

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

Question No. 1 is compulsory. Answer any four questions
from remaining six questions.

Question 1

- (a) While performing an IS audit, the auditors should ascertain that various objectives are properly met. Briefly describe them. (5 Marks)
- (b) What are the duties of certifying authorities in respect of digital signature? (5 Marks)
- (c) Discuss any five benefits which are attained by implementing a computerised model for making decision. (5 Marks)
- (d) Briefly explain the various fact finding techniques which are used by the system analyst for determining the needs of an organization. (5 Marks)

Answer

- (a) The purpose of an IS audit is to review and evaluate the internal controls that protect the system. While performing an IS audit, auditors must ascertain that following objectives are met:
 - (i) Security provisions protect computer equipment, programs, communications and data from unauthorized access, modification or destruction.
 - (ii) Program development and acquisition is performed in accordance with management's general and specific authorisation.
 - (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 handled according to prescribed policies of management.
 - (vi) Computer data files are accurate, complete and confidential.
- (b) (i) Section [30] of Information Technology Act provides that every Certifying Authority shall follow certain procedures in respect of Digital Signature as given below:
 - (a) make use of hardware, software and procedures that are secure from intrusion and misuse;
 - (b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions.
 - (c) adhere to security procedures to ensure that secrecy and privacy of the Digital Signatures are assured and
 - (d) observe such other standards as may be specified by regulations.

- (ii) Every Certifying Authority shall also ensure that every person employed by him complies with the provisions of the act, or rules, regulations or orders made thereunder.
 - (iii) A Certifying Authority must display its licence at a conspicuous place of the premises in which it carries on its business and a Certifying Authority whose licence is suspended or revoked shall immediately surrender the licence to the controller.
 - (iv) Section 34 further provides that every Certifying Authority shall disclose its Digital Signature Certificate which contains the public key corresponding to this private key used by that Certifying Authority and other relevant facts.
- (c) 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.
- (d) Various facts finding techniques used by system analyst for determining the needs of an organization are discussed below:
- (i) Documents: Documents refer to manuals, input forms, output forms, diagrams of how the current system works, organization charts showing hierarchy of users and managers' responsibilities, job descriptions of the people who work with the current system, procedure manuals and program codes. Documents are good source of user needs and the current system.
 - (ii) Questionnaires: Users and managers are asked to complete questionnaire about the information system when the traditional system development approach is chosen. Large amount of data can be collected through properly designed questionnaire. Responses can be analysed rapidly with the help of a computer.

- (iii) Interviews: Users and managers are also interviewed to extract information in depth. The data gathered through interviews provide system developer a complete picture of the problems and opportunities. Interviewers are also useful to note user reaction first hand and probe for further information.
- (iv) Observation: Observation plays an important role in requirement analysis. Only by observing how users react to prototype of a new system, the system can be successfully developed. The analyst should visit the user site to watch how the work is taking place. Such visits often help the analyst in getting a clear picture of the users' environment and to determine why a request for a new system was submitted.

Question 2

- (a) What is "Information Security"? Why is it important in any organization? Explain briefly (10 Marks)
- (b) System analysts develop various categories of information systems to meet a variety of business needs. Discuss any three such systems briefly. (10 Marks)

Answer

- (a) Security refers to the protection of valuable assets against loss, disclosure or damage. "Information Security" covers all information. In this context, the valuable assets are the data or information recorded, processed, stored, shared, transmitted or retrieved from an electronic medium. It is protected against harm from threats leading to its loss, damage, inaccessibility, integrity or unauthorized disclosure. The protection of this unbreakable assets is achieved by deploying a layered series of technological and non-technological safeguards such as physical security measures, user identifiers, passwords, smart cards, biometrics, anti-virus, firewalls etc.

