

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

Question No. 1 is compulsory.

Answer **any four** questions from the remaining **six** questions.

Question 1

- (a) Discuss various factors that render manual audit method ineffective in IS audit. (5 Marks)
- (b) Briefly describe the various objectives to be met while performing an IS audit. (5 Marks)
- (c) "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? (5 Marks)
- (d) Mention any five security management steps an Internet user should take to protect from Cyber crime and computer security threats. (5 Marks)

Answer

- (a) 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.
- (b) 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 authorised is identified and handled according to prescribed managerial policies.

(vi) Computer data files are accurate, complete, and confidential.

(c) 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.

(d) 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 programme 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.

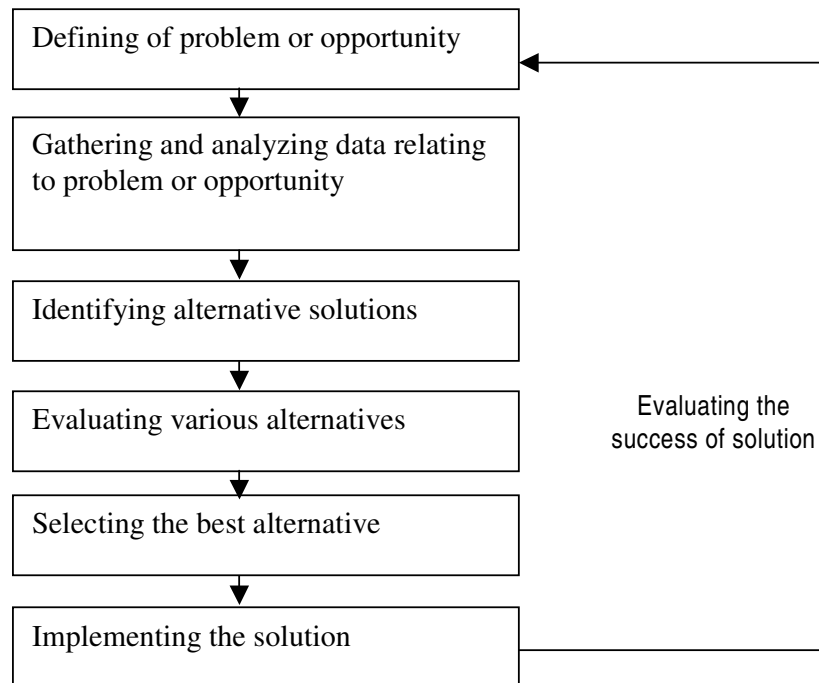
Question 2

- (a) *How system approach can be used for solving problems ?* (10 Marks)
 (b) *Define the term system stress and system change.* (5 Marks)
 (c) *What are the fact finding techniques used by a system analyst ?* (5 Marks)

Answer

- (a) 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.
- (b) 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.

- (c) **Fact Finding Techniques:** Various fact-finding techniques which are used by the system analyst for determining users' needs are discussed below:
- (i) **Documents:** Document means manuals, input forms, output forms, diagrams of how the current system works, organization charts showing hierarchy of users and manager responsibilities, job descriptions for the people who work with the current system, procedure manuals, program codes for the applications associated with the current system etc. Documents are a very good source of information about user needs and the current system. They are easy to collect, convey a lot of information and provide relatively objective data. The analyst should ensure that the documents which he is collecting are current, accurate and contain up-to-date information.
 - (ii) **Questionnaires:** Users and managers are asked to complete questionnaire about the information system when the traditional system development approach is chosen. The main strength of questionnaires is that a large amount of data can be collected through a variety of users quickly. Also, if the questionnaire is skillfully drafted, responses can be analysed rapidly with the help of a computer.
 - (iii) **Interviews:** Users and managers may also be interviewed to extract information in depth. The data gathered through interviews often provide systems developer with a complete picture of the problems and opportunities. Interviews also give analyst the opportunity to note user reaction first-hand and to probe for further information.
 - (iv) **Observation:** In prototyping approaches, observation plays a central role in requirement analysis. Only by observing how users react to prototype of a new system, the system can be successfully developed. In traditional approach, the analyst should visit the user site to watch how the work was taking place. Such a surprise visit often helps the analyst in getting a clear picture of the user's environment and to determine why a request for a new system was submitted.

