Q-1 XYZ Company is a retail chain house having many branches located in different places for its operation. Its business processes are cumbersome and tedious as it has multiple sources of procurement and supply destinations.

The CEO of company feels that existing information system does not meet its present requirements. He seeks for high end solution to stream line and integrate its operation processes and information flow to synergize all its major resources. Further he expects that the new system should provide a structured environment in which decisions concerning demand, supply, operational, personnel, finance, logistics etc. are fully supported by accurate and reliable information. The company follows the best practices of System Development Life Cycle (SDLC), which consists of various phases starting from preliminary investigation till post implementation review, controls and security aspects.

The CEO of the company appoints a committee of three persons, one of them is IT expert, second one is security expert and third one is company’s auditor to suggest the followings:

(a) List the activities to be performed during the phase of System Requirement Analysis. (5 Marks)

(b) What boundary control techniques should be used in user control? (5 Marks)

(c) If committee decides to go for implementing ERP, what general guidelines you would suggest before starting the implementation of ERP package? (5 Marks)

(d) Which aspects should be covered while drafting IS security policy for Business Continuity Planning? (5 Marks)

Q-2

(a) What is the goal of a prototype model approach of software development? Enumerate the strength of this model. (6 Marks)

(b) What activities are involved in system conversion? Explain them briefly. (6 Marks)
Q-3
(a) What is scope of output control of an application system? Suggest various types of output controls which are enforced for confidentiality, integrity and consistency of output.
(6 Marks)
(b) What is an Expert System? List the properties which an application should possess to qualify for Expert System development.
(6 Marks)
(c) What do you mean by ‘Packet Filter Firewall’? Explain the major weaknesses associated with it.
(4 Marks)

Q-4
(a) What do you mean by ‘System Control Audit Review File’ (SCARF)? What types of information can be collected by Auditor using SCARF?
(6 Marks)
(b) What is Business Impact Analysis? Enumerate the tasks which are to be undertaken in this analysis.
(6 Marks)
(c) Describe the procedure to apply for a licence to issue electronic signature certificate under Section 22 of the Information Technology (Amendment) Act, 2008.
(4 Marks)

Q-5
(a) Briefly explain the control and objectives of ‘Asset Classification and Control’ in information security management system.
(6 Marks)
(b) What is the purpose of risk evaluation? Give some of the techniques that are available for risk evaluation.
(6 Marks)
(c) What is Information Security Policy? What are the issues it should address?
(4 Marks)

Q-6
(a) Under the IT Infrastructure Library (ITIL) framework, discuss the importance of following:
(i) Release management
(ii) ICT infrastructure management

(b) Mr. A has received some information about Mr. B on his cellphone. He knows that this information has been stolen by the sender. He not only retained this information but also sends it to Mr. B and his friends. Because of this act Mr. B is annoyed and his life is in danger.

Mr. B seeks your advice, under what sections of Information Technology (Amendment) Act, 2008, he can file an FIR with police? Advise Mr. B detailing the applicable sections of the Act.

(c) ‘Every company that intends to implement ERP has to Re-engineer its processes in one form or other.’ In the light of this statement, describe any four processes that needs to be re-engineered.

Q-7 Write short notes on any four of the following:
(a) Purpose of IS Audit Policy
(b) Audit Tools and Techniques used in Disaster Recovery Plan.
(c) Risk Assessment
(d) Reasons for failure of ERP projects
Ans.1

(a) The activities to be performed during the phase of System Requirements Analysis are given as follows:

- To identify and consult the stakeholders to determine their expectations and resolve their conflicts;
- To analyze requirements to detect and correct conflicts and determine their priorities;
- To verify that the requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable;
- To gather data or find facts using tools like interviewing, research/document collection, questionnaires, observation;
- To model the activities such as developing models to document Data Flow Diagrams, E-R Diagrams; and
- To document the activities such as interview, questionnaires, reports etc. and development of a system (data) dictionary to document the modeling activities.

The final deliverable of this phase of SDLC is SRS.

(b) The major controls of the boundary system are the access control mechanisms. Access controls are implemented with an access control mechanism and links the authentic users to the authorized resources for which they are permitted to access. The access control mechanism has three steps, identification, authentication and authorization with respect to the access control policy.

Major boundary control techniques are given as follows:

- **Cryptography**: It deals with programs for transforming data into codes that are meaningless to anyone, who does not possess the authentication to access the respective system resource or file. A cryptographic technique encrypts data (clear text) into cryptograms (cipher text) and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst. The three techniques of cryptography are transposition (permute the order of characters within a set of data), substitution (replace text with a key-text) and product cipher (combination of transposition and substitution).

- **Passwords**: User identification by an authentication mechanism with personal characteristics like name, birth date, employee code, function, designation or a combination of two or more of these can be used as a password boundary access control. A few best practices followed to avoid failures in this control system are; minimum password length, avoid usage of common dictionary words, periodic change of passwords, encryption of passwords and number of entry attempts.
• **Personal Identification Numbers (PIN):** PIN is similar to a password assigned to a user by an institution based on the user characteristics and encrypted using a cryptographic algorithm, or the institute generates a random number stored in its database independent to a user identification details, or a customer selected number. Hence, a PIN or a digital signature are exposed to vulnerabilities while issuance or delivery, validation, transmission and storage.

• **Identification Cards:** Identification cards are used to store information required in an authentication process. These cards used to identify a user, are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.

• **Biometric devices:** Biometric identification e.g. thumb and/or finger impression, eye retina etc are also used as boundary control techniques.

(c) If the Committee decides to go for implementing ERP, the general guidelines, which are to be followed before starting the implementation of an ERP package, are given as follows:

- Understanding the corporate needs and culture of the organization and then adapt the implementation technique to match these factors;
- Doing a business process redesign exercise prior to starting the implementation;
- Establishing a good communication network across the organization;
- Providing a strong and effective leadership so that people down the line are well motivated;
- Finding an efficient and capable project manager;
- Creating a balanced team of implementation consultants, who can work together as a team;
- Selecting a good implementation methodology with minimum customization;
- Training end users; and
- Adapting the new system and making the required changes in the working environment to make effective use of the system in future.

(d) The following are the major aspects, which should be covered while drafting IS Security Policy for Business Continuity Planning:

- A Business Continuity Plan (BCP) must be maintained, tested and updated if necessary. All staff must be made aware of it.
- A Business Continuity and Impact Assessment must be conducted annually.
- Suppliers of network services must be contractually obliged to provide a predetermined minimum service level.
• If subsidiaries, divisions, departments, and other organizational units wish to be supported by the management information systems department on a priority basis in the event of an emergency or a disaster, they must implement hardware, software, policies, and related procedures consistent with related standards.

• Computer operations management must establish and use a logical framework for segmenting information resources by recovery priority. This will in turn allow the most critical information resources to be recovered first. All departments must use the same framework when preparing information systems contingency plans.

• In addition, recovery priority of all the applications must also be defined by assessing the criticality of the applications. Further, a classification may also be done for application criticality.

• Management must prepare, periodically update, and regularly test emergency response plans and disaster recovery plans that will allow all critical computer systems to continue processing and be available in the event of an interruption or degradation of service and also in the event of a major loss, such as a flood, earthquake.

**Ans.2**

(a) The goal of a prototyping model is to develop a small or pilot version called a prototype of part or all of a system. A prototype is a usable system or system component that is built quickly and at a lesser cost, and with the intention of being modifying or replacing it by a full-scale and fully operational system.

As users work with the prototype, they make suggestions about the ways to improve it. These suggestions are then incorporated into another prototype, which is also used and evaluated and so on. Finally, when a prototype is developed that satisfies all user requirements, either it is refined and turned into the final system or it is scrapped. If it is scrapped, the knowledge gained from building the prototype is used to develop the real system.

Major strengths of Prototyping model are given as follows:

• Prototyping model improves both user participation in system development and communication among project stakeholders.

• This is especially useful for resolving unclear objectives; developing and validating user requirements; experimenting with or comparing various design solutions, or investigating both performance and the human computer interface.

• It has the potential for exploiting knowledge gained in an early iteration as later iterations are developed.

• This helps to easily identify confusing or difficult functions and missing functionality.
• This may generate specifications for a production application.
• This encourages innovation and flexible designs.
• The model provides quick implementation of an incomplete, but functional application.
• Prototyping requires intensive involvement by the system users. Therefore, it typically results in a better definition of these users’ needs and requirements than does the traditional systems development approach.
• A very short time period (e.g., a week) is normally required to develop and start experimenting with a prototype. This short time period allows system users to immediately evaluate proposed system changes.
• Since system users experiment with each version of the prototype through an interactive process, errors are hopefully detected and eliminated early in the developmental process. As a result, the information system ultimately implemented should be more reliable and less costly to develop than when the traditional systems development approach is employed.

Conversion includes all those activities, which must be completed to successfully convert from the previous system to the new information system. These are given as follows:

• **Procedure conversion**: Operating procedures should be completely documented for the new system that 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 control 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.

• **File conversion**: Since large files of information must be converted from one medium to another, this phase should be started long before programming and testing are completed. In order to the conversion to be as accurate as possible, file conversion programs must be thoroughly tested. Adequate control, such as record counts and control totals, should be required output of the conversion program. The existing computer files should be kept for a period of time until sufficient files are accumulated for backup. This is necessary in case the files must be reconstructed from scratch after a “bug” is discovered later in the conversion routine.

• **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. All transactions
initiated after this time are processed on the new system. Consideration should be
given to operating the old system for some more time to permit checking and balanc-
ing the total results of both systems.

- **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. Sched-
ules should be set up by the system manager in conjunction with departmental man-
agers of operational units serviced by the equipment.

- **Alternative plans in case of equipment failure:** Alternative processing plans must
be implemented in case of equipment failure. 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.

(c) Executive Information Systems differs from Traditional Information Systems in many ways.
The following table presents the difference on various related dimensions:

<table>
<thead>
<tr>
<th>Dimensions of Difference</th>
<th>Executive Information System</th>
<th>Traditional Information System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level of management</td>
<td>For top or near top executives</td>
<td>For lower staff</td>
</tr>
<tr>
<td>Nature of Information Access</td>
<td>Specific issues, problems and aggregate reports</td>
<td>Status reporting</td>
</tr>
<tr>
<td>Nature of information provided</td>
<td>Online tools and analysis</td>
<td>Offline status reporting.</td>
</tr>
<tr>
<td>Information Sources</td>
<td>More external, less internal</td>
<td>Internal</td>
</tr>
<tr>
<td>Drill down facility to go through details at</td>
<td>Available</td>
<td>Not available</td>
</tr>
<tr>
<td>Information format</td>
<td>Text with graphics</td>
<td>Tabular</td>
</tr>
<tr>
<td>Nature of interface</td>
<td>User-friendly</td>
<td>Computer-operator</td>
</tr>
</tbody>
</table>

**Ans.3**

(a) The scope of Output controls of an application system is given as follows:

To provide functions that determine the data content available to users, data format, timeliness of
data and how data is prepared and routed to users.

Various types of output controls, which are enforced for confidentiality, integrity and
consistency of output, are given as follows:
• Storage and logging of sensitive, critical forms: Pre-printed stationery should be stored securely to prevent unauthorized destruction or removal and usage. Only authorized persons should be allowed access to stationery supplies such as security forms, negotiable instruments etc.

• Logging of output program executions: When programs used for output of data are executed, it should be logged and monitored. In the absence of control over such output program executions, confidentiality of data could be compromised.

• Spooling/Queuing: This is a process used to ensure that the user is able to continue working, even before the print operation is completed. When a file is to be printed, the operating system stores the data stream to be sent to the printer in a temporary file on the hard disk. This file is then “spooled” to the printer as soon as the printer is ready to accept the data. This intermediate storage of output could lead to unauthorized disclosure and/or modification. A queue is the list of documents waiting to be printed on a particular printer. This queue should not be subject to unauthorized modifications.

• Controls over printing: It should be ensured that unauthorized disclosure of information printed is prevented. Users must be trained to select the correct printer and access restrictions may be placed on the workstations that can be used for printing.

• Report distribution and collection controls: Distribution of reports should be made in a secure way to ensure unauthorized disclosure of data. A log should be maintained as to what reports were generated and to whom it was distributed. Where users have to collect reports, the user should be responsible for timely collection of the report especially if it is printed in a public area. A log should be maintained as to what reports were printed and which of them where collected. Uncollected reports should be stored securely.

• Retention controls: Retention controls consider the duration for which outputs should be retained before being destroyed. Consideration should be given to the type of medium on which the output is stored. Retention control requires that a date should be determined for each output item produced.

• Existence/Recovery Controls: These are needed to recover output in the event that it is lost or destroyed. If the output is written to a spool of files or report files and has been kept, then recovering and new generation is easy and straight-forward.

(b) **Expert System**: An Expert System is highly developed Decision Support System (DSS) that utilizes the knowledge generally possessed by an expert to solve a problem. Expert Systems are software systems that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from such expert systems. For instance, an expert system in the area of investment portfolio management might ask its user a number of specific questions relating to investments for a particular client like – how much can be invested. Does the client have any preferences regarding specific types of securities?
Major properties that an application should possess to qualify for Expert System development are given as follows:

- **Availability**: One or more experts are capable of communicating ‘how they go about solving the problems to which the Expert System will be applied’.

- **Complexity**: Solution of the problems for which the Expert Systems will be used is a complex task that requires logical inference processing, which would not be easily handled by conventional information processing.

- **Domain**: The domain, or subject area, of the problem is relatively small and limited to a relatively well-defined problem area.

- **Expertise**: Solutions to the problem require the efforts of experts. That is, only a few possess the knowledge, techniques, and intuition needed.

- **Structure**: The solution process must be able to cope with ill-structured, uncertain, missing, and conflicting data, and a dynamic problem-solving situation.

**Packet Filter Firewalls**: Packet filter firewalls evaluate the headers of each incoming and outgoing packet to ensure that it has a valid internal address, originates from a permitted external address, connects to an authorized protocol or service, and contains valid basic header instructions. If the packet does not match the pre-defined policy for allowed traffic, then the firewall drops the packet.

Major weaknesses associated with packet filtering firewalls are given as follows:

- The system is unable to prevent attacks that exploit application-specific vulnerabilities and functions because the packet filter does not examine packet contents.

- Logging functionality is limited to the same information used to make access control decisions.

- Most of the packet filtering firewalls do not support advanced user authentication schemes.

- These firewalls are generally vulnerable to attacks and exploitation that take advantage of vulnerabilities in network protocols.

- These firewalls are easy to misconfigure, which allows traffic to pass that should be blocked.

**Ans.4**

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

- **Application system errors** - SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.

- **Policy and procedural variances** - Organizations have to adhere to the policies, procedures and standards of the organization and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.

- **System exception** - SCARF can be used to monitor different types of application system exceptions. For example, salespersons might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.

- **Statistical sample** - Some embedded audit routines might be statistical sampling routines, SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.

- **Snapshots and extended records** - Snapshots and extended records can be written into the SCARF file and printed when required.

- **Profiling data** - Auditors can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.

- **Performance measurement** - Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.

(b) **Business Impact Analysis:** Business Impact Analysis (BIA) is a means of systematically assessing the potential impacts resulting from various events or incidents. It enables the business continuity team to identify critical systems, processes and functions, assess the economic impact of incidents and disasters that result in a denial of access to the system, services and facilities, and assess the “pain threshold,” that is, the length of time business units can survive without access to the system, services and facilities. Major tasks, which are to be undertaken in this analysis, are given as follows:

- Identifying organisational risks - This includes single point of failure and infrastructure risks. The objective is to identify risks and opportunities and to minimize potential threats that may lead to a disaster.

- Identifying critical business processes.
- Identifying and quantifying threats/ risks to critical business processes both in terms of outage and financial impact.
- Identifying dependencies and interdependencies of critical business processes and the order in which they must be restored.
- Determining the maximum allowable downtime for each business process.
- Identifying the type and the quantity of resources required for recovery e.g. tables chairs, faxes, photocopies, safes, desktops, printers, etc.
- Determining the impact to the organization in the event of a disaster, e.g. financial reputation, etc.