In a global information society, where information travels through cyberspace on a routine basis, the significance of information is widely accepted. In addition, information and the information system and communication that deliver the information are truly pervasive throughout organization – from the user's platform to local and wide area networks to servers to main frame computers. Organisations 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. It is clear that there are not only many direct and indirect benefits from the use of information systems, there are also many risks (direct and indirect) relating to information systems. Most risks have led to a gap between the need to protect systems and the degree of protection applied. This gap is caused by various factors such as (i) widespread use of technology, (ii) interconnectivity of systems, (iii) elimination of distance, time and space etc. (iv) unevenness of technological changes, (v) Devolution of management and control, (vi) Attractiveness of conducting unconventional electronic attacks over more conventional physical attacks against organizations, and (vii) External factors such as legislative, legal, and regulatory requirements or technological developments.

Threats to information systems may arise from intentional or unintentional acts and many 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, human factors, unauthorized access or viruses.

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 failure. That is why, the organisations have started giving more and more importance towards information security.

- (b) 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.

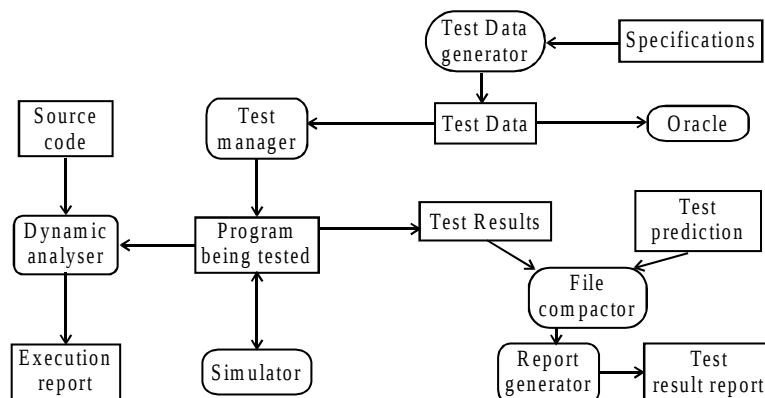
Question 3

- (a) Explain with the help of a diagram the various tools which are included in a testing workbench. (10 Marks)
- (b) What do you understand by Material Inventory Control System? Draw the information flow diagram for designing computerized material inventory control system. (10 Marks)

Answer

- (a) 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:
- 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.
 - 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.
 - Oracle:** It generates predictions of expected results.
 - File compactor:** It compares the results of program tests with previous test results and reports differences between them.
 - Report generator:** It provides report definition and generation facilities for test results.
 - Dynamic analyzer:** It adds code to a program to count the number of times each statement has been executed.
 - Simulators:** Different kinds of simulators such as target simulators, user interface simulators, I/O simulators are available for simulation.

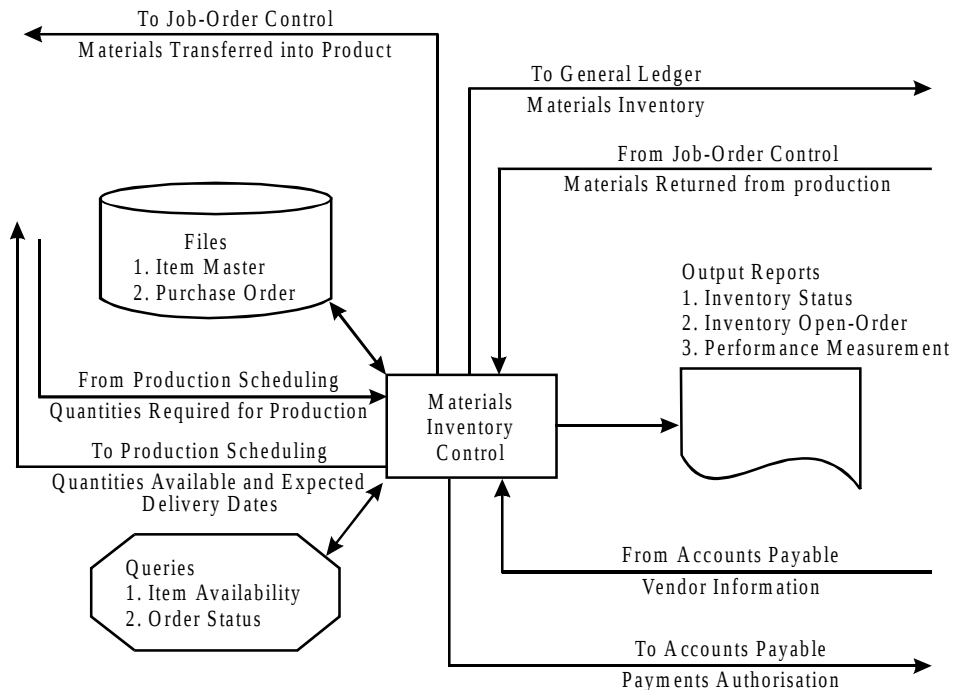
A typical testing layout is shown below:



