot be planned, and they always seem to happen at the most inopportune times.

Question 9

Briefly outline the contents of Information Security policy. (*Final May 2007)*

Answer

The Information Security policy should describe:

- The importance of Information security to the organization;
- A statement from the chief executive officer in support of the goals and principles of effective information security;
- Specific statements indicating minimum standards and compliance requirements for specific areas;

- Assets classification;
- Data Security;
- Personnel security;
- Physical, logical and environmental security;
- Communications security;
- Legal, regulatory and contractual requirements;
- System development and maintenance life cycle requirements;
- Business continuity planning;
- Security awareness, training and education;
- Security breach detection and reporting requirements; and violation enforcement provisions;
- Definitions of responsibilities and accountabilities for information security with appropriate separation of duties;
- Particular information system or issue specific areas; and Reporting responsibilities and procedures.

Question 10

Briefly explain the best approach to implement information security policy? *(Final May 2008)*

Answer

To meet the security objective, develop and maintain adequate controls in compliance with generally accepted core principles, an ongoing and integrated approach is necessary. Executive management and especially chief executive officer support is essential for the successful development, design, implementation, and monitoring of security controls.

(i) Security Policies: Every organization should have a security policy that defines acceptable behaviours and the reaction of the organisation when such behaviours are violated.

(ii) Policy Development: The security objectives and core principles provide a framework for the first critical step for any organization developing a security policy. The security policy should support and complement existing organizational policies.

(iii) Roles and Responsibilities: For security to be effective, it is imperative that individual roles, responsibilities and authority are clearly communicated and understood by all.

(iv) Design: Once a policy has been approved by the governing body of the organization and related roles and responsibilities assigned, it is necessary to develop a security and control framework.

(v) Implementation: Once the design of the security standards, measures, practices and procedures has been approved, the solution should be implemented on a timely basis, and then maintained.

(vi) Monitoring: Information systems are subject to a wide range of disruptive incidence. Hence, there is a need to institute monitoring measures and procedures over systems, processes and their environment to promptly identify, contain damage and expedite recovery.

(vii) Awareness, Training and Education: People are often the weakest link in securing information. Awareness of the need to protect information, training in the skills needed to operate them securely, and education in security measures and practices are of critical importance for the success of an organization's security program.

NOTE

19

USE OF SIMPLE CASE TOOLS, ANALYSIS OF FINANCIAL STATEMENTS USING DIGITAL TECHNOLOGY

Question 1

Explain the term CASE tools. Describe briefly various CASE tools. *(Final May 2001)*

Answer

CASE (Computer Aided Software Engineering) refers to the automation of any thing that humans do to develop systems. 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 specification languages.

The various CASE tools are menu generator, screen generator, report generator and code generator.

Menu generators: Menu generators outline the eventual functions or components of systems. When linked to other menus, they illustrate how users can branch to the various screens and sub-screens to be used for data entry or inquiry.

Screen generators: Screen generators for printed reports are used to format or "paint" the desired layouts and contents of a screen without having to enter complex formatting information. Using the data dictionary, the screen generator retrieves output format for data items for editing, and the data item can be easily moved to various screen locations.

Report generator: Report generators are similar to screen generators in that formats are generated in the same fashion. In addition, they can indicate totals, paging, print edits, sequencing and control breaks in creating samples of the desired systems report.

Code generators: Code generators allow the analyst to generate modular units of source code from the high level specifications, and demonstrate the system again. Code generators play an important role in system development process.

Question 2

What are CASE Tools? Describe in-depth the categories of CASE tools with examples.

(Final Nov. 2002, Nov. 2003 & May 2007)

