Question 1.

(a) What are the different categories of Information systems? Explain each one of them briefly. (10 marks)

(b) What are the duties of certifying authorities in respect of digital signature? (5 marks)

(c) While performing an I.S. Audit, the auditors should ascertain that various I.S. Audit objectives are met. Discuss them briefly. (5 marks)

Answer

(a) There are five types of information systems to meet variety of business needs, as stated below:

(i) Management Information Systems,
(ii) Transaction Processing Systems,
(iii) Decision Support Systems,
(iv) Executive Information Systems, and
(v) Expert Systems.

Each of these is briefly discussed below:

Management Information Systems: Management Information Systems (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 organisation, 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.

Transaction Processing Systems: The most fundamental computer-based system in an organisation pertains to the processing of business transactions. Transaction processing 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. The high volume of well-understood transactions associated with the operating level of an organisation, as well as the ability for managers to develop specific procedures for handling them often trigger the need for computer assistance. Transaction processing systems, if computerized, provide speed and accuracy and can be programmed to follow routines without any variance. Systems Analysts design the systems and processes to handle various activities.
Decision Support Systems: These systems aim at assisting managers who are faced with unique (non-recurring) decision problems. They are of much more use when the decisions are of an unstructured or semi-structured nature. In this situation, the problem area is modeled and various alternatives are explored. In its simplest form, the spreadsheet could be considered as a decision support system. Models can also be built using formulae and variables can be changed to see what would be the outcome. Purpose-built decision-support systems usually incorporate more sophisticated modeling using statistical techniques such as linear programming, regression analysis, time series analysis etc. These decision-support systems are an integrated piece of software incorporating database, model base, and user interface.

Executive Information Systems: These systems are designed primarily for the strategic level of management. They enable executives to extract summary data from the database and model complex problems without the need to learn complex query languages, enter formulae, use complex statistics, or have high computing skills. These systems are easy to use, incorporating touch screens in some instances, and being graphically based. There are standard templates for doing trend analysis and getting high level summary data. The executives need not construct the query or model.

Expert Systems: Expert systems are designed to replace the need for a human expert. They are particularly important where expertise is scarce and therefore expensive. This is a 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 that can be applied to most scenarios. The expert systems are developed using very different programming languages such as PROLOG. These systems are of greater use in the tactical and strategic level.

(b) The duties of certifying authorities [section 30]

(i) The section [30] of Information Technology Act 2000 / Information Technology (Amendment) Act 2008 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 there under.
(iii) A Certifying Authority must display its license at a conspicuous place of the premises in which it carries on its business and a Certifying Authority whose license is suspended or revoked shall immediately surrender the license 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) 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 the management.

(iv) Processing of transactions, files, reports and other computer records is accurate and complete.

(v) Source data that is inaccurate or improperly authorized is identified and handled according to prescribed managerial policies.

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

Question 2

(a) Discuss various constraints that come in the way of operating an effective MIS. How these constraints could be avoided to some extent? (10 marks)

(b) State and briefly explain the components of CASE work bench. (5 marks)

(c) Describe any two inter-related sub-systems of Marketing Information System. (5 marks)

Answer

(a) Constraints in operating an effective MIS

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

(a) Non-availability of experts, who can diagnose the objectives of the organization and provide a desired direction for installing and operating system. The problem may be overcome by grooming internal staff. The grooming of staff should be preceded by proper selection and training.

(b) Experts usually face the problem of selecting the sub-systems of MIS to be installed and operated upon. The criteria, which should guide the experts here, may be the need and importance of a function for which MIS can be installed first.

(c) Due to varied objectives of business concerns, 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 organization in the same industry.

(d) Non-availability of cooperation from staff in fact is a crucial problem. It should be handled tactfully. Educating the staff may solve this problem. This task should be carried out by organizing lectures, showing films and also explaining to them the utility of the system. Besides this, some persons should also be involved in the development and implementation of the system.

(e) There is high turnover of experts in MIS. Turnover in fact arises due to several factors like pay packet; promotion chances; future prospects, behavior of top ranking managers etc. Turnover of experts can be reduced by creating better working conditions and paying at least at par with other similar concerns.

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

These constraints can be resolved by educating the top managers and telling them about the advantages of MIS. Moreover, the example of similar industries could be brought to the notice of top executives which are having better profits. All the benefits should be demonstrated.

(b) Components of a CASE work bench

1. A diagram editing system that is used to create data flow diagrams, structure charts and entity relationship diagrams. It captures information about these entities and saves this information in a central repository.

2. Diagram 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 the 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 central repository with other development tools.

8. Some system support Skelton code generation which generates code segments automatically from the designs captured in the central store.

CASE work bench systems, like structured methods have been mostly used in the development of data processing systems, but there is no reason why they cannot be
used in the development of other classes of system. Productivity improvements up to 40% may be achieved with the use of such systems. The quality of the developed systems is higher with fewer errors and inconsistencies and the development systems are more appropriate to the users needs.