(c) [Section 22] Application for license of Information Technology (Amended) Act, 2008:

(1) Every application for issue of a license shall be in such form as may be prescribed by the Central Government.

(2) Every application for issue of a license shall be accompanied by-
   (a) a certification practice statement;
   (b) a statement including the procedures with respect to identification of the applicant;
   (c) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;
   (d) such other documents, as may be prescribed by the Central Government.

Ans.5

(a) ‘Asset Classification and Control’ in Information Security Management System (ISMS):
The detailed controls and objectives are given as follows:

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

These are briefly discussed as follows:

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

(ii) Accountability for assets: It is achieved using IAR and Contracts Register. An Information Asset Register (IAR) should be created with the details of every information asset within
the organization. For example: Databases, Personnel records, Scale models, Prototypes, Test samples, Contracts, Software licenses, Publicity material.

The Information Asset Register (IAR) should also describe ‘who is responsible for each information asset’ and ‘whether there is any special requirement for confidentiality, integrity or availability’. For administrative convenience, separate register may be maintained under the subject head of IAR e.g. ‘Media Register’ will detail the stock of software and its licenses. Similarly, ‘Contracts Register’ will contain the contracts signed and thus other details. The impact that is an addendum to mere maintenance of a register is control and thus protection of valuable assets of the corporation. The value of each asset can then be determined to ensure appropriate security is in place.

(b) The purpose of risk evaluation is to:

- identify the probabilities of failures and threats,
- calculate the exposure, i.e., the damage or loss to assets, and
- make control recommendations keeping the cost-benefit analysis in mind.

Following are the major techniques, which are available for risk evaluation:

(i) **Judgment and intuition:** In many situations, the auditors have to use their judgment and intuition for risk assessment. This mainly depends on the personal and professional experience of the auditors and their understanding of the system and its environment. Together with it, systematic education and ongoing professional updating is also required.

(ii) **The Delphi Approach:** This technique is used for obtaining a consensus opinion. A panel of experts is engaged and each expert is asked to give his opinion in a written and independent method. They enlist the estimate of the cost benefits and the reasons why a particular system is to be chosen, the risks and exposures of the system. These estimates are then complied together. The estimates falling within a pre-decided acceptable range are taken. The process may be repeated four times for revising estimates falling beyond the range. Then a curve is drawn taking all the estimates as points on the graphs. The median is drawn and this is the consensus opinion.

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

(v) **Qualitative Techniques:** These are by far the most widely used approach to risk analysis. Probability data is not required and only estimated potential loss is used. Most qualitative risk analysis methodologies make use of a number of interrelated elements, namely, threats, vulnerabilities, and controls.

(c) **Information Security Policy:** A Policy is a plan or course of action, designed to influence and determine decisions, actions and other matters. The security policy is a set of laws, rules, and practices that regulates how assets, including sensitive information are managed, protected, and distributed within the user organization.

An Information Security policy addresses many issues such as disclosure, integrity and availability concerns, who may access what information and in what manner, basis on which access decision is made, maximized sharing versus least privilege, separation of duties, who controls and who owns the information, and authority issues.

The policy should address the following major issues:

- a definition of information security,
- reasons for ‘why information security is important to the organization’, and its goals and principles,
- a brief explanation of the security policies, principles, standards and compliance requirements,
- definition of all relevant information security responsibilities, and
- reference to supporting documentation.

**Ans.6 (a)**

(i) **Release Management under ITIL:** Release Management is used for platform-independent and automated distribution of software and hardware, including license controls across the entire IT infrastructure. Proper Software and Hardware Control ensure the availability of licensed, tested, and version certified software and hardware, which will function correctly and respectively with the available hardware. Quality control during the development and implementation of new hardware and software is also the responsibility of Release Management. This guarantees that all software can be conceptually optimized to meet the demands of the business processes. The goals of release management are:
• Plan to rollout of software,
• Design and implement procedures for the distribution and installation of changes to IT systems,
• Effectively communicate and manage expectations of the customer during the planning and rollout of new releases, and
• Control the distribution and installation of changes to IT systems.

(ii) **ICT Infrastructure Management under ITIL:** ICT Infrastructure Management processes recommend best practices for requirements analysis, planning, design, deployment and ongoing operations of management and technical support of an ICT Infrastructure. The Infrastructure Management processes describe those processes within ITIL that directly relate to the ICT equipment and software that is involved in providing ICT services to customers; these are given as follows:

• ICT Design and Planning,
• ICT Deployment,
• ICT Operations, and
• ICT Technical Support.

(b) It is not clear whether Mr. B wants to file an FIR with police against Mr. A or sender, who has stolen his information or both.

Considering the most feasible assumption that if Mr. B wants to file an FIR against Mr. A then he may file the same under the following Section of Information Technology (Amendment) Act, 2008:

• Section 66 A: Punishment for sending offensive messages through communication service, etc.;
• Section 66 B: Punishment for dishonestly receiving stolen computer resource or communication device; and
• Section 66 E: Punishment for violation of privacy.

All these applicable sections in this case are given as follows:

**[Section 66 A] Punishment for sending offensive messages through communication service, etc.**

Any person who sends, by means of a computer resource or a communication device,-

(a) any information that is grossly offensive or has menacing character; or
(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation,
enmity, hatred, or ill will, persistently **by making** use of such computer resource or a communication device,

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation: For the purposes of this section, terms “Electronic mail” and “Electronic Mail Message” means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

**[Section 66 B] Punishment for dishonestly receiving stolen computer resource or communication device.**

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

**[Section 66E] Punishment for violation of privacy**

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

However, the answer may also be written considering the other two assumptions, accordingly.

(c) In the light of the statement given in the question, the following are the major processes that need to be re-engineered:

- **Forecasting**: Shows sales, Fund Flows etc. over a long period of time say next two years.
- **Fund Management**: The necessity of funds and the way to raise these funds. Uncertainty and Risk factors to be considered. Simulation with ‘What if’ type analysis.
- **Price Planning**: Determines the price at which products are offered. It involves application of technology to pricing support such as commercial database services. Also performs feedback and sensitivity analysis.
• **Budget Allocation**: Using computerized algorithms to estimate desirable mix of funds allocated to various functions.

• **Material Requirement Planning**: Process of making new products from raw materials and include production scheduling, requirement planning. Also includes activities for monitoring and planning of actual production.

• **Quality Control**: Takes care of activities to ensure that the products are of desired quality.

Ans.7

(a) **Purpose of IS Audit Policy**: Purpose of the audit policy is to provide the guidelines to the audit team to conduct an audit on IT based infrastructure system. The Audit is done to protect entire system from the most common security threats such as access to confidential data, unauthorized access of the department computers, password disclosure compromise, virus infections, denial of service attacks etc.

Audits may be conducted to ensure integrity, confidentiality and availability of information and resources. The IS Audit Policy should lay out the objective and the scope of the audit. An IS audit is conducted to:

• safeguard the Information System Assets/Resources,
• maintain the Data Integrity,
• maintain the System Effectiveness,
• ensure System Efficiency, and
• comply with Information System related policies, guidelines, circulars, and any other instructions requiring compliance in whatever name called.

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

• **Automated Tools**: Automated tools make it possible to review the large computer systems for a variety of flaws in a short time period. They can be used to find threats and vulnerabilities such as weak access controls, weak passwords, lack of integrity of the system software, etc.

• **Internal Control Auditing**: This includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance of laws and regulations.

• **Disaster and Security Checklists**: A checklist can be used against which the system can be audited. The checklist should be based upon disaster recovery policies and
practices, which form the baseline. Checklists can also be used to verify changes to the system from contingency point of view.

- **Penetration Testing:** Penetration testing can be used to locate vulnerabilities.

(c) **Risk Assessment:** A risk assessment activity can provide an effective approach, which acts as the foundation for avoiding the disasters. Risk assessment is also termed as a critical step in disaster and business continuity planning. Risk assessment is necessary for developing a well-tested contingency plan. In addition, Risk assessment is the analysis of threats to resources (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status in the minimum time in case of a disaster. Disasters may lead to vulnerable data and crucial information suddenly becoming unavailable. The unavailability of data may be due to the non-existence or inadequate testing of the existing plan. Risk assessment is a useful technique to assess the risks involved in the event of unavailability of information, to prioritize applications, identify exposures and develop recovery scenarios.

(d) **Reasons for failure of ERP projects:** At its simplest level, ERP is a set of best practices for performing the various duties in the departments of a company, including finance, manufacturing and the warehouse. To get the most from the software, we have to get people inside our company to adopt the work methods outlined in the software. If the people in the different departments that will use ERP don’t agree that the work methods embedded in the software are better than the ones they currently use, they will resist using the software or will want IT to change the software to match the ways they currently do things. This is where ERP projects break down.

Political fights erupt over how or even whether the software will be installed. IT gets bogged down in long, expensive customization efforts to modify the ERP software to fit with powerful business barons’ wishes. Customizations make the software more unstable and harder to maintain when it finally does come to life. Because ERP covers so much of ‘what a business does’; a failure in the software can bring a company to a halt, literally. The mistake companies make is assuming that changing people’s habits will be easier than customizing the software. It’s not the case. Getting people inside the company to use the software to improve the ways they do their jobs is by far the harder challenge. If people are resistant to change, then the ERP project is more likely to fail.

(e) **[Section 19] Recognition of foreign Certifying Authorities:** Section 19 provides the power of the Controller with the previous approval of the Central Government to grant recognition to foreign Certifying Authorities subject to such conditions and restrictions as may be imposed by regulations. As per ITAA 2008, Section 19 is given as under:

(1) Subject to such conditions and restrictions as may be specified by regulations, the Controller
may with the previous approval of the Central Government, and by notification in the Official Gazette, recognize any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognized under sub-section (1), the Electronic Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.
Q-1  ABC Appliances Limited is a popular marketing company, which has many branches located in different places. It does all its business activities such as receiving orders, placing orders, payments, receipts etc. through online. With increased business activities, the company faces several problems with the existing information system. It realizes that the existing system is outdated and needed improvement. Hence, it wishes to enhance the existing system with adequate measures for information security in order to ensure the smooth functioning of new information system and protect the company from loss or embarrassment caused by security failures. To develop such a new system, the company has formed a system development team with professionals like project managers, system analysts and system designers. The team has executed all the phases involved in the SDLC and implemented the new system successfully. Finally, the Post Implementation Review has also been conducted to determine whether the new system adequately meets present business requirements and the company is satisfied with the PIR report. Read the above carefully and answer the following:

(a) State the advantages of SDLC from the perspective of the IS Audit. (5 Marks)
(b) Being an IS Auditor, what objectives can you set for the audit of systems under development and how can you achieve your objectives? (5 Marks)
(c) Suggest some points that may be considered for establishing better information protection. (5 Marks)
(d) What are the activities to be undertaken during the Post Implementation Review? (5 Marks)

Q-2  

(a) XYZ Ltd. is a large multinational company with offices in many locations. It stores all its data in just one centralized computer centre. It uses Internal Controls in order to asset safeguarding, data integrity, system efficiency and effectiveness. What could be the interrelated components of its Internal Control? Discuss them briefly. (6 Marks)
(b) What is meant by EIS? What are its characteristics? (6 Marks)
(c) Explain any four features of Electronic Mail. (4 Marks)

Q-3  

(a) Threat is any circumstance or event with the potential to cause harm to an information system. What can be the threats due to cyber crimes? (6 Marks)
(b) What is the skill set expected from an IS Auditor? (6 Marks)
(c) In Information Technology (Amended) Act 2008, what do Section 25 and Section 26 say about suspension of license to issue electronic signature certificate? (4 Marks)
Q-4
(a) Access to information and business processes should be controlled on the business and security requirements. In that case, what can be the detailed control and objectives with respect to Information Security Management Standard?

(6 Marks)

(b) During the review of hardware, how will you review the change in the management controls?

(6 Marks)

(c) Describe the duties of certifying authority in respect of Digital Signature under Section 30 of Information Technology (Amended) Act 2008.

(4 Marks)

Q-5
(a) Any system has to possess few key characteristics to qualify for a true Enterprise Resource Planning Solution. What are they?

(6 Marks)

(b) What are the characteristics of a good coded program?

(6 Marks)

(c) What are the points to be included when the documented audit program is developed?

(4 Marks)

Q-6
(a) What is the scope of IS Audit process? Explain the categories of IS Audit.

(6 Marks)

(b) What are the elements to be included in the methodology for the development of disaster recovery / business resumption plan?

(6 Marks)

(c) What are the goals of Business Continuity Plan?

(4 Marks)

Q-7
Write short notes on any four of the following:

(a) Business Engineering

(4 Marks)

(b) Constitution of Cyber Regulations Advisory Committee under Section 88 of Information Technology (Amended) Act 2008

(4 Marks)

(c) Limitations of MIS

(4 Marks)

(d) Basic ground rules for protecting computer held information system

(4 Marks)

(e) Domains of COBIT

(4 Marks)
(a) From the perspective of the IS Audit, the following are the major advantages of SDLC:
• The IS Auditor can have a clear understanding of the various phases of the SDLC on the basis of the detailed documentation created during each phase of the SDLC.
• The IS Auditor on the basis of his/her examination, can state in his/her report about the compliances by the IS management of the procedures, if any, set up by the management.
• The IS Auditor, if has a technical knowledge and ability of the area/s of SDLC, can be a guide during various phases of SDLC.
• The IS Auditor can provide an evaluation of the methods and techniques used during various development phases of the SDLC.

(b) The audit of systems under development can have the following main objectives:
• to provide an opinion on the efficiency, effectiveness, and economy of the project management;
• to assess the extent to which the system being developed provides adequate audit trails and controls to ensure the integrity of data processed and stored; and
• to assess the controls being provided for the management of the system's operation.

For the first objective to achieve, an auditor will have to attend project and steering committee meetings and examine project control documentation and conducting interviews. This is to ensure what project control standards are to be complied with, (such as a formal systems development process) and determining the extent to which compliance is being achieved.

For addressing the second objective, the auditor can examine system documentation, such as functional specifications, to arrive at an opinion on controls. The auditor's opinion will be based on the degree to which the system satisfies the general control objectives that any Information Technology system should meet. A list of such objectives should be provided to the auditee.

The same is true for the third objective, viz. system's operational controls. The auditor should provide a list of the standard controls over such operational concerns as response time, CPU usage, and random access space availability that the auditor has used as assessment criteria.

(c) Major points that may be considered for establishing better information protection are given as follows:
• **Not all data has the same value**: Each data has a different value and accordingly, the information may be handled and protected differently. Organizations must determine the value of the different types of information in their environment before they plan for the appropriate levels of protection.
• **Know where the critical data resides**: Identification of the location where each data is located enables an organization to establish an integrated security solution.
Protection solution must be based on the most valuable information assets. The network environment also present additional challenges for protecting information.

- **Develop an access control methodology**: Information does not have to be removed to cause damage or to have financial impact. Information that is inadvertently damaged, disclosed or copied without the knowledge of the owner may render the data useless. To guard against this, organizations must establish some type of access control methodology. There are many solutions available to provide this protected access.

- **Protect information stored on media**: Employees can cause considerable damage by walking out the door with information on USB Drives or CD-ROMS. In addition, companies should control magnetic media to reduce the loss of software (both application and operating system) and finally, when migrating from one platform to another, the status of all hard drives and the associated data should be controlled.

- **Review hardcopy output**: The hardcopy output of employees’ daily work should also be reviewed. In addition, ‘what measures are used to safeguard all drafts and working papers’ should also be reviewed.

(d) During the Post Implementation Review, the team should, according to their terms of reference, review:

- the main functionality of the operational system against the User Requirements Specification along with the confirmation that all the anticipated benefits, both tangible and intangible, have been delivered;
- system performance and operation;
- the development techniques and methodologies employed;
- estimated time-scales and budgets, and identify reasons for variations, if any;
- changes to requirements, and confirm that they were considered authorized and implemented in accordance with change and configuration management standards; and
- the findings, conclusions and recommendations documented in a report for the authorizing authority to consider.