- (b) The materials inventory control system is the point at which materials enter the manufacturing accounting systems. This system controls inventory and minimizes the costs of purchasing and holding of inventory shortage. Therefore, it needs the following information to function:

- ◆ The timing of purchases.
- ◆ Whether materials received meet specifications and have been properly costed.
- ◆ The status of inventory on hand.
- ◆ The status of unfilled orders.
- ◆ Anticipated demand.

The figure given below depicts the flow of information to and from the materials inventory system. One of the major functions is to maintain a subsidiary ledger with accounts for each item in the inventory. This ledger should balance in total to the materials inventory control account contained in the general ledger.



Question 4

- (a) Explain briefly various activities that should be completed for successful conversion of an existing system to the new information system. (10 Marks)
- (b) Discuss the various activities which are part of the system development life cycle. (5 Marks)

- (c) State the standards that should be followed while designing graphical output. (5 Marks)

Answer

- (a) Various activities which should be completed for successful conversion of an existing system to the new information system are classified as follows:

- (i) Procedure conversion
- (ii) File conversion
- (iii) System conversion
- (iv) Scheduling personnel and equipment
- (v) Alternative plans in cast of equipment failure.

These are discussed briefly below:

- (i) 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, output 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. Once the new system is completely operational, the system implementation group should discuss with all supervisory personnel about their respective areas. As with every new installation, minor adjustments should be expected. All supervisory personnel should freely discuss with the systems development team members so that necessary changes can be initiated as conditions change. Thus proper machinery for making changes must be put in place.
- (ii) 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 or off-line files. If the existing system is operating on a computer but of different configuration, the formats of the present computer files are generally unacceptable for the new system. Besides the need to provide a compatible format, there are several other reasons for file conversion. Data may be required to put on magnetic disk or other mass storage device to construct an on-line common database.
- (iii) 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 database 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 the systems. The old system can be dropped as soon as the data processing group is satisfied with new system's performance.

- (iv) **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, the job becomes more routine. Before the newly designed project is complete, it is often necessary to schedule the new equipment. Schedules should be set up by the system manager in conjunction with departmental managers of operational units serviced by the equipment. The master schedule for next month should provide sufficient computer time to handle all required processing. Just as the equipment must be scheduled for its maximum utilization, so must be personnel who operate the equipment. It is essential that each person follow the methods and procedures set forth by the MIS section.
 - (v) **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 which are 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 organisation's systems and procedures manual.
- (b) The system development life cycle consists of the following activities:
- (i) Preliminary investigation
 - (ii) Requirement analysis or systems analysis
 - (iii) Design of the system
 - (iv) Development of software
 - (v) Systems testing
 - (vi) Implementation and maintenance.

Each of these activities is discussed below briefly:

- (i) **Preliminary investigation:** A preliminary investigation 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) **Requirement analysis or systems analysis:** If, after studying the results of preliminary investigation, management decides to continue the development process, the needs of the users are studied. Analysts work closely with employees and managers of the organization for determining information requirements of the users. After gathering the details of information through several fact finding

techniques and tools, 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. This step is also referred to as "systems analysis".