Answer

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

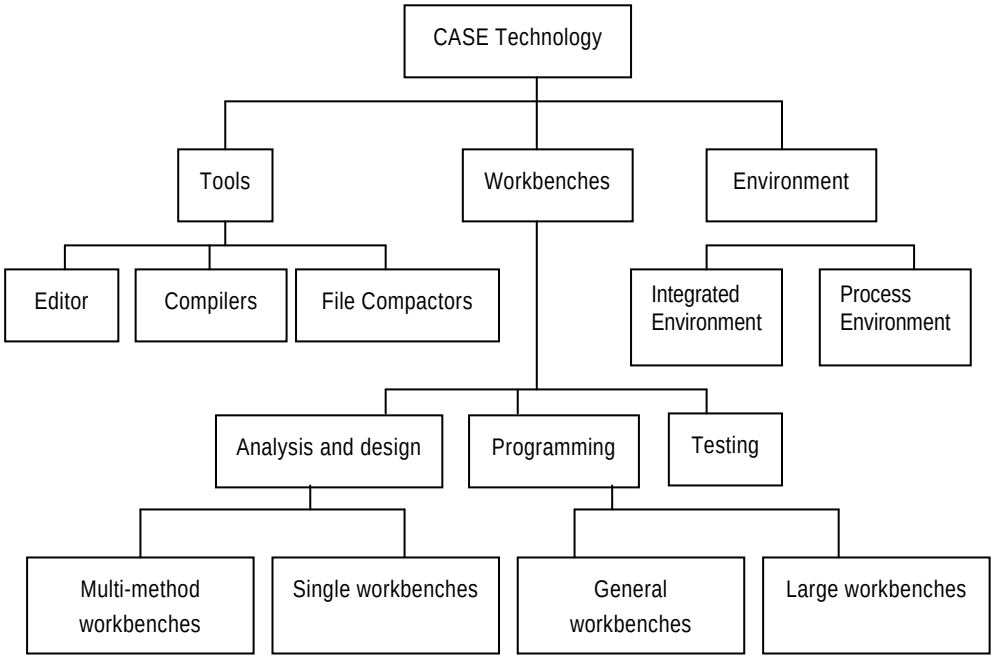
There are three categories of CASE tools:

(i) Tools that support individual process task such as checking the consistency of a design, compiling a program, comparing test results and so on.

(ii) Work benches to support process phases such as specification, design etc. They consist of sets of tools with variable degree of integration.

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

Figure below lists this classification:



Tools, Work benches and Environments

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

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

Question 3

Explain the significance of ratio analysis generally carried out for financial analysis.

(Final May 2004)

Answer

Significance of Ratio Analysis: The financial planning for an enterprise is carried out by suitably examining and analyzing the financial data centrally available. Based on these data, corrective actions are taken on future processes for onward progress and development.

One important benefit of having an up-to-date accounting system with a flexible reporting facility on a powerful computer is the speed with which complex business calculations can be provided with the information necessary to ensure that they are valid. A frequently used outcome of business calculations is the ratio analysis – a comparison between two numerical values obtained by dividing one by the other.

A ratio that compares one production period with another can be a useful indicator to guide internal management. The financial position of the company can be compared with that of a rival company by means of one or more ratios. Ratios between individual company performance and consolidated financial statement amounts can be used to explain or amplify the annual report.

Facilities are available to define the same mathematical procedure for all these ratios and calculations, but the actual variables and data depend on the purpose and the version number of the ratio calculation specified when the result is called. Suppose the ratio calculations are defined in two stages. The specifications required are:

- specifying where information is to come from,
- specifying how the information is to take part in the calculation.

There are certain financial ratios, which help financial personnel make better use of financial information for planning and control. These ratios can be broadly classified into three main areas. They are:

(i) Profitability ratios.

(ii) Liquidity ratios

(iii) Efficiency or Activity ratios.

Question 4

Explain briefly the Profitability ratio. *(Final May 2004)*

Answer

Profitability Ratios: These ratios help in assessing the adequacy of profits earned by the company and also in finding out whether profitability is increasing or declining. The profitability ratios show the combined effects of liquidity, asset management and debt management on operating results. They are measured with reference to sales, capital employed, total assets employed, shareholders funds, etc. The major profitability ratios are:

(i) *Return on Capital Employed (ROCE) or Return on Investment (ROI):* This ratio provides a strong incentive for optimal utilization of the assets of the company.

$$\text{ROI} = \frac{\text{Net Profit}}{\text{Capital employed}} \times 100$$

(ii) *Earnings Per Share (EPS):* It is one of the important measures of economic performance of a corporate entity.

$$\text{EPS} = \frac{\text{Net Profit after tax and preference dividend}}{\text{Number of equity shares}}$$

(iii) *Gross Profit Margin:* This ratio measures the efficiency of the company's operations.

$$\text{Gross Profit Margin} = \frac{\text{Gross profit}}{\text{Sales}} \times 100$$

(iv) *Net Profit Margin:* This ratio focuses on the net profit margin arising from business operations before interest and tax is deducted. It measures the efficiency of operation of the company.