**Ans.2**

(a) Internal controls used within XYZ Ltd. may comprise of the following five interrelated components:

- Control environment,
- Risk assessment,
- Control activities,
A brief overview of each component is given as follows:

- **Control environment**: These are the elements that establish the control context in which specific accounting systems and control procedures must operate. The control environment is manifested in management’s operating style, the ways authority and responsibility are assigned, the functional method of the audit committee, the methods used to plan and monitor performance and so on.

- **Risk assessment**: This relates to the elements that identify and analyze the risks faced by an organization and the ways the risk can be managed. Both external and internal auditors are concerned with errors or irregularities that cause material losses to an organization.

- **Control activities**: These are the elements that operate to ensure transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded, and independent checks on performance and valuation of recorded amounts occur. These are called accounting controls. Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency objectives.

- **Information and communication**: These are related to the elements, in which information is identified, captured and exchanged in a timely and appropriate form to allow personnel to discharge their responsibilities.

- **Monitoring**: These are the elements for ensuring that internal controls operate reliably over time.

(b) **Executive Information System (EIS)**: An EIS – sometimes also referred as an Executive Support System (ESS) is a DSS that is designed to meet the special needs of top-level managers. Some people use the terms “EIS” and “ESS” interchangeably. Any distinction between the EIS and ESS usually is because Executive Support Systems are likely to incorporate additional capabilities such as electronic mail etc. Some of the important characteristics of EIS are given as follows:

- **EIS** is a Computer based information system that serves the information needs of top executives.

- **EIS** enables users to extract summary data and model complex problems without the need to learn query languages, statistical formulas or high computing skills.

- **EIS** provides rapid access to timely information and direct access to management reports.
- EIS is capable of accessing both internal and external data.
- EIS provides extensive online analysis tools like trend analysis, market conditions etc.
- EIS can easily provide a DSS support for decision making.

(c) Major features of an Electronic Mail are given as follows:

- **Electronic transmission**: The transmission of messages with email is electronic and message delivery is very quick, almost instantaneous. The confirmation of transmission is also quick and the reliability is very high.
- **Online development and editing**: The email message can be developed and edited online before transmission. The online development and editing eliminates the need for the use of paper/s in communication. It also facilitates the storage of messages on magnetic media, thereby reducing the space required to store the messages.
- **Broadcasting and Rerouting**: Email permits sending a message to a large number of target recipients. Thus, it is easy to send a circular to all the branches of a bank using Email resulting in a lot of saving of papers. The email could be rerouted to people having direct interest in the message with or without changing or appending related information to the message.
- **Integration with other Information systems**: The E-mail has the advantage of being integrated with the other information systems. Such an integration helps in ensuring that the message is accurate and the information required for the message is accessed quickly.
- **Portability**: Email renders the physical location of the recipient and sender. The email can be accessed from any Personal computer equipped with the relevant communication hardware, software and link facilities.
- **Economical**: The advancements in communication technologies and competition among the communication service providers have made Email the most economical mode for sending messages. Since the speed of transmission is increasing, the time and cost on communication media per page is falling further, adding to the popularity of email. The email is proving to be very helpful not only for formal communication but also for informal communication within the business enterprise.

Ans.3

(a) Following are the major threats due to cyber crimes:

- **Embezzlement**: It is unlawful misappropriation of money or other things of value, by the person to whom it was entrusted (typically an employee) for his/her own use or purpose.
- **Fraud**: It occurs on account of internal misrepresentation of information or identity
to deceive others, the unlawful use of credit/ debit card or ATM, or the use of electronic means to transmit deceptive information, to obtain money or other things of value. Fraud may be committed by someone, inside or outside the company.

- Theft of proprietary information: It is illegal to obtain the designs, plans, blueprints, codes, computer programs, formulas, recipes, trade secrets, graphics, copyrighted material, data, forms, files, lists, and personal or financial information, usually by electronic copying.

- Denial of Service (DoS): There can be disruption or degradation of service that is dependent on external infrastructure. Problems may erupt through internet connection or e-mail service that result in an interruption of the normal flow of information. DoS is usually caused by the events such as ping attacks, port scanning probes, and excessive amounts of incoming data.

- Vandalism or sabotage: It is the deliberate or malicious damage, defacement, destruction or other alteration of electronic files, data, web pages, and programs.

- Computer virus: Viruses are hidden fragments of computer codes, which propagate by inserting themselves into or modifying other programs.

- Others: Threat includes several other cases such as intrusion, breaches and compromises of the respondent’s computer networks (such as hacking or sniffing) regardless of whether damage or loss were sustained as a result.

(b) The skill set expected from an IS auditor includes the following:

- Sound knowledge of business operations, practices and compliance requirements,
- Should possess the requisite professional technical qualification/s and certification/s;
- A good understanding of information Risks and Controls;
- Knowledge of IT strategies, policies and procedure controls;
- Ability to understand technical and manual controls relating to business continuity; and
- Good knowledge of Professional Standards and best practices of IT controls and security.

(c) As per Section 25 of the Information Technology (Amended) Act, 2008, the Controller may revoke a license on the grounds such as incorrect or false material, particulars being mentioned in the application and also on the ground of contravention of any provisions of the Act, rule, regulation or order made there under.

However, no license shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.
Also, no license shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

Thereafter, as per Section 26 Information Technology (Amended) Act, 2008, Controller shall publish a notice of suspension or revocation of license as the case may be in the database maintained by him.

Further, the database containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site, which shall be accessible round the clock.

It is also provided that the Controller may, if he considers necessary, publicize the contents of database in such electronic or other media, as he may consider appropriate.

**Ans.4**

(a) The detailed controls and objectives of Access Control with respect to Information Security Management Standard/System are given as follows:

- Business requirement for access control: To control the access to the information;
- User access management: To prevent unauthorized access to the information systems;
- User responsibilities: To prevent unauthorized user access;
- Network access control: Protection of networked services;
- Operating system access control: To prevent unauthorized computer access;
- Application Access Control: To prevent unauthorized access to information held in information systems;
- Monitoring System Access and use: To detect unauthorized activities; and
- Mobile Computing and teleworking: To ensure information security when using mobile computing & teleworking facilities.

(b) During the review of hardware, review in the change in management controls is accomplished by the following:

- Determine if changes to hardware configuration are planned and timely information is given to the individual/s responsible for scheduling.
- Determine whether the change schedules allow time for adequate installation and testing of new hardware.
- Verify that the operator documentation is appropriately updated to reflect the changes in the hardware.
• Select samples of hardware changes that have affected the scheduling of IS processing and determine if the plans for changes are being addressed in a timely manner.
• Ensure that there is a cross-reference between the change and its cause, i.e. the problem.
• Ascertain whether the system programmers, application programmers and the IS staff have been informed about all the hardware changes to ensure that changes are coordinated properly.

(c) [Section 30] Duties of Certifying Authorities of Information Technology (Amended) Act, 2008:

This section provides that every Certifying Authority shall follow certain procedures in respect of Digital Signatures as given below:

Every Certifying Authority shall-

(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 Electronic Signature are assured (Amended vide ITAA 2008)

(c) be the repository of all Electronic Signature Certificates issued under this Act (Inserted vide ITAA 2008)

(c) publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and (Inserted vide ITAA 2008)

(d) observe such other standards as may be specified by regulations.

Ans.5

(a) To qualify for a true Enterprise Resource Planning (ERP) solution, a system has to possess the following key characteristics:

• Flexibility,

• Modular and Open,

• Comprehensive,

• Beyond the Company, and

• Best Business Practices.

A brief discussion on each characteristic is given as follows:

• **Flexibility**: An ERP system should be flexible to respond to the changing needs of an
enterprise. The client server technology enables ERP to run across various database back ends through Open Database Connectivity (ODBC).

- **Modular & Open**: ERP system has to have open system architecture. It means, any module can be interfaced or detached whenever required without affecting the other modules. It should support multiple hardware platforms for the companies having heterogeneous collection of the systems. It must support some third party add-ons also.

- **Comprehensive**: It should be able to support variety of organizational functions and must be suitable for a wide range of business organizations.

- Beyond the Company: It should not be confined to the organizational boundaries; rather support the on-line connectivity to the other business entities of the organization.

- **Best Business Practices**: It must have a collection of the best business processes applicable worldwide. An ERP package imposes its own logic on a company’s strategy, culture and organization.

(b) A good coded program should have the following characteristics:

- **Reliability**: It refers to the consistency, which is provided by a program over a period of time. However, poor setting of parameters and hard coding of some data subsequently could result in the failure of a program after some time.

- **Robustness**: It refers to the process of taking into account all the possible inputs and outputs of a program in case of least likely situations.

- **Accuracy**: It refers not only to ‘what program is supposed to do’, but should also takes care of ‘what it should not do’. The second part becomes more challenging for quality control personnel and auditors.

- **Efficiency**: It refers to the performance, which should not be unduly affected with the increase in input values.

- **Usability**: It refers to a user-friendly interface and easy-to-understand document required for any program.

- **Readability**: It refers to the ease of maintenance of program even in the absence of the program developer.

(c) The points to be included when a documented audit program is developed are given as follows:

- Documentation of the information system auditor's procedures for collecting, analyzing, interpreting, and documenting information during the audit;
• Objectives of the audit;
• Scope, nature, and degree of testing required to achieve the audit objectives in each phase of the audit;
• Identification of technical aspects, risks, processes, and transactions, which should be examined; and
• Procedures for audit prepared prior to the commencement of the audit work and modified, as appropriate, during the course of the audit.

Ans.6

(a) The scope of IS Audit process should include the examination and evaluation of the adequacy and effectiveness of the system of internal controls and the quality of performance by the information system. In addition, IS Audit process will also examine and evaluate the planning, organizing, and directing processes to determine whether reasonable assurance exists so that objectives and goals will be achieved. Such evaluations, in the aggregate, provide information to appraise the overall system of internal control.

The scope of the audit will also include the internal control system/s for the use and protection of information and the information systems, such as, Data, Application systems, Technology, Facilities, and People.

IS Audit has been categorized into the following five major types:

• Systems and Applications: An audit to verify that systems and applications are appropriate, efficient, and adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.

• Information Processing Facilities: An audit to verify that the processing facility is controlled to ensure timely, accurately, and efficiently processing of applications under normal and potentially disruptive conditions.

• Systems Development: An audit to verify that the systems under development meet the objectives of the organization and to ensure that the systems are developed in accordance with generally accepted standards for systems development.

• Management of IT and Enterprise Architecture: An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.

• Telecommunications, Intranets, and Extranets: An audit to verify that controls are in place on the client (computer receiving services), server, and on the network connecting the clients and servers.

(b) The elements to be included in the methodology for the development of a disaster recovery/business resumption plan are given as follows:
• Identification and prioritization of the activities, which are essential for continuous functioning.
• Determining that the plan is based upon a business impact analysis, which considers the impact of the loss of essential functions.
• Determining that Operation managers and key employees participated in the development of the plan.
• Determining that the plan identifies the resources that will likely to be needed for recovery and the location of their availability.
• Determining that the plan is simple and easily understood so that it will be effective when it is needed.
• Determining that the plan is realistic in its assumptions.

(c) The goals of a Business Continuity Plan should be to:
• identify the weaknesses and implement a disaster prevention program;
• minimize the duration of a serious disruption to business operations;
• facilitate effective co-ordination of recovery tasks; and
• reduce the complexity of the recovery efforts.

Ans.7

(a) Business Engineering: The term ‘Business Engineering’ has emerged by merging the two concepts namely, Information Technology and Business Process Reengineering. Business Engineering is the method of development of business processes according to changing requirements.

Business Engineering is the rethinking of Business Processes to improve the speed, quality and output of materials or services. The emphasis of business engineering is on the concept of Process Oriented Business Solutions enhanced by the Client-Server computing through 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 the enterprise and customers. Information technology helps to develop business models, which assists in redesigning the business processes.

(b) [Section 88] Constitution of Advisory Committee of Cyber regulations of Information Technology (Amended) Act, 2008:

(1) The Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber Regulations Advisory Committee.

(2) The Cyber Regulations Advisory Committee shall consist of a Chairperson and such
number of other official and non-official members representing the interests principally affected or having special knowledge of the subject-matter as the Central Government may deem fit.

(3) The Cyber Regulations Advisory Committee shall advise –

(a) the Central Government either generally as regards any rules or for any other purpose connected with this Act;

(b) the Controller in framing the regulations under this Act

(4) There shall be paid to the non-official members of such Committee such traveling and other allowances as the Central Government may fix.

(c) Limitations of MIS: Major limitations of MIS are given as follows:

• The quality of the output of MIS is basically governed by the quantity of input and processes.

• MIS is not a substitute for effective management; it means that it cannot replace managerial judgment in the decision making for different functional areas. It is merely an important tool in the hands of executives for decision making and problem solving.

• MIS may not have requisite flexibility to quickly update itself with the changing needs of the time, especially in fast changing and complex environment.

• MIS cannot provide tailor-made information packages suitable for the purpose of every type of decisions made by executives.

• MIS takes into account mainly quantitative factors, thus it ignores the non-quantitative factors like morale and attitude of members of the organization, which have an important bearing on the decision making process of executives.

• MIS is less useful for making non-programmed decisions. Such type of decisions is not of the routine type and thus requires information, which may not be available from existing MIS to executives.

• The effectiveness of MIS may be reduced in the organizations, where the culture of hoarding information and not sharing with other holds exist.

• MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.

(d) Basic Ground rules for protecting Computer held Information System: A few basic ground rules for protecting Information Systems that must be addressed sequentially are given as follows:

• Rule #1: We need to know that ‘what the information systems are’ and ‘where these are located’.
• Rule #2: We need to know the ‘value of the information held’ and ‘how difficult it would be to recreate if it were damaged or lost’.

• Rule #3: We need to know that ‘who is authorized to access the information’ and ‘what they are permitted to do with the information’.

• Rule #4: We need to know that ‘how quickly information needs to be made available and should it become unavailable for whatever reason (loss, unauthorized modification, etc.)’

(e) **Domains of COBIT**: COBIT covers four domains, which are given as follows:

• **Plan and Organize**: The Plan and Organize domain covers the use of IT and how best it can be used in a company to achieve the company’s goals and objectives. It also highlights the organizational and infrastructural form in order to achieve the optimal results and to generate the maximum benefits from the use of IT.

• **Acquire and Implement**: The Acquire and Implement domain covers identifying IT requirements, acquiring the technology, and implementing it within the company’s current business processes. This domain also addresses the development of a maintenance plan that a company should adapt in order to prolong the life of an IT system and its components.

• **Deliver and Support**: The Deliver and Support domain focuses on the delivery aspects of IT. It covers areas such as the execution of the applications within the IT system and its results as well as the support processes that enable the effective and efficient execution of these IT systems. These support processes include security issues and training.

• **Monitor and Evaluate**: The Monitor and Evaluate domain deals with a company’s strategy in assessing the needs of the company and whether or not the current system still meets the objectives for which it was designed and the controls necessary to comply with regulatory requirements. Monitoring also covers the issue of an independent assessment of the effectiveness of IT system in its ability to meet the business objectives and the company’s control processes by internal and external auditors.
Q-1  
ABC is a leading company in the manufacturing of food items. The company is in the process of automation of its various business processes. During this phase, technical consultant of the company has highlighted the importance of information security and has suggested to introduce it right from the beginning. He has also suggested to perform the risk assessment activity and accordingly, to mitigate the assessed risk. For carrying out all these suggestions, various best practices have been followed by the company. In addition, after each activity, appropriate standards' compliances have been tested to check the quality of each process. Various policies related with business continuity planning and disaster recovery planning have been implemented to ensure three major expectations from the software, namely, resist, tolerate and recover.

Read the above carefully and answer the following:

(a) What are the major suggestions given by the technical consultant? How the company is implementing these suggestions?  

(b) Discuss risk assessment with the help of risk analysis framework in brief.  

(c) Out of various types of plans used in business continuity planning, discuss recovery plan in brief.  