(c) Two inter-related sub-systems of marketing information system are given as follows:

1. **Sales:** The objective of the sales manager is to co-ordinate the sales effort so that the long run profitability of the company is maximized. To achieve these, s/he may use sales support and sales analysis information systems. Sales support information system must provide to sales personnel about product description, specifications, prices, discounts, incentives and promotions information to sales personnel, financing plans to customers, competitors information and all other related information. Sales analysis information system must provide information relating to product sales trend, product-wise profit, performance of sales regions and performance of sales persons.

2. **Marketing Research and Intelligence:** The objective of marketing research is to investigate problems confronting the other managers in the marketing functions. These problems may involve sales, product development advertising and promotion and customer service. To satisfy these decision making and reporting requirements, the marketing research department should provide information at specified interval of time or it may, upon demand, gather information from a wide variety of sources. Marketing research investigates past, present and future states of the market place. The investigations help in satisfaction of information needs of managers on various aspects such as economic trends, sales trends, potential new markets for products, competitors, their strengths and weaknesses etc.

Question 3

(a) **Explain the process of evaluation of various ERP packages.** (10 marks)

(b) **Briefly explain the various stages of developing an in-house software.** (5 marks)

(c) **Discuss the measures that can significantly decrease the potential for Computer frauds.** (5 marks)

Answer

(a) Evaluation of ERP packages are 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 makers.

(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 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 application solutions and services including the web.

(iii) **Integrated:** Here functions like sales and materials planning, production planning, warehouse 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:** 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.

Other factors to be considered are:

- Global presence package,
- Local presence,
- Market targeted by the package,
- Price of the package,
- Obsolescence of package,
- Ease of implementation of package,
- Cost of implementation, and
- Post-implementation support availability.

(b) An In-house development of software commonly involves the following six stages:

(i) **Program Analysis:** In this stage, the programmer ascertains for a particular application, the outputs required, the inputs available and the processing. 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:** In this stage, the designer 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, inputs, outputs, file layouts and flowcharts are quite
useful at this state. These layouts and flow charts 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. The programmers broadly pursue three objectives namely, simplicity, efficient utilization of storage and least processing time. Future changes and development on the programs should also be kept in mind.

(iv) **Debugging of Program:** The process of debugging a program refers to correcting 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.

(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. Since these documents are used by the persons who are doing the tasks, it is to be remembered that persons will come and go but systems (procedures and instructions) will remain in the organizations.

(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. They face a difficult task of understanding and then revising the program they did not write. This should bring out the necessity of writing programs in the first place that are simple to understand.

(c) The measures that can significantly decrease the potential for computer frauds are as under:

1. **Make frauds less likely to occur:** Some computer consultants claim that the most effective method of obtaining adequate system security is to rely on the integrity of company employees. At the same time, research shows that most frauds are committed by current and former employees. Thus, employees are both the greatest control strength and weakness. Organizations can take steps to increase employee integrity and reduce the likelihood of employees committing a fraud.

2. **Use proper hiring and firing practices:** A manager’s most important responsibilities is to hire and retain honest people. Similarly, a company should be very careful when firing employees. Dismissed employees should be removed from sensitive jobs immediately and denied access to the computer system to prevent sabotage or copying confidential data before they leave.

3. **Manage disgruntled Employees:** Many employees who commit fraud are seeking revenge or “justice” for some wrong they perceive has been done to them. Hence,
companies should have procedures for identifying these individuals and either helping them resolve their feelings or removing them from jobs with system access.

4. **Train Employees in Security and Fraud Presentation Measures:** Training and education are very essential for security program. The organization must create an atmosphere where each and every employee believes that security is everyone’s business.

5. **Develop the culture:** A culture should be developed through education, training and commitment with regard to security measures, telephone disclosures, fraud awareness, ethical considerations, punishment for unethical behavior and managing software licenses. All employees, vendors and contractors should be required to sign and abide by confidentiality agreement.

**Question 4**

(a) Describe various components of client/server architecture. (10 marks)

(b) Discuss any three control objectives of an operating system. (5 marks)

(c) Briefly state the role of a Security administrator. (5 marks)

**Answer**

(a) **Components of a Client Server Model**

Various components of client server architecture are briefly described below:

(i) **Client:** 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, and (c) Object-Oriented User Interface (OOUI) clients.

(a) Non-GUIs 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 client and regulate access to shared resources. There are four types of servers as discussed below:

(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. Middleware is all the distributed software needed to allow clients and servers to interact. General middleware allows for communication, directory services, queuing, distributed file sharing, and printing. 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. During the early stage of middleware development, the transfer method was both slow and unreliable.

(iv) Fat-client or Fat-server: Fat-client and fat-server are popular terms in computer literature. These terms serve as vivid description 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 minimize the processing done by clients. Examples of fat-servers are transaction, GroupWare, and web servers. It is also common to hear fat-clients referred to as “2-Tier” systems 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. Network technology is not well understood by business people and end users, since it involves wiring in the wall and function boxes that are usually in a closet.