Question 3

- (a) *What is an Executive Information system ? Discuss its various purposes. (10 Marks)*
- (b) *Discuss various issues that should be considered while designing systems input. (10 Marks)*

Answer

- (a) 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 managers 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 organisation, 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 manager obtains the answer to a question, that answer typically sparks other related questions in the manager'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.

- (b) 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.

- (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 the new system often means new information and new information often requires new sources of data. Some times, 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. Timely input of data is very important in transaction processing 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 are available in the market such as workstations, magnetic disc, OCR, 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 must be defined. Designing input formats 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 anyone 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

- (a) *Discuss various stages through which an in-house creation of program has to pass.* (10 Marks)
- (b) *What are the benefits achieved by implementing the ERP packages ?* (10 Marks)

Answer

- (a) An in-house creation of programs commonly involves the following six stages:
- (i) **Program analysis:** In this stage, the programmer ascertains for a particular application (e.g. up-dating of the stock file) the outputs required (i.e. the updated stock file, listing of replenishment orders etc.), the inputs available (i.e. the stock master file, the receipts and issues transactions file) and the processing (i.e. updating the physical balance, computing stock value for various items et.). The programmer then determines whether the proposed application should be programmed at all. It may be possible that the proposal is shelves for modification 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 layouts and flowcharts etc. are provided to the programmer by the systems analyst.
 - (iii) **Program coding:** The logic of the program outlined on the flowcharts is converted into program statements or instructions at this stage. For each language, there are specific rules concerning format and syntax. It is highly desirable that the programs are simple to understand. Each coded instruction is then entered on to a magnetic media. These coded instructions known as source programs are then translated into a machine language by an interpreter or a compiler. These translators have diagnostic capabilities i.e., they point out the syntax errors in the program.
 - (iv) **Debug the program:** The process of debugging a programme refers to correcting programming 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 programmer into machine language instructions. Once the programmer gets a clean compile, the program is ready for execution. Thereafter, a careful and thorough testing of program is done using structured walk throughs. A careful and thorough testing of each program is imperative to the successful installation of any system. The programmer should plan the testing to be performed including all possible exceptions. A long of test results and all conditions successfully tested should be kept.
 - (v) **Program documentation:** The writing of narrative procedures and instructions for people who will use software is done throughout the program life cycle. Managers and users should carefully review documentation in order to ensure that the software and the system behave as the documentation indicates. If they do not,

documentation should be revised. User documentation should also be reviewed for understandability.

- (vi) **Programme maintenance:** The requirements of business data processing applications are subject to continual change. This calls for modification of the various programmes. There are, usually separate categories of programmers called maintenance programmers who are entrusted with this task. There is a difficult task of understanding and then revising the programmes they did not write. This should bring out the necessity of writing simple programs which could be easily understood.

These six stages are known as the program development life cycle.

- (b) The benefits accruing to any business enterprise by implementing an ERP are unlimited. Following are some of the benefits achieved by implementing the ERP package:
 - (i) 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.
 - (ii) Reduces paper documents by providing on-line formats for quickly entering and retrieving information.
 - (iii) Improves timeliness of information by permitting posting daily instead of monthly.
 - (iv) Greater accuracy of information with detailed content, better presentation satisfactory for the auditors.
 - (v) Improved cost control.
 - (vi) Faster response and follow-up on customers.
 - (vii) More efficient cash collection, say, material reduction in delay in payments by customers.
 - (viii) Better monitoring and quicker resolution of queries.
 - (ix) Enables quick response to changes in business operations and market conditions.
 - (x) Helps to achieve competitive advantage by improving its business processes.
 - (xi) Improves supply-demand linkage with remote locations and branches in different countries.
 - (xii) Provides a unified customer database usable by all applications.
 - (xiii) Improves international operations by supporting a variety of tax structures, invoicing schemes, multiple currencies, multiple period accounting and languages.
 - (xiv) Improves information access and management throughout the enterprise.
 - (xv) Provides solution for problems like Y2K and Single Monetary Unit or Euro Currency.