(d) What should be the major components of a good information security policy, as per your opinion?  

Q-2  

(a) What do you understand by unauthorized intrusion? What is hacking and what damage can a hacker do?  

(b) What are the guidelines to be followed before starting the implementation of an ERP package?  

(c) Describe the power to make rules by Central Government in respect of Electronic Signature under Section 10 of Information Technology (Amended) Act 2008.  

Q-3  

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

(b) What is Decision Support System? Discuss its characteristics in brief.  

(c) What are the major activities involved in the design of a database?
Q-4
(a) What is IT Infrastructure Library? Discuss the configuration management under ITIL framework. (6 Marks)
(b) List any six ERP vendors and describe the ERP packages offered by them. (6 Marks)
(c) Discuss the parameters that would help in planning a documentation process of an audit. (4 Marks)

Q-5
(a) What is a Virus? What policy and procedure controls can be recommended for ensuring control over virus proliferation and damage? (6 Marks)
(b) How is the term 'Electronic Record' defined in IT (Amended) Act 2008? What is the provision given in the IT Act for the retention of Electronic Records? (6 Marks)
(c) Discuss the constraints in operating a MIS. (4 Marks)

Q-6
(a) The unique nature of each LAN makes it difficult to define standard testing procedures to effectively perform a review. So, what information a Reviewer/IS Auditor should identify and understand prior to commencing a LAN review? (6 Marks)
(b) As an IS Auditor, what are the steps to be followed by you while conducting IT auditing? (6 Marks)
(c) What are the two types of Service Auditor's Reports under SAS 70? Describe the contents of each type of report. (4 Marks)

Q-7 Write short notes on any four of the following:
(a) Data Dictionary (4 Marks)
(b) Risk Mitigation Measures (4 Marks)
(c) Software Process Maturity (4 Marks)
(d) Preventative and Restorative Information Protection (4 Marks)
(e) Objectives of Information Technology Act 2000 (4 Marks)
Ans.1

(a) During the automation of various processes of ABC Company, the technical consultant of the company has given the following major suggestions:

- By realizing the importance of information security, he suggested to introduce it right from the beginning.
- In addition, he also suggested to perform the risk assessment activity.
- Finally, he advised to mitigate the assessed risk.

For the implementation of all the above mentioned suggestions, the company took the following steps:

- The company followed various best practices for each process for the proper implementation of the suggestions.
- In addition, the company also tested the compliance of appropriate standards after each activity, to check the quality of each process.
- Further, the company also implemented the policies related to business continuity planning and disaster recovery to ensure three broad expectations from the software: resist, tolerate and recover.

(b) **Risk Assessment**: A risk assessment activity can provide an effective approach, which acts as the foundation for avoiding the disasters. Risk assessment is also termed as a critical step in disaster and business continuity planning. Risk assessment is necessary for developing a well tested contingency plan. In addition, Risk assessment is the analysis of threats to resources (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status in the minimum time in case of a disaster. Risk assessment is a useful technique to assess the risks involved in the event of unavailability of information, to prioritize applications, identify exposures and develop recovery scenarios.

A risk analysis can provide an effective approach that will serve as the foundation for avoiding the disasters. Through risk analysis, it is possible to identify, assess, and then mitigate the risk. Such an analysis entails the development of a clear summary of the current situation and a systematic plan for risk identification, characterization, and mitigation.
The framework of risk analysis is given as follows:

(c) **Recovery Plan**: The backup plan is intended to restore operations quickly so that the information system function can continue to service an organization, whereas, recovery plans set out procedures to restore full information system capabilities. Recovery plans should identify a recovery committee that will be responsible for working out the specification of the recovery to be undertaken.

The plan should specify the responsibilities of the committee and provide guidelines on priorities to be followed. The plan might also indicate 'which applications are to be recovered first'. Members of a recovery committee must understand their responsibilities. Here, there is a major issue that they will be required to undertake unfamiliar tasks. Periodically, they must review and practice for executing their responsibilities so that they are prepared for a disaster. If committee members leave the organization, new members must be appointed immediately and briefed about their responsibilities.

(d) A good Information Security Policy should clearly state the following:

- Purpose and scope of the document and the intended audience,
- The Security infrastructure,
- Security policy document maintenance and compliance requirements,
- Incident response mechanism and incident reporting,
- Security organization structure,
- Inventory and classification of assets,
- Description of technologies and computing structure,
- Physical and environmental security,
- Identity management and access control,
- IT operations management,
- IT communications,
- System development and maintenance controls,
- Business Continuity Planning (BCP),
- Legal compliances,
- Monitoring and auditing requirements, and
- Underlying technical policy

**Ans. 2**

(a) Unauthorized Intrusion: Intrusion detection is an attempt to monitor and possibly prevent the attempts to intrude into or otherwise compromise the system and network resources of an organization. The computer systems of an organization are attached to a network, and also to the internet. The organization would allow access to that computer system from the network, by authorized people, for acceptable reasons.

For example; if there is a web server, attached to the internet, only clients, staff, and potential clients, are allowed to access the web pages stored on that web server. It does not allow unauthorized access to the system by anyone, be that staff, customers, or unknown third parties. For example, it does not want people (other than the web designers that the company has employed) to be able to change the web pages on that computer. Typically, a firewall or authentication system of some kind will be employed to prevent unauthorized access.

**Hacking** : Hacking is an act of penetrating computer systems to gain knowledge about the system and how it works. Technically, a hacker is someone, who is enthusiastic about computer programming and all things relating to the technical workings of a computer. There are many ways in which a hacker can hack. Some of them are given as follows:

- NetBIOS,
- ICMP Ping,
- FTP,
- rpc.statd, and
- HTTP.

**What damage can a Hacker do?**

This depends upon ‘what backdoor program(s) are hiding on the PC’. Different programs can do different amounts of damage. However, most of them allow a hacker to smuggle another program onto our PC. This means that if a hacker can’t do something using the backdoor program, s/he can easily put something else onto the computer.
Hackers can see everything we are doing, and can access any file on the disk. Hackers can write new files, delete files, edit files, and do practically anything to a file that could be done to a file. A hacker can install several programs on to the system without our knowledge. Such programs can also be used to steal personal information such as passwords and credit card information.

(b) There are certain general guidelines, which are to be followed before starting the implementation of an ERP package. These are given as follows:

- Understanding the corporate needs and culture of the organization and then adopting the implementation technique to match these factors;
- Doing a business process redesign exercise prior to starting the implementation;
- Establishing a good communication network across the organization;
- Providing a strong and effective leadership so that people down the line are well motivated;
- Finding an efficient and capable project manager;
- Creating a balanced team of implementation consultants, who can work together as a team;
- Selecting a good implementation methodology with minimal customization;
- Training end users; and
- Adapting the new system and making the required changes in the working environment to make an effective use of the system in future.

(c) Section 10  Power to make rules by Central Government in respect of Electronic Signature (Modified Vide ITAA 2008):

The Central Government may, for the purposes of this Act, by rules, prescribe

(a) the type of Electronic Signature;
(b) the manner and format in which the Electronic Signature shall be affixed;
(c) the manner or procedure which facilitates identification of the person affixing the Electronic Signature;
(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and
(e) any other matter which is necessary to give legal effect to Electronic Signature.

Ans.3

(a) The benefits, which result from developing new or improved information systems that utilize computers 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. Both these aforementioned 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) Improved competitive position (faster and better response to actions of competitors); and
(xii) Improved business and community image (progressive image as perceived by customers, investors etc.).

(b) A Decision Support System (DSS) can be defined as a system providing tools to the decision making managers to address unstructured/partially structured problems in their own personalized manner. It empowers the managers with a set of capabilities that enable them to generate the information required by them in decision making process. A DSS does not require any high technology. It is considered as more flexible and adaptable for changing decision making requirements than traditional Management reporting system. There are three major characteristics of a Decision Support System, namely:

(i) Semistructured or unstructured decision-making;
(ii) Adaptable to the changing needs of decision makers; and
(iii) Ease of learning and use.

Each of these characteristics is briefly discussed below:

(i) Semistructured and Unstructured Decisions: Unstructured decisions and
semistructured decisions are made when information obtained from a computer system is only a portion of the total knowledge needed to make the decision. DSS is well adapted to help with semistructured and unstructured decisions. A well-designed DSS helps in decision making process with the depth to which the available data can be tapped for useful information.

(ii) Ability to adapt to changing needs: Semistructured and unstructured decisions often do not conform to a predefined set of decision-making rules. DSS provides flexibility to enable users to model their own information needs. Rather than locking the system into rigid information producing requirements, capabilities and tools are provided by DSS to enable users to meet their own output needs.

(iii) Ease of Learning and Use: DSS software tools employ user-oriented interfaces such as grids, graphics, non-procedural fourth - generation languages (4GL), natural English, and easily read documentation. These interfaces make it easier for users to conceptualize and perform the decision-making process.

(c) The designing of a database involves four major activities, which are given as follows:

- **Conceptual Modeling**: These describe the application domain via entities/objects, attributes of these entities/objects and static and dynamic constraints on these entities/objects, their attributes, and their relationships.

- **Data Modeling**: Conceptual Models need to be translated into data models so that they can be accessed and manipulated by both high-level and low-level programming languages.

- **Storage Structure Design**: Decisions must be made on how to linearize and partition the data structure so that it can be stored on some device. For example, tuples (row) in a relational data model must be assigned to records, and relationships among records might be established via symbolic pointer addresses.

- **Physical Layout Design**: Decisions must be made on how to distribute the storage structure across specific storage media and locations—for example, the cylinders, tracks, and sectors on a disk and the computers in a LAN or WAN.

**Ans.4**

(a) ITIL (IT Infrastructure Library): ITIL is a collection of books (standards); each covering a specific 'practice' within IT management. After the initial published works, the number of publications quickly grew (within ITIL v1) to over 30 books. In order to make ITIL more accessible (and affordable) to those wishing to explore it, one of the aims of the ITIL v2 project was to consolidate the works into a number of logical 'sets' that aimed to group related sets of process guidelines for different aspects of the management of Information Technology systems, applications and services together.
The eight ITIL books and their disciplines are:

The IT Service Management sets relating to:

1. Service Delivery
2. Service Support

Other operational guidance relating to:

3. ICT Infrastructure Management
4. Security Management
5. The Business Perspective
6. Application Management
7. Software Asset Management
8. Planning to Implement Service Management

**Configuration Management**: It is a process that tracks all of the individual Configuration Items (CI) in a system. A system may be as simple as a single server, or as complex as the entire IT department. Configuration Management includes:

- Creating a parts’ list of every CI (hardware or software) in the system;
- Defining the relationship of CIs in the system;
- Tracking of the status of each CI, both its current status and its history;
- Tracking all Requests for Change to the system; and
- Verifying and ensuring that the CI parts list is complete and correct.

There are five basic activities in configuration management:

- Planning,
- Identification,
- Control,
- Status accounting, and
- Verification and Audit.

(b) There are quite a few ERP packages available in the market these days. Out of these, most popular six ERP packages along with the vendors are listed below:

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Brief Description of ERP Package offered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baan Corporation</td>
<td><strong>Baan</strong>: Initially developed for an aircraft company, it was subsequently launched as a generalized package in 1994. It offers sound technology and coverage of broad functional scope.</td>
</tr>
<tr>
<td>Company</td>
<td>Solution Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Oracle</td>
<td><strong>Oracle ERP Solutions</strong>: It gives Internet-enabled, network-centric computing. It also offers database, tools, implementation, applications and UNIX operating systems under one stop-shop umbrella. It is currently running on wide choice of hardware.</td>
</tr>
<tr>
<td>Marcam Corporation</td>
<td><strong>Prism</strong>: Prism is a specialist process manufacturing solution for the AS/400. Its production model, which is similar to a flowchart, handles process industry problems elegantly. Although out dated, it does the job.</td>
</tr>
<tr>
<td>SAP</td>
<td><strong>SAP R/3</strong>: It is a market leader with excellent philosophy of matching business processes with its modules. It covers almost all business segments.</td>
</tr>
<tr>
<td>JBA</td>
<td><strong>JBA System 21</strong>: Its software license revenues are small compared to other major ERP vendors. It offers a rugged, reliable manufacturing solution.</td>
</tr>
<tr>
<td>Microsoft</td>
<td><strong>Axapta (AX) and Navision (NAV)</strong>: Microsoft Dynamics AX is an adaptable business management solution to streamline the business practices. Microsoft Dynamics NAV is basically designed for small and medium size companies. It is a cost effective solution that can be customized for organizations.</td>
</tr>
</tbody>
</table>

(c) The following three parameters would help in planning a documentation process of IS Audit:

(i) The importance of planning and understanding the planning process requires identifying three planning questions:

- **Knowing Your Resources**: The three basic resources are: time, people, money. One has to check for their availability and affordability.
- **Defining the Scope and Audience**: The same report may undergo significant changes depending on the character of the report and nature of the audience. Presentation on Balance Sheet made to bankers and to investors would be quite different in content and focus.
- **Using a Scope Definition Report**: It is critical to know how to complete a Scope Definition Report. This report helps in developing a workable schedule for completing the project.

(ii) The Documentation Writer: The qualities and skills that the documentation writer would need. The requirement may often be legal in nature.

(iii) Rules to guide documentation writing: The four steps of writing documentation...
namely, writing in active voice, giving the consequences, writing from general to specific, consistency and writing online documentation.

Ans.5

(a) **Virus:** A virus is a program (usually destructive) that attaches itself to a legitimate program to penetrate the operating system. The virus destroys application programs, data files, and operating systems in a number of ways. One common technique for the virus is to simply replicate itself over and over within the main memory, thus destroying whatever data or programs are resident. One of the most insidious aspects of a virus is its ability to spread throughout the system and to other systems before perpetrating its destructive acts.

The policy and procedural controls that can be recommended for ensuring control over virus proliferation and damage are given as follows:

- The Security Policy should address the virus threats, systems vulnerabilities and controls. A separate section on anti-virus is appropriate to address the various degrees of risks and suitable controls thereof.
- Anti-virus awareness and training on symptoms of attacks, methods of reducing damage, cleaning and quarantining should be given to all employees.
- Hardware installations and associated computing devices should be periodically verified for parameter settings.
- As a part of SDLC Controls, the development area should be free of viruses and sufficient safeguards must be in place to secure the area from viruses.
- Provision of drives to read media should be restricted to certain controlled terminals and should be write-protected.
- Network access to the Internet should be restricted preferably to stand-alone computers.
- Networks should be protected by means of firewalls that can prevent entry of known viruses.
- The servers and all terminals must have rated anti-virus software installed with sufficient number of user licenses.
- Procedures should ensure that systematic updates are applied to all anti-virus installations at frequent intervals.
- External media such as disks, CDs, tapes need to be avoided. If necessary such media should be scanned on a stand-alone machine and certified by the department.
- Vendors and consultants should not be allowed to run their demonstrations and presentations on organizational systems.
• All new software acquisitions should follow a controlled procedure of centralized acquisition and testing for viruses.
• Patches to operating systems and other software and upgrades thereof should be acquired from authentic sources and scanned before installation.
• Reporting and incident handling procedures should be in place to suitably handle virus incidents and eradicate them at the earliest.
• An effective backup plan must be implemented and monitored to ensure that back-up media is not infected and preferably encrypted. Only new media must be used for back-up purposes.

(b) "Electronic Record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche. [Section 7]

Retention of Electronic Records:

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form. -
   (a) the information contained therein remains accessible so as to be usable for a subsequent reference;
   (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;
   (c) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

However,

this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records. Publication of rules, regulation, etc. in Electronic Gazette.

(c) Major constraints, which come in the way of operating a MIS are given as follows:
• Non-availability of experts, who can diagnose the objectives of the organization and provide a desired direction for installing and operating a system. This problem may be overcome by grooming internal staff, which should be preceded by proper selection and training.
• Experts usually face the problem of selecting the sub-system of MIS to be installed and operated upon. The criteria, which should guide the experts, depending upon the need and importance of a function for which MIS can be installed first.
• Due to varied objectives of business concerns, the approach adopted by experts for designing and implementing MIS is a non-standardized one.
• Non-availability of cooperation from staff is a crucial problem, which should be handled tactfully. This task should be carried out by organizing lecturers, 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.