- (iii) Design of the system: During system design, the user requirements that arise from analyzing the user applications environment are incorporated into a new system design. The design of an information system produces the details that state how a system will meet the requirements identified above. The analyst designs various reports, data entry procedures, inputs, files and database.
 - (iv) Development of software: After the system design details are resolved, such resources needs as specific type of hardware, software and services are determined. Subsequently, choices are made regarding which products to buy or lease from which vendors. Software can be purchased from this market or it can be developed within the organization also. The choice depends on many factors such as time, cost and availability of programs.
 - (v) Systems testing: Before the information system is finally used, it must be tested. Systems testing is done experimentally to ensure that the software does not fail i.e. it will run according to its specifications and in the way users expect. Special test data are input for processing and results examined. If it is found satisfactory, it is eventually tested with actual data from the current system.
 - (vi) Implementation and maintenance: After the system is found to be fit, it is implemented with the actual data. Hardware is installed and users are trained on the new system. The results of the development efforts are reviewed to ensure that the new system satisfies users requirements. After implementation, the system is maintained; it is modified to adapt to changing users' and business needs so that the system can be useful to the organization for a longer period.
- (c) 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.

Question 5

- (a) Briefly discuss any five program design tools. (10 Marks)
- (b) State and explain the four back up and recovery features necessary in a DBMS.(5 Marks)
- (c) Briefly explain five categories of Computer frauds based on the data processing model. (5 Marks)

Answer

- (a) Five program design tools are discussed below:
 - (i) Program Flow Chart: Program flow chart is among the most common program design tools. Flow chart depicts the logical steps through which a computer program must proceed when solving a problem. Often it does not provide a broad view of how the program is organized. Also, sometimes it is difficult for programmers to translate a program flow chart directly into a structured code.
 - (ii) Pseudo Code: When reviewing the work done by a program designer, users may also need to review narrative descriptions of a program logic. Pseudo-code, 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. Pseudo-code is generally preferred by programmers over flow charts because it represents program code more closely. Many users also find pseudo code more understandable than program flow charts. Pseudo-code is particularly useful when designing transaction processing and information – retrieval programs.
 - (iii) Structure Chart: Structure Chart which looks similar to corporate organization chart is useful for organising problems. The structure chart organizes each of the program tasks into well-defined modules. The higher level modules represent control portion of the program; the lowest level modules do the actual task of the program. It does not give any detail of the actual program logic and the order in which various tasks are performed. Instead they show how all the logical functions of the program fit together as a whole.
 - (iv) 4GL Tools: Fourth generation languages provide a way out to remove the obstacles of the above three design 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.
 - (v) 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. It results in a model that describes objects, classes and their relationships to one another. It is often taken from DFD. In fact, every input and output screen, every process and data store found in a fully decomposed DFD may be a candidate of an object in an object – oriented design.

- (b) 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.
- (c) 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 6

- (a) What is Enterprise Resource Planning? Briefly describe its benefits. (10 Marks)
- (b) State the steps involved in selection of a Computer System. (5 Marks)
- (c) Briefly explain the principles to guide the design of measures and indicators to be included in EIS. (5 Marks)

Answer

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

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.

(b) 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.

(c) 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 7

Write short notes on the following:

- (a) Objectives of Information Technology Act, 2000.
- (b) Review areas of an IS Auditor.
- (c) Process Integration.
- (d) End user development approach in system development. (4 × 5 = 20 Marks)

Answer

- (a) Objectives of Information Technology Act, 2000 are:
 - (1) To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication in place of paper based communication methods.
 - (2) To give legal recognition to Digital Signature for authentication of any information or matter which requires authentication under any law.
 - (3) To facilitate electronic filing of documents with Government departments.
 - (4) To facilitate electronic storage of data.
 - (5) To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions.
 - (6) To give legal recognition for keeping books of account by bankers in electronic form.
 - (7) To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934.
- (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.
- (c) 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.
- (d) 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.