(b) Control Objectives of an operating system are discussed below:

(i) The operating system must protect itself from users. User applications must not be able to gain control of, or damage in anyway, 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.

(c) **Role of Security Administrator**

A 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 the board approval.

(iii) S/he also investigates, monitors, and 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. S/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. S/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) Advices senior management on matters of information resource control.

(viii) Consults on matters of information security.

(ix) S/he is responsible for conducting security program, which is a series of ongoing, regular periodic evaluations of the facilities available.

(x) S/he is responsible to consider an extensive list of possible threats to the organization. Also s/he evaluates the existing controls and implements new controls.

(xi) S/he requires assistance from many experts in that particular field.

(xii) S/he should see whether the aforementioned steps are performed on a regular basis. The results of the reviews are analyzed and documented. S/he then advises the management on appropriate action in the light of the result.

**Question 5**

*Write short notes on the following:*

(a) **Advantages of prewritten application software packages**

(b) **Contents of system manual of Systems Design**
(c) Data Dictionary

(d) Training for (i) system operators and (ii) users.  (4 x 5 = 20 marks)

Answer

(a) Advantages of Prewritten Application Software packages

The advantages are as follows:

(i) Rapid / Quick Implementation: They are available in ready to use form whereas software developed in-house may take months or years for implementation.

(ii) Low Risks: As it is available in finished and ready to use form, the organization knows with certainty ‘what it is going to get for the price, it has paid’, whereas for an in-house development, the longer time and frequent mobility of the developers breeds lot of uncertainty regarding the cost and quality.

(iii) Quality: The firms writing application software are generally specialist in the product requirement areas and hence provide better solutions. In-house developers have to encounter problems spread over a wider range of applications areas, their expertise may be inferior.

(iv) Lower Cost: Similar products or same products are sold to several customers, realizing lower cost from each purchaser, whereas, in-house developments cost the organization in full. In addition, there is hidden cost also and thus the pre-written applications software packages are cheaper.

(b) Contents of System Manual

It contains:

(i) General description of the existing system.

(ii) Flow of the existing system.

(iii) Outputs of the existing system - the documents produced by existing system are listed and briefly described, including distribution of copies.

(iv) General description of the new system - its purposes and functions and major differences from the existing system are stated together with a brief justification for the change.

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

(vi) Output Layouts.

(vii) Output distribution - the distribution of the new output document is indicated and the number of copies, routing and purpose in each department shown. The output distribution is summarized to show what each department will receive as a part of the proposed system.

(viii) Input layouts - the inputs to the new system are described and complete layouts of the input documents and input disks or tapes provided.
(ix) Input responsibility - the source of each input document is indicated as also the user department responsible for each item on the input documents.

(x) Macro-logic the overall logic of the internal 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. There must be complete layouts for intermediate or work file; these may be prepared later by the programmer.

(xii) List of programs - a list of the programs to be written shall be a part of the systems specifications.

(xiii) Timing estimates - a summary of approximate computer timing is provided by the systems analyst.

(xiv) Controls - this shall include type of controls, and the method in which it will be operated.

(xv) Audit trail - a separate section of the systems specifications shows the audit trail for all financial information. It indicates the methods with which errors and defalcation will be prevented or eliminated.

(xvi) Glossary of terms used.

(c) Data Dictionary

A data dictionary is a computer file that contains descriptive information about data items in the files of a business information system. Each computer record of a data dictionary contains information about a single data item used in a business information system. This includes:

- Codes describing the data item’s length, data type and range,
- The identity of the source documents used to create the data items,
- The names of computer files that store the data item,
- The names of computer programs that modify the data item,
- The identity of the computer programs or individual permitted to access the data items for the purpose of file maintenance, upkeep or enquiry, and
- The identity of the computer programs or individuals not permitted to access the data item.

Accountants and auditors can also make good use of a data dictionary. For example, a data dictionary can help establish an audit trail because it can identify the input sources of data items, the computer programs that modify particular data items, and the managerial reports on which the data items are output. When an accountant is participating in the design of a new system, a data dictionary can also be used to plan the flow of transaction data through the system.
Finally, a data dictionary can serve as an important aid when investigating or documenting internal control procedures. This is because the details about edit tests, methods of file security, and similar information can be stored in the dictionary.

(d) (i) Training for 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 and knowledge of what constitutes normal operation and use. The operators should also be interested in what common malfunctioning may occur, how to recognize them and what steps to be taken 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.

(ii) Training for Users

User training may involve equipment use, particularly in the case where a microcomputer is in use and the individual involved is both operator as well as user. In these cases, users must be instructed on how to operate the equipment. User training must also understand 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 of the user trainings deal 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.

Training is often seen as a necessary evil by managers. While recognizing its importance, many managers have to release employees from their regular job activities so that they can be trained. When managers are actively involved in determining training needs, they are usually more supportive of training efforts. It is generally wise to have managers directly involved in evaluating the effectiveness of training activities because training deficiencies can translate into reduced user productivity level.