Ans.6
(a) The unique nature of each LAN makes it difficult to define standard testing procedures to effectively perform a review. The reviewer/IS Auditor should identify the following prior to commencing a LAN review:
• LAN topology and network design;
• Significant LAN components (such as servers and modems);
• Network topology (including internal LAN configuration as well as interconnections to other LANs, WANs or public networks);
• LAN uses, including significant traffic types and main applications used over the network;
• LAN administrator; and
• Significant groups of LAN users.
In addition, the reviewer should gain an understanding of the following:
• Functions performed by the LAN Administrator;
• The company’s division or department procedures and standards relating to network design support, naming conventions and data security; and
• LAN transmission media and techniques, including bridges, routers and gateways.
Understanding the above information should enable the reviewer to make an assessment of the significant threats to the LAN, together with the potential impact and probability of occurrence of each threat. Having assessed the risks to the LAN, the reviewer should evaluate the controls used to minimize the risks.

(b) Steps in Information Technology Audit: Different audit organizations go about IT auditing in different ways and individual auditors have their own favourite ways of working. However, it can be categorized into six major stages:
(i) Scoping and pre-audit survey: Auditors determine the main area/s of focus and any
areas that are explicitly out-of-scope, based normally on some form of risk-based assessment. Information sources at this stage include background reading and web browsing, previous audit reports, pre audit interview, observations and, sometimes, subjective impressions that simply deserve further investigation.

(ii) Planning and preparation: During this stage, the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan or risk-control matrix.

(iii) Fieldwork: It is related to gathering the evidence by interviewing staff and managers, reviewing documents, printouts and data, observing processes etc.

(iv) Analysis: This step involves desperately sorting out, reviewing and trying to make sense of all that evidence gathered earlier. SWOT (Strengths, Weaknesses, Opportunities, and Threats) or PEST (Political, Economic, Social, Technological) techniques can be used for analysis.

(v) Reporting: Reporting to the management is done after analysis of data gathered and analysis.

(vi) Closure: Closure involves preparing notes for future audits and following up management to complete the actions they promised after previous audits.

(c) Service Auditor's Report under SAS 70: The most effective ways a service organization can communicate information about its controls is through a service Auditor’s Report. There are two types of Service Auditor’s Report: Type I and Type II.

A Type I report describes the service organizations description of controls at a specific point in time (e.g. June 30, 2011). A type II report not only includes the service organization description of controls, but also includes detailed testing of the service organization’s controls over a minimum six month period (e.g. January 1, 2011 to June 30, 2011). The contents of each type of report are described in the following table:

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Report Contents</th>
<th>Type I Report</th>
<th>Type II Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Independent service auditor’s report (i.e. opinion)</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>2.</td>
<td>Service organization’s description of controls</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>3.</td>
<td>Information provided by the independent service auditor; includes a description</td>
<td>Optional</td>
<td>Included</td>
</tr>
<tr>
<td></td>
<td>of the service auditor’s tests of operating effectiveness and the results of those tests.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Other information provided by the service organization (e.g. glossary of terms)</td>
<td>Optional</td>
<td>Optional</td>
</tr>
</tbody>
</table>
In a Type I report, the service auditor will express an opinion on (1) whether the service organization’s description of its controls presents fairly, in all material respects, the relevant aspects of the service organizations controls that had been placed in operation as of a specific data and (2) whether the controls were suitably designed to achieve specified control objectives.

In a type II report, the service auditor will express an opinion on the same items noted above in a type I report, and (3) whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.

Ans.7

(a) **Data Dictionary**: A data dictionary is a computer file that contains descriptive information about the data items in the files of a business information system. Thus, a data dictionary is a computer file about data. Each computer record of a data dictionary contains information about a single data item used in a business information system. This information may include:

- Codes describing the data item’s length (in characters), data type (alphabetic, numeric, alphanumeric, etc.), and range (e.g., values from 1 to 99 for a department code)
- The identity of the source document(s) used to create the data item.
- The names of the computer files that store the data item.
- The names of the computer programs that modify the data item.
- The identity of the computer programs or individuals permitted to access the data item for the purpose of file maintenance, upkeep, or inquiry.
- The identity of the computer programs or individuals not permitted to access the data item.

(b) **Risk Mitigation Measures**: In risk mitigation, there is a term called, Cause analysis, which identifies events and their impact on losses. Cause models help in the implementation of risk mitigation measures. In addition to establishing causal relationship, other risk mitigation measures are:

- Self assessment;
- Calculating reserves and capital requirements;
- Creating culture supportive of risk mitigation;
- Strengthening internal controls, including internal and external audit of systems, processes and controls, including is audit and assurance);
• Setting up operational risks limits (so business will have to reduce one or more of frequency of loss, severity of loss or size of operations);
• Setting up independent operational risk management departments;
• Establishing a disaster recovery plan and backup systems;
• Insurance; and
• Outsourcing operations with strict service level agreements so that operational risk is transferred.

Out of these afore mentioned measures, generally the following common mitigation techniques are used:

• **Insurance**: An organization may buy insurance to mitigate such risk. Under the scheme of the insurance, the loss is transferred from the insured entity to the insurance company in exchange of a premium. However while selecting such an insurance policy one has to look into the exclusion clause to assess the effective coverage of the policy.

• **Outsourcing**: The organization may transfer some of the functions to an outside agency and transfer some of the associated risks to the agency. One must make careful assessment of whether such outsourcing is transferring the risk or is merely transferring the management process.

• **Service Level Agreements**: Some of risks can be mitigated by designing the service level agreement. This may be entered into with the external suppliers as well as with the customers and users. The service agreement with the customers and users may clearly exclude or limit responsibility of the organization for any loss suffered by the customer and user consequent to the technological failure.

Here, it is noteworthy that the organization should not be so obsessed with mitigating the risk that it seeks to reduce the systematic risk - the risk of being in business. The risk mitigation tools available should not eat so much into the economics of business that the organization may find itself in a position where it is not earning adequate against the efforts and investments made.

(c) **Software Process Maturity**: This is the extent to which a specific process is explicitly defined, managed, measured, controlled, and effective. Maturity implies a potential for growth in capability and indicates both the richness of an organization’s software process and the consistency with which it is applied in projects throughout the organization.

As a software organization gains in software process maturity, it institutionalizes its software process via policies, standards, and organizational structures. Institutionalization entails building an infrastructure and a corporate culture that supports the methods,
practices, and procedures of the business so that they endure after those who originally defined them have gone.

(d) Preventative Information Protection: It is based on the use of security controls, which itself is a group of three types of controls such as Physical, Logical, and Administrative. Theses are briefly given as follows:

- Physical controls deal with Doors, Locks, Guards, Floppy Disk Access Locks, Cables locking systems to desks/ walls, CCTV, Paper Shredders, Fire Suppression Systems,
- Logical controls deal with Passwords, File Permissions, Access Control Lists, Account Privileges, Power Protection Systems, and
- Administrative controls deal with Security Awareness, User Account Revocation, and Policy.

Restorative Information Protection: If an organization cannot recover or recreate critical information systems in an acceptable time period, the organization will suffer and possibly have to go out of business. Hence, the key requirement of any restorative information system protection plan is that the information systems can be recovered. The claim of back program to backup data automatically cannot be reliable. It has so many problems. The restorative information protection program must address the following:

- Whether the recovery process has been evaluated and tested recently?
- The time taken for restoration,
- The quantum of productivity loss,
- The strict adherence of plan, and
- The time needed to input the data changes since the last backup.

(e) Objectives of Information Technology Act 2000: The objectives of Information Technology Act 2000 are given as follows:

- To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as “electronic commerce” in place of paper based methods of communication;
- To give legal recognition to Digital signatures for authentication of any information or matter, which requires authentication under any law;
- To facilitate electronic filing of documents with Government departments;
- To facilitate electronic storage of data;
- To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions;
- To give legal recognition for keeping of books of accounts by banker’s in electronic form; and
- To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker’s Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934.
ABC Udyog, a leading automobile company is having several manufacturing units, located in different parts of the world and manufacturing several types of automobiles. The units are working on legacy systems using an internet and collating information, but using different software and varied platforms (Operating Systems) which do not allow communication with each other. This results in huge inflow of duplicate data.

The company wishes to centralize and consolidate the information flowing from its manufacturing units in a uniform manner across various levels of the organizations, so that the necessary data required for preparing MIS reports, budget, and profit/loss accounts etc. could be available timely.

The company decided to engage XYZ consultancy Services for the development of new system. Being a Senior Project Leader of the Consultancy Services, you are entrusted with the responsibilities of handling this project.

Read the above carefully and answer the following with justifications:

(a) What areas are required to be studied in order to know about the present system? Write the problems that the ABC Udyog is presently facing.

(5 Marks)

(b) Will you suggest ERP solution to overcome the problems? If yes, explain why.

(5 Marks)

(c) What kind of training you will recommend to enrich the human resources for effective utilization of the proposed new system and standards?

(5 Marks)

(d) What are various backup techniques? Which backup technique, you will recommend and why?

(5 Marks)

Q-2

(a) Define the term “Information”. Discuss various important attributes that are required for useful and effective information.

(8 Marks)
(b) At the end of analysis phase, the System Analyst prepares a document called “Systems Requirement Specifications (SRS)”. Write the contents of SRS.  

(4 Marks)

(c) What is the significance of Post Implementation Review? How it is performed?  

(4 Marks)

Q-3  

(a) How will you define a risk assessment? Briefly explain various review areas to be focused upon.  

(8 Marks)

(b) Following are involved in the System Development Life Cycle (SDLC). Discuss their roles:  

(i) Project Manager  
(ii) System Analyst  
(iii) Database Administrator (DBA)  
(iv) IS Auditor  

(4 Marks)

(c) Draw the flowchart to find the sum of first 50 even numbers, starting from 2.  

(4 Marks)

Q-4  

(a) Explain the various general components of Disaster Recovery Plan.  

(6 Marks)

(b) What is Data Privacy? Explain the major techniques that are used to address Privacy Protection for IT Systems.  

(6 Marks)

(c) In what ways, an audit trails is used to support security objectives? Describe each one of them.  

(4 Marks)

Q-5  

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

(8 Marks)

(b) Describe the advantage and disadvantage of Continuous Auditing Techniques in brief.  

(4 Marks)
Q-6

(a) What is the significance of a Business Impact Analysis? Enumerate the tasks to be undertaken in this analysis. In what ways can the information be obtained for this analysis? (8 Marks)

(b) Give the hierarchy of Information Security Policies and discuss each one of them. (4 Marks)

(c) Describe the composition and powers of Cyber Regulatory Appellate Tribunal. (4 Marks)

Q-7

Write Short Notes on any FOUR of the following:

(a) Objectives of an Operating System (4 Marks)

(b) Information System Maintenance (4 Marks)

(c) Client/Server Technology (4 Marks)

(d) Locks on Doors with respect to Physical Access Control (4 Marks)

(e) HIPAA (4 Marks)
(a) The following are the major areas, which should be studied in depth in order to understand the present system:

(i) **Review historical aspects:** A brief history of the organization is a logical starting point for an analysis of the present system. The historical facts shall identify the major turning points and milestones that have influenced its growth. A review of annual reports and organization charts can identify the growth of management levels as well as the development of various functional areas and departments.

(ii) **Analyze inputs:** A detailed analysis of the present inputs is important since they are basic to the manipulation of data. Source documents are used to capture the originating data for any type of system.

(iii) **Review data files maintained:** The analyst should investigate the data files maintained by each department, noting their number and size, where they are located, who uses them and the number of times per given time interval these are used.

(iv) **Review methods, procedures and data communications:** A system analyst also needs to review and understand the present data communications used by the organization. S/he must review the types of data communication equipments, including data interface, data links, modems, dial-up and leased lines and multiplexers.

(v) **Analyze outputs:** The outputs or reports should be scrutinized carefully by the system analysts in order to determine ‘how well they will meet the organization’s needs’.

(vi) **Review internal controls:** A detailed investigation of the present information system is not complete until internal controls are reviewed. Locating the control points helps the analyst to visualize the essential parts and framework of a system.

(vii) **Model the existing physical system and logical system:** As the logic of inputs, methods, procedures, data files, data communications, reports, internal controls and other important items are reviewed and analyzed in a top down manner; the process must be properly documented.

(viii) **Undertake overall analysis of present system:** The final phase of the detailed investigation includes the analysis of the present work volume; the current personnel requirements; the present benefits and costs and each of these must be investigated thoroughly.

Presently, ABC Udyog is facing the following major problems:

- The company having its branches all over the world, is engaged in manufacturing of several types of automobiles. The units are working on legacy systems using an internet
and collating information. Each unit is using different type of software on varied platforms (operating systems), therefore, they are not able to communicate with each other. Because of this reason, there is a huge inflow of data which could not be consolidated for analysis.

- Lack of communication among units has resulted into duplication of the data entry, which is very costly. In addition, timely availability of necessary and relevant data required for the preparation of MIS Reports, budget, profit/loss account etc. is another important concern in the present system.

- It is confronted with the problem of centralizing and consolidating the information flowing in from its various units in uniform manner across various levels of the organization. Hence, there is an urgent need of a system that would entrust the company to address these important issues.

(b) Yes, we recommend that ABC Udyog should implement ERP Solution to overcome the above mentioned problems. ERP implementation will bring different business functions, personalities, procedures, ideologies and philosophies on one platform. In addition, ERP effectively integrates different modules and brings worthwhile and beneficial changes throughout the organization.

Following are the major reasons to implement ERP solutions:

- It provides multi-platform, multi-facility, multi-mode manufacturing, multi-currency, multi-lingual facilities.

- It supports strategic and business planning activities, operational planning and execution activities etc. All these functions are effectively integrated for flow and update of information immediately upon entry of any information.

- It facilitates company-wide Integrated Information System covering all functional areas like manufacturing, selling and distribution, payables, receivables, inventory, accounts, human resources, purchases etc.

- It provides complete integration of systems not only across the departments but also across the companies under the same management.

- It is the solution for better project management.

- It allows automatic introduction of the latest technologies like Electronic Fund Transfer (EFT), Internet, Intranet, Video conferencing, E-Commerce etc.

- It eliminates most business problems like material shortages, productivity enhancements, customer service, cash management, inventory problems, quality problems, prompt delivery etc.
• It provides intelligent business tools like decision support system, Executive information system, Data mining and easy working systems to enable better decisions.

(c) The human resources involved in the proposed new system and standards can be enriched by the following activities/trainings:

• Training Personnel: A system can succeed or fail depending on the way it is operated and used. Therefore, the quality of training received by the personnel involved with the system in various capacities helps in the successful implementation of the proposed system and standards. Thus, training is a major component of systems implementation. When a new system is acquired, which often involves new hardware and software, both users and computer experts need training organized by the vendor through hands-on learning techniques.

• Training Systems Operators: The effective implementation of new systems and standards also depend on the computer-centre personnel, who are responsible for keeping the equipment running as well as for providing the necessary support services. Their training must ensure that they are able to handle all possible operations, both routine and extra-ordinary. As part of their training, operators should be given a trouble shooting list that identifies possible problems and remedies for them. Training also involves familiarization with run procedures, which involve working through the sequence of activities needed to use a new system on an on-going basis.

• User’s training: User’s training deals with the operation of the system itself. The users need to have the skill for using the functionality relevant to their roles. They should understand the basic concepts of ERP and also how to perform the day-to-day activities in the ERP system.

• Managers’ Training: Others, who require training, include managers, who should have at least an appreciation of ‘what the system does’. Ideally, the project manager should have a good understanding of all the aspects of the system so that s/he can be effective in dealing with any issues raised. It is also required to have managers directly involved in evaluating the effectiveness of training activities because training deficiencies can translate into reduced user productivity level.

• System Administrators’ Training: The system administrators need to be able to setup the system and then maintain it. They will require knowledge about how to handle system security and deal with technical problems. They will need to develop a level of understanding of the functionality so that, at some stage after implementation when the project team is disbanded, they are able to manage the system smoothly.