$$\text{Net Profit Margin} = \frac{\text{Net Profit before interest and tax}}{\text{Sales}} \times 100$$

(iv) *Return on Assets (ROA):* This ratio indicates the efficiency of utilization of assets in generating revenue.

$$\text{ROA} = \frac{\text{Net Profit after tax}}{\text{Total assets}} \times 100$$

(vi) *Return on Net Worth:* This ratio is an important yardstick of performance for equity shareholders since it indicates the return on the funds employed by them.

$$\text{Return on Net Worth} = \frac{\text{Net Profit after interest and tax}}{\text{Net worth}} \times 100$$

(vii) *Price Earnings (P/E) Ratio:* It measures investor's expectations and the market appraisal of the performance of a firm.

$$\text{P / E ratio} = \frac{\text{Market price of share}}{\text{EPS}}$$

(viii) *Expenses Ratio:* It is very important for analyzing the profitability of a firm.

$$\text{Expenses Ratio} = \frac{\text{Expenses}}{\text{Sales}}$$

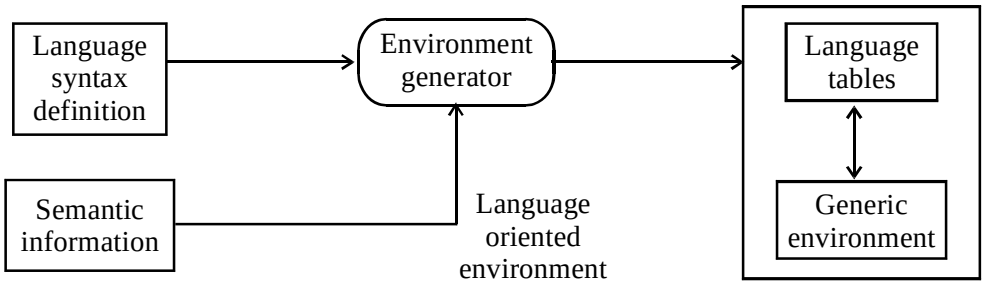
Question 5

Write a short note on Meta- CASE Workbenches. *(Final May 2003)*

Answer

Meta CASE Workbenches: Meta-CASE workbenches are CASE tools, which are used to generate other CASE tools. They are based on a description of the rules and notifications of design or analysis methods. The general principle will be based on the diagram given below:

Environment generator for Meta CASE tools



There are five different aspects, which are to be considered in Meta-CASE workbench.

(i) A data model for data capture and output generation.

(ii) A frame model, which defines the views of the data model to be generated. Each possible view of the data model is termed as frame. Links between frames, which allow navigation from one representation to another are defined in the model.

(iii) Diagrammatic rotation for each diagram frame.

(iv) Textual presentation for each text frame.

Report structures.

Question 6

What are called Work benches ? Describe the various tools used in programming work bench. *(Final May 2005)*

Answer

CASE Work Benches - CASE work benches are used to support process phases such as specification, design etc. They consist of sets of tools with variable degree of integration. There are many types of work benches to support most software process activities, for example, software development work benches, cross development work benches, configuration management, documentation and project management work benches.

The programming work bench is made up of a set of tools to support the process of program development. Some of these tools, which are part of a programming workbench, are:

(i) Language Compiler – It translates host programs to object code. As part of a translation process, an abstract syntax tree and a symbol table is created.

(ii) Structured editor – It incorporates embedded programming language knowledge and edits the syntax representation of the program in the AST rather than its source code text.

(iii) Linker – It is used to link the object code programme with components, which have already been compiled.

(iv) Loader – It loads the executable program into the computer memory prior to execution.

(v) Cross-referencer – It produces a cross-reference listing showing where all program names are declared and used.