Question 5

- (a) *What kind of controls can be incorporated in the system to make frauds difficult to perpetrate ?* (10 Marks)

- (b) *Discuss various ways in which audit trail can be used to support security objectives ?*
(5 Marks)
- (c) *Explain the importance of source documents and associated control techniques.*
(5 Marks)

Answer

- (a) 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 authorised 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.
- (b) Audit trails can be used to support security objectives in three ways:
 - (i) **Detecting unauthorized access to the system:** Detecting unauthorised 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 unauthorised 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 used to reconstruct accounting data files that were corrupted by a system failure.
 - (iii) **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.
- (c) 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 6

- (a) *What are the various Tangible and Intangible benefits that can result from the development of a computerised system ?* (10 Marks)
- (b) *What are the advantages of using pre-written application packages?* (5 Marks)
- (c) *What are the duties of certifying authorities with respect to digital signature ?* (5 Marks)

Answer

- (a) 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.

(b) Advantages of using pre-written application packages:

The four most compelling advantages of using pre-written application packages are summarised below:

- (i) **Rapid implementation:** Application packages are readily available to implement after they are purchased. In contrast, software developed in-house may take months or even years until it is ready for implementation.
- (ii) **Low risk:** Since the application package is available in the finished form, the organisation knows what it is going to get for the price it has paid. With in-house developed software, the long development time breeds uncertainty with regard to both the quality of the final product and its final cost.
- (iii) **Quality:** The firms engaged in application package developments are typically specialist in their products' niche area. Generally, they have a lot of experience in their specialised application field and hence can provide better software. In contrast, in-house programs often have to work over a wide range of application areas; they may not be possessing expertise for undertaking proposed software development.
- (iv) **Cost:** Software vendors can leverage the cost of developing a product by selling the product to several other firms, thereby realising a lower cost from each application user. Thus, an application package generally costs less than an in-house developed package. In addition, many hidden costs are faced by organisations that want to develop applications in-house. Hence, application packages, sometimes, turn out to be cheaper compared to in-house developed software.

(c) Duties of Certifying Authorities: [Section 30]

- (i) This section provides that every Certifying Authority shall follow certain procedures in respect of Digital Signatures as given below:
 - (a) make use of hardware, software and procedures that are secure from intrusion and misuse;

- (b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;
- (c) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured and
- (d) observe such other standards as may be specified by regulations.
- (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 the private key used by that Certifying Authority and other relevant facts.

Question 7.

Write short notes on the following:

- (a) *Server-centric model*
- (b) *Analysis and design work bench*
- (c) *Business Engineering*
- (d) *System maintenance.* (4×5 = 20 Marks)

Answer

- (a) **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.

- (b) **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. The components of this model are:
- (i) Diagram editors to create DFD, structured chart, etc.

- (ii) Design, analysis and checking tools which process the design and then submit reports on errors and anomalies.
 - (iii) Repository query languages which allow the designer to find designs and associate design information in the repository.
 - (iv) A data dictionary which maintains information about entities used in a system design.
 - (v) Report definition and general tools which generate system documentation after taking information from store.
 - (vi) Forms definition tools which allow screen and document formats to be specified.
 - (vii) Import / Export facilities.
 - (viii) Code generators which generate code from the design captured in central store.
- (c) **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.
- (d) **System Maintenance:** Most information systems require at least some modification after development. The need for modification arises from a failure to anticipate all requirements during system design and/or from changing organisational requirements. The changing organizational requirements continue to impact most information systems as long as they are in operation. Consequently periodic systems maintenance is required for most of the information systems. Systems maintenance involves adding new data elements, modifying reports, adding new report, changing calculation etc.
- Maintenance can be categorized in the following two ways:
- (i) Scheduled maintenance is anticipated and can be planned for. For example, the implementation of a new inventory coding scheme can be planned in advance.
 - (ii) Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate solution. A system that is properly developed and tested should have few occasions of rescue maintenance.