• Training other Personnel: A selected number of people will require more specific technical training so that they can design databases, write scripts, manage users, generate reports and run query in the database for specific requirements.
(d) Various back-up techniques are described as follows:

(i) **Full Backup**: A full backup captures all the files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data.

(ii) **Incremental Backup**: An incremental backup captures files that were created or changed since the last backup, regardless of backup type. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space.

Normally, incremental backup are very difficult to restore. You will have to start with recovering the last full backup, and then recovering from every incremental backup taken since.

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

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

(iv) **Mirror back-up**: A mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they can not be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

In the present system, we recommend incremental backup because ABC Udyog has manufacturing units working on the legacy systems. Secondly, incremental backup is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space, which is the current need of the automobile company.

Ans.2

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

**Attributes of Information**: The important attributes of useful and effective information are as follows:

- **Availability**: This is a very important property of information. If information is not available at the time of need, it is useless. Data is organized in the form of facts and figures in databases and files from where various information is derived for useful purpose.

- **Purpose**: Information must have purposes at the time, it is transmitted to a person or machine, otherwise it is simple data. Information communicated to people has a variety of purposes because of the variety of activities performed by them in business organizations. The basic purpose of information is to inform, evaluate, persuade, and organize.

- **Mode and format**: The modes of communicating information to humans are sensory (through sight, hear, taste, touch and smell) but in business they are either visual, verbal or in written form. Format of information should be so designed that it assists in decision making, solving problems, initiating planning, controlling and searching.

- **Decay**: Value of information usually decays with time and usage and so it should be refreshed from time to time. For example, we access the running score sheet of a cricket match through Internet sites and this score sheet is continually refreshed at a fixed interval or based on status of the state.

- **Rate**: The rate of transmission/reception of information may be represented by the time required to understand a particular situation. Quantitatively, the rate for humans may be measure by the number of numeric characters transmitted per minute, such as sales reports from a district office. For machines the rate may be based on the number of bits of information per character (sign) per unit of time.

- **Frequency**: The frequency with which information is transmitted or received affects its value. Financial reports prepared weekly may show so little changes that they have small value, whereas monthly reports may indicate changes big enough to show problems or trends.

- **Completeness**: The information should be as complete as possible. The classical ROI or Net Present Value (NPV) models just provide a point estimate and do not give any indication of the range within which these estimates may vary. Hartz’s model for investment decisions provides information on mean, standard deviation and the shape
of the distribution of ROI and NPV. With this complete information, the manager is in a much better position to decide whether or not to undertake the venture.

- **Reliability**: It is just not authenticity or correctness of information; rather technically it is a measure of failure or success of using information for decision making. If information leads to correct decision on many occasions, we say the information is reliable.

- **Validity**: It measures the closeness of the information to the purpose which it purports to serve. For example, some productivity measure may not measure, for the given situation, what they are supposed to do e.g., the real rise or fall in productivity. The measure suitting the organization may have to be carefully selected or evolved.

- **Quality**: Quality refers to the correctness of information. Information is likely to be spoiled by personal bias. For example, an over-optimistic salesman may give rather too high estimates of the sales. This problem, however, can be circumvented by maintaining records of salesman’s estimates and actual sales and deflating or inflating the estimates in the light of this.

- **Transparency**: If information does not reveal directly ‘what we want to know for decision-making’, it is not transparent. For example, total amount of advance does not give true picture of utilization of fund for decision about future course of action; rather deposit-advance ratio is perhaps more transparent information in this matter.

- **Value of information**: It is defined as difference between the value of the change in decision behavior caused by the information and the cost of the information. In other words, given a set of possible decisions, a decision-maker may select one on basis of the information at hand. If new information causes a different decision to be made, the value of the new information is the difference in value between the outcome of the old decision and that of the new decision, less the cost of obtaining the information.

- **Adequacy**: To be useful, an information must be adequate so that the desired actions can be initiated. Required information should flow on different directions within the organization and to and from its environment. Further, the type of information that flows within the organization or across, it should have adequate and relevant contents.

(b) At the end of the analysis phase, the System Analyst prepares a document called “Systems Requirement Specifications (SRS)”. A SRS contains the following:

- **Introduction**: Goals and Objectives of the software context of the computer-based system;
• **Information Description:** Problem description; Information content, flow and structure; Hardware, software, human interfaces for external system elements and internal software functions.

• **Functional Description:** Diagrammatic representation of functions; Processing narrative for each function; Interplay among functions; Design constraints.

• **Behavioral Description** : Response to external events and internal controls

• **Validation Criteria:** Classes of tests to be performed to validate functions, performance and constraints.

• **Appendix:** Data flow / Object Diagrams; Tabular Data; Detailed description of algorithms charts, graphs and other such material.

• **SRS Review** : It contains the following:

  - The development team makes a presentation and then hands over the SRS document to be reviewed by the user or customer.

  - The review reflects the development team’s understanding of the existing processes. Only after ensuring that the document represents existing processes accurately, should the user sign the document. This is a technical requirement of the contract between users and development team / organization.

(c) A Post Implementation Review answers the question “Did we achieve what we set out to do in business terms?” It examines the efficacy of all elements of the working business solution to see if further improvements can be made to optimize the benefits delivered.

After a development project is completed, a post implementation review should be performed to determine if the anticipated benefits were achieved. Reviews help to control project development activities. The full scope of a post implementation review (“PIR”) will depend largely on the scale and complexity of the project.

The post implementation review is performed jointly by the project development team and the appropriate end users. Alternatively, an independent group not associated with the development process, either internal or external, should carry out the audit, to meet the following objectives:

• Business objectives e.g. delivered within budget and deadline; producing predicted savings and benefits, etc.;

• User expectations e.g. user friendly, carries the workload, produces the required outputs, good response time, reliable, good ergonomics, etc.;

• Technical requirements e.g. capable of expansion, easy to operate and maintain, interfaces with other systems, low running cost, etc.
The PIR is undertaken after any changes and tuning that are necessary to achieve a stable system have been completed, and any significant problems have had a chance to surface. Sufficient time should also be allowed for the system's users to become familiar with it. These criteria should be met between six and twelve months after implementation. If the PIR is delayed beyond twelve months there will be an increasing risk that changing requirements - leading to further releases of the system - will obscure the outcome from the original development; also, that the need for a PIR will be overtaken by other priorities.

Ans.3

(a) Risk assessment is the analysis of threats to resources (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status in the minimum time in case of a disaster. Risk assessment is a useful technique to assess the risks involved in the event of unavailability of information, to priorities applications, identify exposures and develop recovery scenarios.

The areas to be focused upon for review are given below:

(a) Prioritization: All applications are inventoried and critical ones identified. Each of the critical applications is reviewed to assess its impact on the organization, in case a disaster occurs. Subsequently, appropriate recovery plans are developed.

(b) Identifying critical applications: Amongst the applications currently being processed the critical applications are identified. Further analysis is done to determine specific jobs in the applications which may be more critical. Even though the critical value would be determined based on its present value, future changes should not be ignored.

(c) Assessing their impact on the organization: Business continuity planning should not concentrate only on business disruption but should also take into account other organizational functions which may be affected. The areas to be considered include:
   • Legal liabilities;
   • Interruptions of customer services;
   • Possible losses; and
   • Likelihood of fraud and recovery procedures.

(d) Determining recovery time-frame: Critical recovery time period is the period of time in which business processing must be resumed before the organization incurs severe losses. This critical time depends upon the nature of operations. It is essential to involve the end users in the identification of critical functions and critical recovery time period.
(e) **Assess Insurance coverage:** The information system insurance policy should be a multiperil policy, designed to provide various types of coverage. Depending on the individual organization and the extent of coverage required, suitable modifications may be made to the comprehensive list, which include various items namely, hardware facilities, software reconstruction, extra expenses, business interruption, valuable paper and records, Errors and omissions, fidelity coverage, and media transportation.

(f) **Identification of exposures and implications:** It is not possible to accurately predict as to when and how a disaster would occur. So, it is necessary to estimate the probability and frequency of disaster.

(g) **Development of recovery plan:** The plan should be designed to provide for recovery from total destruction of a site.

(b) (i) **Project Manager:** A project manager is normally responsible for more than one project and liaisons with the client or the affected functions. S/he is responsible for delivery of the project within the time and budget and periodically reviewing the progress of the project with the project leader and his/her team.

(ii) **Systems Analyst:** The systems/business analysts’ main responsibility is to conduct interviews with users and understand their requirements. S/he is a link between the users and the programmers to convert the users requirements in the system requirements and plays a pivotal role in the Requirements analysis and Design phase.

(iii) **Database Administrator (DBA):** The data in a database environment has to be maintained by a specialist in database administration so as to support the application program. The DBA handles multiple projects; ensures the integrity and security of information stored in the database and also helps the application development team in database performance issues. Inclusion of new data elements has to be done only with the approval of the database administrator.

(iv) **IS Auditor:** As a member of the team, IS Auditor ensures that the application development also focuses on the control perspective. He should be involved at the Design Phase and the final Testing Phase to ensure the existence and the operations of the Controls in the new software.
Ans.4

(a) The general components of a disaster recovery plan are given as follows:

- The conditions for activating the plans, which describe the process to be followed before each plan, are activated.
- Emergency procedures, which describe the actions to be taken following an incident which jeopardizes business operations and/ or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities e.g. police, fire, services and local government.
- Fallback procedures, which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time-scale.
- Resumption procedures, which describe the actions to be taken to return to normal business operations.
• A maintenance schedule, which specifies how and when the plan will be tested, and the process for maintaining the plan.

• Awareness and education activities, which are designed to create an understanding of the business continuity, process and ensure that the business continues to be effective.

• The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.

• Contingency plan document distribution list.

• Detailed description of the purpose and scope of the plan.

• Contingency plan testing and recovery procedure.

• List of vendors doing business with the organization, their contact numbers and address for emergency purposes.

• Checklist for inventory taking and updating the contingency plan on a regular basis.

• List of phone numbers of employees in the event of an emergency.

• Emergency phone list for fire, police, hardware, software, suppliers, customers, back-up location, etc.

• Medical procedure to be followed in case of injury.

• Back-up location contractual agreement, correspondences.

• Insurance papers and claim forms.

• Primary computer centre hardware, software, peripheral equipment and software configuration.

• Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.

• Alternate manual procedures to be followed such as preparation of invoices.

• Names of employees trained for emergency situation, first aid and life saving techniques.

• Details of airlines, hotels and transport arrangements.

The answer stated above described general components of a Disaster Recovery Plan (DRP). However, these components can be categorized under the four heads namely, Emergency Plan, Recovery Plan, Backup Plan and Test Plan. The solution to the question can also be presented as follows:

The general components of the disaster recovery plan which is described as the contingency measures that organizations have adopted at key computing sites to recover from, or to prevent any monumentally bad event or disaster are as follows:
• **Emergency Plan:** This part of the Disaster Recovery Plan (DRP) outlines the actions to be undertaken immediately after a disaster occurs. It identifies the personnel to be notified immediately, for example, fire service, police, management, insurance company etc. It provides guidelines on shutting down the equipment, termination of power supply, removal of storage files and disks, if any. It sets out evacuation procedures like sounding the alarm bell, activating fire extinguishers, evacuation of personnel. It also provides return procedures as soon as the primary facility is ready for operation like backing up data files at offsite, deleting data from disk drives at third party’s site, relocation of proper versions of backup files, etc.

• **Recovery Plan:** This part of the DRP sets out how the full capabilities will be restored. A recovery committee is constituted. Preparing specifications of recovery like setting out priorities for recovery of application systems, hardware replacement etc. will be the responsibility of the Recovery Committee. The following steps may be carried out under this plan:

  (i) An inventory of the hardware, application systems, system software, documentation etc. must be taken.

  (ii) Criticality of application systems to the organization and the importance of their loss must be evaluated. An indication must be given of the efforts and cost involved in restoring the various application systems.

  (iii) An application systems hierarchy must be spelt out.

  (iv) Selection of a disaster recovery site must be made. A reciprocal agreement with another organization having compatible hardware and software could be made.

  (v) A formal back agreement with another company must be made. This should cover the periodical exchange of information between the two sites regarding changes to hardware/software, the time and duration of systems availability, modalities of testing the plan etc.

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

• **Test Plan:** To provide assurance that the disaster recovery plan is complete, it should be tested, several times. A disaster recovery test plan contains information for simu-
lating various levels of disasters and recording an organization’s ability to cover. Any needed recovery actions that are not specified in the plan should be added.

(b) Data Privacy: This refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data. Privacy problems exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. The most common sources of data that are affected by data privacy issues are:

- Health information,
- Criminal justice,
- Financial information,
- Genetic information, and
- Location information.

Privacy protection for IT systems: Increasingly, as heterogeneous information systems with different privacy rules are interconnected, technical control and logging mechanisms (policy appliances) will be required to reconcile, enforce and monitor privacy policy rules (and laws) as information is shared across systems and to ensure accountability for information use. There are several technologies to address privacy protection in enterprise IT systems. These falls into two categories: communication and enforcement.

(i) Policy Communication
- P3P – This is the Platform for Privacy Preferences. P3P is a standard for communicating privacy practices and comparing them to the preferences of individuals.

(ii) Policy Enforcement
- XACML - The extensible Access Control Markup Language (XACML) together with its Privacy Profile is a standard for expressing privacy policies in a machine readable language which a software system can use to enforce the policy in enterprise IT systems.
- EPAL - The Enterprise Privacy Authorization Language (EPAL) is very similar to XACML, but is not yet a standard.
- WS-Privacy - “Web Service Privacy” will be a specification for communicating privacy policy in web services. For example, it may specify how privacy policy information can be embedded in the SOAP envelope of a web service message.

(c) Audit trails can be used to support security objectives in three ways:
- Detecting unauthorized access to the system,
Facilitating the reconstruction of events, and
Promoting personal accountability.

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

(i) **Detecting Unauthorized Access**: Detecting unauthorized 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 attempting 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. 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 unauthorized access was accomplished, or attempted and failed.

(ii) **Reconstructing 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 to avoid similar situations in the future.

(iii) **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 behavior. Individual accountability will normally increase because their actions will be recorded in an audit log.

Ans.5

(a) Various control measures that will be checked by the system auditor to minimize threats, risks and exposures in a computerized system are discussed below:

(i) **Lack of integrity**: Control measures to ensure integrity include implementation of security policies, procedures and standards, use of encryption techniques and digital signatures, inclusion of data validation, editing, and reconciliation techniques for inputs, processes and outputs, updated antivirus software, division of job and layered control to prevent impersonation, use of disk repair utility, implementation of user identification, authentication and access control techniques, backup of system and data, security awareness programs and training of employees, installation of audit trails, and audit of adequacy of data integrity etc.

(ii) **Lack of confidentiality**: Control measures to ensure confidentiality include use of encryption techniques and digital signatures, implementation of a system of accountability by logging and journaling system activity, development of a security policy, procedures and standards, employee awareness and training, requiring employees to sign a non-disclosure undertaking, implementation of physical and logical access con-
(iii) **Lack of system availability:** Control measures to ensure availability include implementation of software configuration controls, a fault tolerant hardware and software for continuous usage and an asset management software to control inventory of hardware and software, insurance coverage, system backup procedure to be implemented, implementation of physical and logical access controls, use of passwords and other authentication techniques, incident logging and report procedure, backup power supply, updated antivirus software, security awareness programs and training of employees, installation of audit trails, audit of adequacy of availability safeguards.

(iv) **Unauthorized users attempt to gain access to the system and system resources:** Control measures to stop unauthorized users to gain access to system and system resources include identification and authentication mechanism such as passwords, biometric recognition devices, tokens, logical and physical access controls, smart cards, disallowing the sharing of passwords, use of encryption and checksum, display of warning messages and regular audit programs. Data transmitted over a public or shared network may be intercepted by an unauthorized user, security breaches may occur due to improper use or bypass of available security features, strong identification and authentication mechanisms such as biometric, tokens, layered system access controls, documentation procedures, quality assurance controls and auditing.