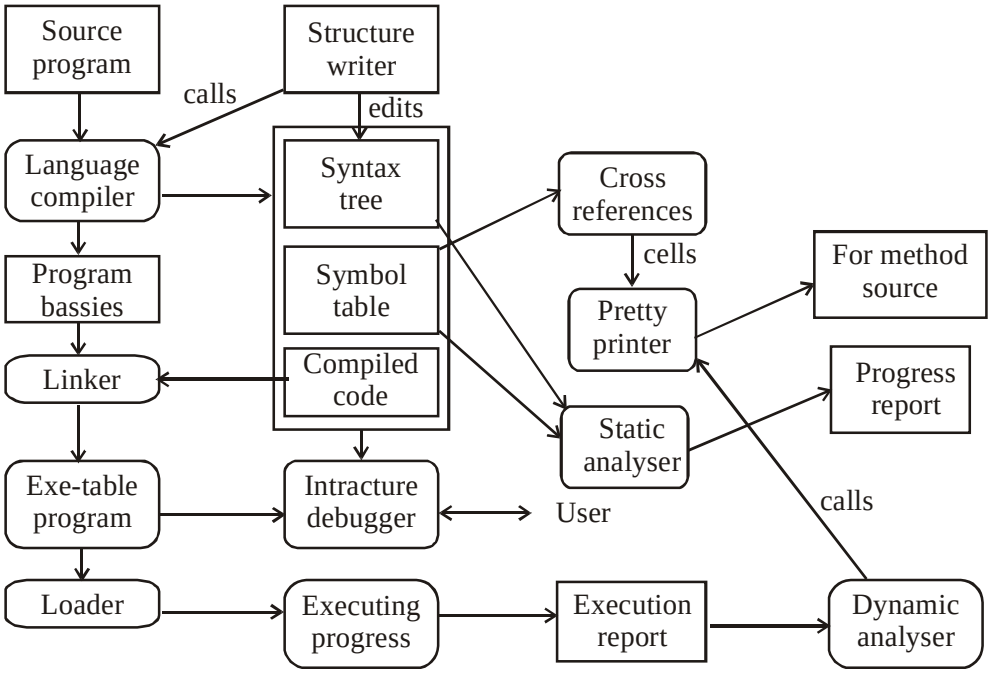
(vi) Pretty Printer – It scans the AST and prints the source program according to embedded formatting rules.

(vii) Static Analyser - It analyses the source code to discover anomalies such as uninitialized variables, unreachable code, uncalled functions and procedures.

(viii) Dynamic Analyser – It produces a source code listing annotated with the number of times each statement was executed when the program was run. It may also generate information on program branches and loops and statistics of processor usage.

(ix) Interactive debugger – It allows the user to control the execution sequence and view the program state as execution progresses.

A typical programming work bench is shown below:



Question 7

Describe briefly five components of a CASE work bench. *(Final May 2006)*

Answer

Components of A CASE Workbench:

(1) *A diagram editing system* that is used to create data flow diagrams, structure charts, entity relationship diagrams etc. It captures information about these entities and saves this information in a central responsibility.

(2) *Design analysis and checking facilities* that process the design and correct errors. These are integrated with the editing system so that the users may be informed of errors during diagram creation.

(3) *Query language facilities* that allow the user to browse the stored information and examine completed designs.

(4) *Data dictionary* that maintains information about named entities in a system design.

(5) *Report generation facilities* that take information from the central store and automatically generate system documentation.

(6) *Forms generation tools* that allow screen and document formats to be specified.

(7) *Import/export facilities* that allow interchange of information from the central repository with other development tools.

(8) *Some systems support skeleton code generation* which generates codes or code segments automatically from the design captured in the central store.

Question 8

What are the five different levels of integration of CASE tools? *(Final Nov. 2006)*

Answer

There are five different levels of integration of CASE tools as stated below:

(1) Platform integration: Here the tools to be implemented run on the same platform where platform means either a single computer/operating system or a network of system.

(2) Data integration: It is the process of exchange of data by CASE tools. The result from one tool can be passed on as input to other tools.

(3) Presentation integration: It means that the tools in the system use a common metaphor or style and a set of common standards for user interaction.

(4) Control Integration: It is the mechanism of one tool in a workbench or environment to control the activation of other tools in the CASE system.

(5) Process integration: This means that the CASE system has embedded knowledge about the process activities, their phasing, their constraints and the tools needed to support their activities.

Question 9

Explain with the help of a diagram the various tools which are included in a testing workbench.

(Final Nov 2007 & Nov 2008)

Answer

Testing workbenches are open systems which evolve to suit the needs of the system being tested. The tools which might be included in a testing work benches are:

(i) *Test Manager*: It manages the running and reporting of program tests. This involves keeping track of test data, expected results, program facilities tested and so on.

(ii) *Test data generator*: It generates test data for the program to be tested. This may be accomplished by selecting data from a database or by using patterns to generate random data of the correct form.

(iii) *Oracle*: It generates predictions of expected results.