(v) **Hostile software e.g. virus, worm, Trojan horses, etc.:** Establishment of policies regarding sharing and external software usage, updated anti-virus software with detection, identification and removal tools, use of diskless PCs and workstations, installation of intrusion detection and prevention tools and network filter tools such as firewalls, use of checksums, cryptographic checksums and error detection tools for sensitive data, installation of change detection tools, protection with permissions required for the 'write' function.

(vi) **Disgruntled employees:** Control measures to include installation of physical and logical access controls, logging and notification of unsuccessful logins, use of disconnect feature on multiple unsuccessful logins, protection of modem and network devices, installation of one time use only passwords, security awareness programs and training of employees, application of motivation theories, job enrichment and job rotation.

(vii) **Hackers and computer crimes:** Control measures to include installation of firewall and intrusion detection systems, change of passwords frequently, installation of one
time use passwords, discontinuance of use of installed and vendor installed passwords, use of encryption techniques while storage and transmission of data, use of digital signatures, security of modem lines with dial back modems, use of message authentication code mechanisms, installation of programs that control change procedures, and prevent unauthorized changes to programs, installation of logging feature and audit trails for sensitive information.

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

(b) **Continuous Auditing Technique**: Continuous auditing enables auditors to shift their focus from the traditional ‘transaction’ audit to the ‘system and operations’ audit.

**Advantages**: Some of the advantages of continuous audit techniques are as under:

- Timely, comprehensive and detailed auditing: Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analyzed rather than examining the inputs and the outputs only.

- Surprise test capability: As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.

- Information to system staff on meeting of objectives: Continuous audit techniques provides information to systems staff regarding the testing to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.

- Training for new users: Using the ITFs, new users can submit data to the application system, and obtain feedback on any mistakes they make via the system’s error reports.

**Disadvantages**: The following are some of the disadvantages and limitations of the continuous audit system:

- Auditors should be able to obtain resources required from the organization to support development, implementation, operation, and maintenance of continuous audit techniques.

- Continuous audit techniques are more likely to be used if auditors are involved in the development work associated with a new application system.
• Auditors need the knowledge and experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.
• Continuous auditing techniques are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.
• Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.

(c) Following are the most commonly used techniques to access and evaluate risks:
• Judgment and intuition,
• The Delphi Approach,
• Scoring,
• Quantitative Techniques, and
• Qualitative Techniques.

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

(i) **Judgment and intuition:** In many situations, the auditors have to use their judgment and intuition for risk assessment. This mainly depends on the personal and professional experience of the auditors and their understanding of the system and its environment. Together with it, systematic education and ongoing professional updating is also required.

(ii) **The Delphi Approach:** This technique is used for obtaining a consensus opinion. A panel of experts is engaged and each expert is asked to give his opinion in a written and independent method. They enlist the estimate of the cost benefits and the reasons why a particular system is to be chosen, the risks and exposures of the system. These estimates are then complied together. The estimates falling within a pre-decided acceptable range are taken. The process may be repeated four times for revising estimates falling beyond the range. Then a curve is drawn taking all the estimates as points on the graphs. The median is drawn and this is the consensus opinion.

(iii) **The Scoring Approach:** In this approach, the risks in the system and their respective exposures are listed. Weights are then assigned to the risks and to the exposures depending on the severity, impact of occurrence and costs involved. The product of the risk weight with the exposure weight of every characteristic gives the weighted score. The sum of these weighted score gives the risk and exposure score of the system. System risks and exposures are then ranked according to the scores.

(iv) **Quantitative Techniques:** Quantitative techniques involve the calculating of an annual loss exposure value based on the probability of the event and the exposure in terms of estimated costs. This helps the organization to select cost effective solutions.
It is the assessment of potential damage in the event of occurrence of unfavorable events, keeping in mind how often such an event may occur.

(v) **Qualitative Techniques:** These are by far the most widely used approach to risk analysis. Probability data is not required and only estimated potential loss is used. Most qualitative risk analysis methodologies make use of a number of interrelated elements, namely, threats, vulnerabilities, and controls.

**Ans.6**

(a) **Business Impact Analysis:** Business Impact Analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. It enables the business continuity team to identify critical systems, processes, and functions, assess the economic impact of incidents and disasters that result in a denial of access to the system, services, and facilities, and assess the “pain threshold,” that is, the length of time business units can survive without access to the system, services, and facilities.

The business impact analysis is intended to help and understand the degree of potential loss (and various other unwanted effects), which could occur. This will cover not just direct financial loss, but other issues, such as reputation damage, regulatory effects, etc.

A number of tasks are to be undertaken in this phase as enumerated under:

(i) Identify organizational risks - This includes single point of failure and infrastructure risks. The objective is to identify risks and opportunities and to minimize potential threats that may lead to a disaster.

(ii) Identify critical business processes.

(iii) Identify and quantify threats/risks to critical business processes both in terms of outage and financial impact.

(iv) Identify dependencies and interdependencies of critical business processes and the order in which they must be restored.

(v) Determine the maximum allowable downtime for each business process.

(vi) Identify the type and the quantity of resources required for recovery e.g. tables, chairs, faxes, photocopiers, safes, desktops, printers, etc.

(vii) Determine the impact to the organization in the event of a disaster, e.g. financial reputation, etc.

There are a number of ways to obtain this information:

- Questionnaires,
- Workshops,
- Interviews,
(b) The hierarchy of various Information Security Policies is shown in the following figure:

Each of the Information Security Policy given in the above figure is briefly discussed below:

- **Information Security Policy** - This policy provides a definition of Information Security, its overall objective and the importance that applies to all users.

- **User Security Policy** - This policy sets out the responsibilities and requirements for all IT system users. It provides security terms of reference for Users, Line Managers and System Owners.

- **Acceptable Usage Policy** - This sets out the policy for acceptable use of email and Internet services.

- **Organizational Information Security Policy** - This policy sets out the Group policy for the security of its information assets and the Information Technology (IT) systems processing this information. Though it is positioned at the bottom of the hierarchy, it is the main IT security policy document.

- **Network & System Security Policy** - This policy sets out detailed policy for system and network security and applies to IT department users

- **Information Classification Policy** - This policy sets out the policy for the classification of information

- **Conditions of Connection** - This policy sets out the Group policy for connecting to their network. It applies to all organizations connecting to the Group, and relates to the conditions that apply to different suppliers’ systems.
(c) **Cyber Regulatory Appellate Tribunal:** As per Information Technology (Amendment) Act, 2008, the cyber regulation appellate tribunal shall consist of one person only called the Presiding Officer of the Tribunal who shall be appointed by the Central Government. The person must be qualified to be a Judge of a High Court or is or has been a member of Indian Legal Services in the post in Grade I of that service for at least three years. The Presiding Officer shall hold the office for a term of five years or upto a maximum age limit of 65 years, whichever is earlier.

Some of the powers specified are given as follows:

(i) Summoning and enforcing the attendance of any person and examining him on oath;
(ii) Requiring the discovery and production of documents or other electronic records;
(iii) Receiving evidence on affidavits;
(iv) Issuing commissions for examination of witnesses or documents;
(v) Reviewing the decisions;
(vi) Dismissing an application for default or deciding its ex party;
(vii) Any other matter which may be prescribed.

**Ans.7**

(a) **Objectives of an Operating System:** An operating system (OS) is a program that controls the execution of an application program and acts as an interface between the user of a computer and computer hardware. The purpose of an OS is to provide an environment in which a user can execute programs in a convenient and efficient manner. An operating system is an important part of almost every computer system. It is considered to be the backbone of a computer, managing both software and hardware resources. Operating systems are responsible for everything from the control and allocation of memory to recognizing input from external devices and transmitting output to computer displays. They also manage files on computer hard drives and control peripherals, like printers and scanners.

Major objectives/ functions of an operating system are given as follows:

- **Scheduling of Jobs:** Operating Systems can determine the sequence in which jobs are executed, using priorities established.
- **Managing Hardware and Software Resources:** They can first cause the user’s application program to be executed by loading it into primary storage and then cause the various hardware units to perform as specified by the application.
- **Maintaining System Security:** They may require users to enter a password - a group of characters that identifies users as being authorized to have access to the system.
- Enabling Multiple User Resource Sharing: They can handle the scheduling and execution of the application programs for many users at the same time, a feature called multiprogramming.
- Handling Interrupts: An interrupt is a technique used by the operating system to temporarily suspend the processing of one program in order to allow another program to be executed. Interrupts are issued when a program requests an operation that does not require the CPU, such as input or output, or when the program exceeds some predetermined time limit.
- Maintaining Usage Records: They can keep track of the amount of time used by each user for each system unit - the CPU, secondary storage, and input and output devices. Such information is usually maintained for the purpose of charging users’ departments for their use of the organization’s computing resources.

(b) Information System Maintenance: Maintaining the system is an important aspect of SDLC. As key personnel change positions in the organization, new changes will be implemented, which will require system updates. Most information systems require at least some modification after development. The need for modification arises from a failure to anticipate all requirements during system design and/or from changing organizational requirements.

Maintenance can be categorized in the following ways:
- Scheduled maintenance: Scheduled maintenance is anticipated and can be planned for. For example, the implementation of a new inventory coding scheme can be planned in advance.
- Rescue maintenance: 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.
- Corrective maintenance: Corrective maintenance deals with fixing bugs in the code or defects found. A defect can result from design errors, logic errors; coding errors, data processing and system performance errors. The need for corrective maintenance is usually initiated by bug reports drawn up by the end users. Examples of corrective maintenance include correcting a failure to test for all possible conditions or a failure to process the last record in a file.
- Adaptive maintenance: Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system. The term environment in this context refers to the totality of all conditions and influences which act from outside upon the system, for example, business rule, government policies,
work patterns, software and hardware operating platforms. The need for adaptive maintenance can only be recognized by monitoring the environment.

- Perfective maintenance: Perfective maintenance mainly deals with accommodating to new or changed user requirements and concerns functional enhancements to the system and activities to increase the system's performance or to enhance its user interface.

- Preventive maintenance: Preventive maintenance concerns activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system. The long-term effect of corrective, adaptive and perfective changes increases the system's complexity. As a large program is continuously changed, its complexity, which reflects deteriorating structure, increases unless work is done to maintain or reduce it. This work is known as preventive change.

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

Client/server is described as a ‘cost-reduction’ technology. Some of the Implementation examples of client/server technology are: Online banking application, internal call centre application, Applications for end-users that are stored in the server etc. Major characteristics that reflect the key features of a client/server system are given as follows:

- Client/server architecture consists of a client process and a server process that can be distinguished from each other.

- The client portion and the server portions can operate on separate computer platforms.

- Either the client platform or the server platform can be upgraded without having to upgrade the other platform.

- The server is able to service multiple clients concurrently; in some client/server systems, clients can access multiple servers.

- The client/server system includes some sort of networking capability.

- A significant portion of the application logic resides at the client end.
• Action is usually initiated at the client end, not the server end.
• A user-friendly graphical user interface (GUI) generally resides at the client end.
• A structured query language (SQL) capability is characteristic of the majority of client/server systems.
• The database server should provide data protection and security.

(d) **Locks on Doors with respect to physical access control:** Different types of locks on doors for physical security are discussed below:

- **Cipher Locks (combination Door Locks):** The Cipher Lock consists of a pushbutton panel that is mounted near the door outside of a secured area. There are ten numbered buttons on the panel. To enter, a person presses a four digit number sequence, and the door will unlock for a predetermined period of time, usually ten to thirty seconds. Cipher Locks are used in low security situations or when a large number of entrances and exits must be usable all the time. More sophisticated and expensive cipher locks can be computer coded with a person’s handprint. A matching handprint unlocks the door.

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

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

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

(e) **HIPAA:** Health Insurance Portability and Accountability Act (HIPAA) was enacted by the U.S. Congress in 1996. Major points are given as follows:

- **Title I of HIPAA** protects health insurance coverage for workers and their families when they change or lose their jobs.

- **Title II of HIPAA,** the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The AS provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation’s health care system by encouraging the widespread use of electronic data interchange in the US health care system. What is of interest here is the Security Rule issued under the Act.
Q-1  XYZ Industries Ltd., a company engaged in a business of manufacturing and supply of electronic equipments to various companies in India. It intends to implement E-Governance system at all of its departments. A system analyst is engaged to conduct requirement analysis and investigation of the present system. The company’s new business models and new methods presume that the information required by the business managers is available all the time; it is accurate and reliable. The company is relying on Information Technology for information and transaction processing. It is also presumed that the company is up and running all the time on 24 x 7 basis. Hence, the company has decided to implement a real time ERP package, which equips the enterprise with necessary capabilities to integrate and synchronise the isolated functions into streamlined business processes in order to gain a competitive edge in the volatile business environment. Also, the company intends to keep all the records in digitized form.

(a) What do you mean by system requirement analysis? What are the activities to be performed during system requirement analysis phase?  

(b) What are the business risks that an organization faces when migrating to real time integrated ERP system?  

(c) What are the points that need to be taken into account for the proper implementation of physical and environmental security in respect of Information System Security?  

(d) What is the provision given in Information Technology (Amended) Act 2008 for the retention of electronic records?  

Q-2  

(a) Discuss the policies and controls that any financial institution needs to consider when utilizing public key infrastructure.  

(b) Describe the benefits of performing a technology risk assessment.
(c) Why do you think a separate standard (SAS 70) is useful for auditing a service organization especially with respect to examination of general controls over Information Technology and related processes?

Q-3

(a) As an IS Auditor, discuss the various contents in brief to be included in a standard audit report.

(b) What are the characteristics of Executive Information System?

(c) Discuss the various backup options considered by a security administrator when arranging alternate processing facility.

Q-4

(a) Explain the common threats to the computerized environment of an organization.

(b) Describe the role of an IS auditor in the evaluation of physical access control.

(c) What are the tasks for which the company should be ready for post implementation period of an ERP System?

Q-5

(a) An organization is audited for effective implementation of ISO 27001 - Information Security Management Standard. What are the factors verified under
   (i) establishing management framework?
   (ii) Implementation?
   (iii) documentation?

(b) Enumerate the characteristics of a Computer Based Information System.

(c) Describe the duties of certifying authorities under Section 30 of Information Technology (Amended) Act 2008.
Q-6

(a) Discus in brief the various functional areas to be studied by a system analyst for a detailed investigation of the present system.

(8 Marks)

(b) As an IS Auditor, explain the types of information collected for auditing by using System Control Audit Review File (SCARF) technique.

(4 Marks)

(c) What are the audit tools and techniques used by an IS Auditor to ensure that disaster recovery plan is in order? Briefly explain them.

(4 Marks)

Q-7

Write Short notes on any four of the following:

(a) Business applications of Expert systems for Management Support systems.
(b) Firewalls.
(c) Delphi technique for risk evaluation.
(d) Capability Maturity Model.

(4 × 4=16 Marks)
Ans.1

(a) System requirements analysis is a phase, which includes a thorough and detailed understanding of the current system, identification of the areas that need modification/s to solve the problem, the determination of user/managerial requirements and to have fair ideas about various system development tools.

The following activities are performed in this phase:

- To identify and consult the stake owners to determine their expectations and resolve their conflicts;
- To analyze requirements to detect and correct conflicts and determine priorities;
- To verify requirements in terms of various parameters like completeness, consistency, unambiguous, verifiable, modifiable, testable and traceable;
- To gather data or find facts using tools like interviewing, research/document collection, questionnaires, observation;
- To develop models to document Data Flow Diagrams, E-R diagrams; and
- To document activities such as interviews, questionnaires, reports etc. and development of a system dictionary to document the modeling activities.

The document/deliverable of this phase is a detailed system requirements report, which is generally termed as SRS.