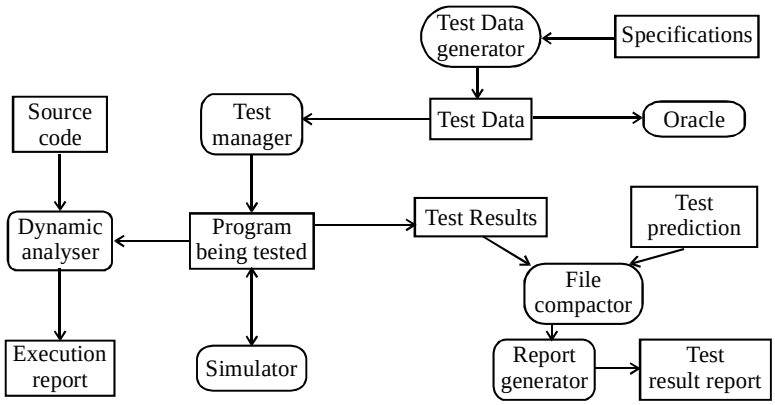
(iv) *File compactor*: It compares the results of program tests with previous test results and reports differences between them.

(v) *Report generator*: It provides report definition and generation facilities for test results.

(vi) *Dynamic analyzer*: It adds code to a program to count the number of times each statement has been executed.

(vii) *Simulators*: Different kinds of simulators such as target simulators, user interface simulators, I/O simulators are available for simulation.

A typical testing layout is shown below:



Question 10

Write short notes on the following:

Process Integration. *(Final Nov. 2007)*

Answer

Process integration: It means that the CASE system has embedded knowledge about the process activities, their phasing, their constraints and the tools needed to support their activities. The CASE system participates in the scheduling of these activities and in checking that the required activity reference is maintained. Process integration requires that the CASE system maintains a mould of the software process and uses this mould to drive the process activities. In a sense, activities and deliverable are identified, a coordination strategy defined and the tools required to support activities are specified. All of this is embedded in the mould and a process interpreter then extracts this mould to drive the software process.

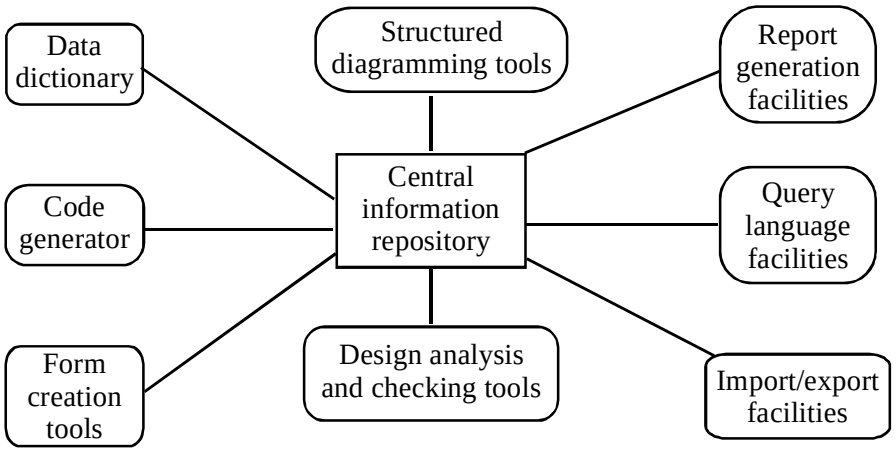
Question 11

Briefly explain the components of an analysis and design work bench.

(Final Nov 2005 & May 2008)

Answer

Analysis and design work benches are designed to support the analysis and design stages of the software process where models of the system are created. A typical model is shown in the figure below:



The components of this model are:

(i) *Diagram editors* to create data flow diagrams, structured charts, entity relationship diagram and so on.

(ii) *Design analysis and checking tools* which process the design and then submit report o=n errors and anomalies. These are integrated with editing system so that user errors are trapped at an early stage in the process.

(iii) *Repository query languages* which allow the designer to find the designs and associate design information in the repository.

(iv) *A data dictionary* which maintains precise and unambiguous information about all data elements used in a system design.

(v) *Report definition and generation* tools which take information from the central store and automatically generate system documentation.

(vi) *Forms definition tools* which allow screen and document formats to be specified.

(vii) *Import-export facilities* which allow the interchange of information from the central repository with other development tools.

(viii) *Code generators* which generate code or code skeletons automatically from the design captured in the central store.