(b) Organizations face several business risks when migrating to real-time, integrated ERP systems. These risks are given as follows:

- Single point of failure: Since all the organization’s data and transaction processing is within one application system, single point failure may be a major risk.
- Structural changes: Significant personnel and organizational structure changes associated with reengineering or redesigning business processes may pose a big challenge.
- Job role changes: Transition of traditional user’s roles to empowered-based roles with much greater access to enterprise information in real time and the point of control shifting from the back-end financial processes to the front-end point of creation are also great risks.
- Online, real-time: An online real-time environment requires a continuous business environment capable of utilizing the new capabilities of the ERP application and responding quickly to any problem requiring re-entry of information.
• Change management: The level of user acceptance of the system has a significant influence on its success. Users must understand that their actions or inaction have a direct impact upon other users and, therefore, must learn to be more diligent and efficient in the performance of their day-to-day duties.

• Distributed computing experience: Inexperience with implementing and managing distributed computing technology may pose significant challenges.

• Broad system access: Increased remote access by users and outsiders and high integration among application functions allow increased access to application and data.

• Dependency on external assistance: Organization accustomed to in-house legacy systems may find that they have to rely on external help. Unless such external assistance is properly managed, it could introduce an element of security and resource management risk that may expose the organizations to greater risk.

• Program interfaces and data conversions: Extensive interfaces and data conversions from legacy systems and other commercial software are often necessary. The exposure of data integrity, security and capacity requirements for ERP are therefore often much higher.

• Audit expertise: Specialist expertise is required to effectively audit and control an ERP environment. The relative complexity of ERP systems has created specialization such that each specialist may know a small fraction of the entire ERP’s functionality in a particular core module.

(c) For the proper implementation of Physical and Environmental Security, the following points need to be taken into account:

• Physical security should be maintained and checks must be performed to identify all vulnerable areas within each site.

• The IT infrastructure must be physically protected.

• Access to secure areas must remain limited to authorized staff only.

• Confidential and sensitive information and valuable assets must be securely locked away, when they are not in use.

• Computers must never be left unattended whilst displaying confidential or sensitive information or whilst logged on to the systems.

• Supplies and equipments must be delivered and loaded in an isolated area to prevent any unauthorized access to key facilities.

• Equipment, information or software must not be taken off-site without proper authorization.
• Wherever practical, premises housing computer equipment and data should be located away from, and protected against threats of deliberate or accidental damage such as fire and natural disaster.

• The location of the equipment rooms must be away from, and protected against threats of unauthorized access and deliberate or accidental damage, such as system infiltration and environmental failures.

(d) Retention of Electronic Records: [Section 7] of ITAA 2008

The provision for the retention of electronic records is discussed in Section 7 of ITAA 2008, which is given as follows:

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, –

(a) the information contained therein remains accessible so as to be usable for a subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format, which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) The details, which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record.

However,

this clause does not apply to any information, which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents records or information in the form of electronic records, publication of rules, regulation etc. in Electronic Gazette.

Ans.2

(a) When utilizing PKI, financial institutions need to consider the following policies and controls:

• Defining within the certificate issuance policy, the methods of initial verification that are appropriate for different types of certificate applicants and the controls for issuing digital certificates and key pairs;

• Selecting an appropriate certificate validity period to minimize transactional and reputation risk exposure - expiration provides an opportunity to evaluate the continuing
adequacy of key lengths and encryption algorithms, which can be changed as needed before issuing a new certificate;

• Ensuring that the digital certificate is valid by such means as checking a certificate revocation list before accepting transactions accompanied by a certificate;

• Defining the circumstances for authorizing a certificate’s revocation, such as the compromise of a user’s private key or the closing of user accounts;

• Updating the database of revoked certificates frequently, ideally in real-time mode;

• Employing stringent measures to protect the root key including limited physical access to Certifying Authority (CA) facilities, tamper-resistant security modules, dual control over private keys and the process of signing certificates, as well as the storage of original and backup keys on computer that do not connect with outside networks;

• Requiring regular independent audits to ensure controls are in place, public and private key lengths remain appropriate, cryptographic modules conform to industry standards, and procedures are followed to safeguard the CA system;

• Recording in a secure audit log all significant events performed by the CA system, including the use of the root key, where each entry is time/ date stamped and signed;

• Regularly reviewing exception reports and system activity by the CA’s employees to detect malfunctions and unauthorized activities; and

• Ensuring the institution’s certificates and authentication systems comply with widely accepted PKI standards to retain the flexibility to participate in ventures that require the acceptance of the financial institution’s certificates by other CAs.

(b) Benefits of performing a technology risk assessment are given as follows:

• To have a business driven process to identify, quantify, and manage risks while detailing future suggestions for improvement in technical delivery;

• To have a framework that governs technical choice and delivery processes with cyclic checkpoints during the project lifecycle;

• Interpretation and communication of potential risk impact and where appropriate, risk reduction to a perceived acceptable level; and

• Implementation of strict disciplines for active risk management during the project lifecycle.

The technology risk assessment needs to a mandatory requirement for all projects to ensure that proactive management of risks occurs and that no single point of failure are in advertently built into the overall architecture.
Yes, to our opinion, a separate statement on Auditing Standard (SAS) No. 70 is useful for auditing a service organization especially with respect to examination of general controls. A SAS 70 audit or service auditor’s examination is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over Information Technology and related processes.

SAS 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers’ auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. A formal report including the auditor’s opinion (Service Auditor’s Report) is issued to the service organization at the conclusion of SAS 70 examination.

SAS 70 provides guidance to enable an independent auditor (Service Auditor) to issue an opinion on a service organization’s description of controls through a Service Auditor’s Report. SAS 70 is not a predetermined set of control objectives or control activities that service organization must achieve.

SAS 70 is generally applicable when an auditor (user auditor) is auditing the financial statements of an entity (user organization) that obtains services from another organization (service organization). Service organizations that provide such services could be application service providers, bank trust departments, claims processing centres, Internet data centres or other data processing service bureaus.

**Ans.3**

(a) An Audit report includes the following sections: title page, table of contents, summary (including recommendations), introduction, findings and appendices. These are discussed below:

- **Cover and Title Page:** Audit reports should use a standard cover page, with a window showing the title “Information System Audit” or “Data Audit”, the department’s name and the report’s date of issue. These items are repeated at the bottom of each page. The title page may also indicate the names of the audit team members.

- **Table of contents:** The table lists the sections and subsections with page numbers including summary and recommendations, introduction, findings and appendices.

- **Summary/Executive Summary:** The summary gives a quick overview of the salient features at the time of the audit in light of the main issues covered by the report. It should not exceed three pages, including recommendations.

- **Introduction:** It should include the following elements:
  - **Context:** This subsection briefly describes conditions in the audit entity during
the period under review, for instance, the entity’s role, size and organization with regard to information system management, significant pressures on information system management during the period under review, events that need to be noted, organizational changes, IT disruptions, changes in roles and programs, results of internal audits or follow-up to our previous audits, if applicable.

- **Purpose**: This subsection is a short description of what functions and special programs were audited and the client’s authorities.

- **Scope**: The scope lists the period under review, the issues covered in each function and program, the locations visited and the on-site dates.

- **Methodology**: This section briefly describes sampling, data collection techniques and the basis for auditor’s options. It also identifies any weaknesses in the methodology to allow the client and auditee to make informed decisions as a result of the report.

- **Findings**: Findings constitute the main part of an audit report. They result from the examination of each audit issue in the context of established objectives and client’s expectations. If the auditor is using any standard grading, the arrived value should also be stated.

- **Opinion**: If the audit assignment requires the auditor to express an audit opinion, the auditor shall do so in consonance to the requirement.

- **Appendices**: Appendices can be used when they are essential for understanding the report. They usually include comprehensive statistics, quotes from publications, documents, and references.

(b) Major characteristics of an Executive Information System (EIS) are given as follows:

- EIS is a computer-based-information system that serves the information need of top executives.

- EIS enables users to extract summary data and model complex problems without the need to learn query languages, statistical formulae or high computing skills.

- EIS provides rapid access for timely information and direct access to the management reports.

- EIS is capable of accessing internal and external data both.

- EIS provides extensive online analysis tools like trend analysis, market conditions etc.

- EIS can easily be given a DSS support for decision making.

(c) Security administrators should consider the following backup options while arranging alternate processing facility:
Cold site: If an organization can tolerate some downtime, cold site backup might be appropriate. A cold site has all the facilities needed to install a mainframe system, raised floors, air conditioning, power, communication lines, and so on. An organization can establish its own cold site facility or enter into an agreement with another organization to provide a cold site facility.

Hot site: If fast recovery is critical, an organization might need hot site backup. All hardware and operations facilities will be available at the host site. In some cases, software, data, and supplies might also be stored there. A hot site is expensive to maintain. They are usually shared with other organizations that have hot site needs.

Warm site: It provides an intermediate level of backup. It has all cold site facilities in addition with hardware that might be difficult to obtain or install. For example, a warm site might contain selected peripheral equipment plus a small mainframe with sufficient power to handle critical applications in the short run.

Reciprocal agreement: Two or more organizations might agree to provide backup facilities to each other in the event of one suffering a disaster. This backup option is relatively cheap, but each participant must maintain sufficient capacity to operate another’s critical system.

Ans.4

(a) The common threats to the computerized environment of an organization are given as follows:

(i) **Power failure**: Power failure can cause disruption of entire computing equipments since computing equipments depend on power supply.

(ii) **Communication failure**: Failure of communication lines result in inability to transfer data which primarily travel over communication lines. Where the organization depends on public communication lines, e.g. for e-banking, communication failure presents a significant threat that will have a direct impact on operations.

(iii) **Disgruntled Employees**: A disgruntled employee presents a threat since, with access to sensitive information of the organization, he may cause intentional harm to the information processing facilities or sabotage operations.

(iv) **Errors**: Errors which may result from technical reasons, negligence or otherwise can cause significant integrity issues. A wrong parameter setting at the firewall to ‘allow’ attachments instead of ‘deny’ may result in the entire organization network being compromised with virus attacks.

(v) **Malicious code**: Malicious codes such as viruses and worms which freely access the unprotected networks may affect organizational and business networks that use these unprotected networks.
(vi) **Abuse of access privileges by employees:** The security policy of the company authorizes employees based on their job responsibilities to access and execute select functions in critical applications.

(vii) **Natural disasters:** Natural disasters such as earthquakes, lighting, floods, tornado, tsunami, etc. can adversely affect the functioning of the Information System operations due to damage to Information System facilities.

(viii) **Theft or destruction of computing resources:** Since the computing equipments form the back-bone of information processing, any theft or destruction of the resource can result in compromising the competitive advantage of the organization.

(ix) **Downtime due to technology failure:** Information System facilities may become unavailable due to technical glitches or equipment failure and hence the computing infrastructure may not be available for short or extended periods of time. However, the period for which the facilities are not available may vary in criticality depending on the nature of business and the critical business process that the technology supports.

(x) **Fire, etc:** Fire due to electric short circuit or due to riots, war or such other reasons can cause irreversible damage to the IS infrastructure.

(b) **Role of an IS auditor in evaluation of Physical Access Controls is described below:**

(i) **Risk assessment:** The auditor must satisfy him/herself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposure therefrom.

(ii) **Controls assessment:** The auditor based on the risk profile evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks.

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

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

- Tour of organizational facilities including outsourced and offsite facilities;
- Physical inventory of computing equipment and supporting infrastructure;
- Interviewing personnel can also provide information on the awareness and knowledge of procedures;
- Examination of physical access logs and reports. Review of physical access procedures including user registration and authorization etc.; and
• Observation of safeguards and physical access procedures.

(c) Having evolved the processes while the configuration, construction and implementation are in progress, the organization needs to ready itself for the post-implementation period. Some of the tasks that are to be performed are to:
  • develop the new job descriptions and organization structure to suit the post ERP Scenario;
  • determine the skill gap between existing jobs and envisioned jobs;
  • assess training requirements, and create and implement a training plan;
  • develop and amend HR, financial and operational policies to suit the future ERP environment; and
  • develop a plan for workforce logistics adjustment.

Ans.5

(a) ISO 27001-Information Security Management Standard: The requirements of information security system as described by the standard are stated below. An organization must take a clear view on these issues before trying to implement an Information Security Management Systems (ISMS).

General: Organization shall establish and maintain documented ISMS addressing assets to be protected, organizations approach to risk management, control objectives and controls, and degree of assurance required.

Establishing Management Framework: This would include the following:
  • Defining information security policy;
  • Defining scope of ISMS including functional, asset, technical, and locational boundaries;
  • Making appropriate risk assessment;
  • Identifying areas of risk to be managed and degree of assurance required;
  • Selecting appropriate controls;
  • Preparing Statement of Applicability,

Implementation: Effectiveness of procedures to implement controls to be verified while reviewing security policy and technical compliance.

Documentation: The documentation shall consist of evidence of actions undertaken under establishment of the following:
  • Management control;
• Management framework summary, security policy, control objective, and implemented controls given in the Statement of Applicability;
• Procedure adopted to implement control under Implementation clause;
• ISMS management procedure;
• Document Control: The issues focused under this clause would be:
  • Ready availability,
  • Periodic review,
  • Maintain version control,
  • Withdrawal when obsolete, and
  • Preservation for legal purpose.
• Records: The issues involved in record maintenance are as follows:
  • Maintain evidence compliance to the standard,
  • Procedure for identifying, maintaining, retaining, and disposing of such evidence,
  • Records to be legible, identifiable and traceable to activety involved, and
  • Storage to augment retrieval, and protection against damage.

(b) Major characteristics of a Computer Based Information System are as follows:

1. All systems work for predetermined objectives and the system is designed and developed, accordingly.
2. In general, a system has a number of interrelated and interdependent subsystems or components. No subsystem can function in isolation; it depends on other subsystems for its inputs.
3. If one subsystem or component of a system fails, in most of the cases, the whole system does not work. However, it depends on ‘how the subsystems are interrelated’.
4. The way a subsystem works with another subsystem is called interaction. Different subsystems interact with each other to achieve the goal of the system.
5. The work done by individual subsystem is integrated to achieve the central goal of the system. The goal of the individual subsystem is of lower priority than the goal of the entire system.

(c) Duties of Certifying Authorities—Section 30 of ITAA 2008

This section provides that every Certifying Authority shall follow certain procedures with respect of Digital Signatures as given below.

Every Certifying authority shall-
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 Electronic Signature are assured (Amended vide ITAA 2008).

(c) be the repository of all Electronic Signature Certificates issued under this Act (Inserted vide ITAA 2008)

(cb) publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and (Inserted vide ITAA 2008)

d. Observe such other standards as may be specified by regulations.

**Ans.6**

(a) Detailed investigation of the present system involves collecting, organizing and evaluating facts about the system and the environment in which it operates. Survey of existing methods, procedures, data flow, outputs, files, input and internal controls should be done intensively to fully understand the present system and its related problems.

The following areas should be studied in depth by a System Analyst for a detailed investigation of the present system:

(i) **Review historical aspects:** A brief history of the organization is a logical starting point for an analysis of the present system. The historical facts should identify the major turning points and milestones that have influenced its growth. A review of annual reports and organization chart can identify the growth of management levels as well as the development of various functional areas and departments. The system analyst should investigate what system changes have occurred in the past including operations that have been successful or unsuccessful with computer equipments and techniques.

(ii) **Analyze inputs:** A detailed analysis of present inputs is important since they are basic to the manipulation of data. Source documents are used to capture the originating data for any type of system. The system analyst should be aware of the various sources from where the data are initially captured, keeping in view the fact that outputs for one area may serve as an input for another area. The system analyst must understand the nature of each form, what is contained in it, who prepared it, from where the form is initiated, where it is completed, the distribution of the form and other similar considerations. If the analyst investigates these questions thoroughly, he will be able to determine how these inputs fit into the framework of the present system.
(iii) **Review data files maintained**: The analyst should investigate the data files maintained by each department, noting their number and size, where they are located, who uses them and the number of times per given time interval these are used. Information on common data files and their size will be an important factor, which will influence the new information system. This information may be contained in the systems and procedures manuals. The system analyst should also review all on-line and off-line files which are maintained in the organization as it will reveal information about data that are not contained in any outputs. The related cost of retrieving and processing the data is another important factor that should be considered by the systems analyst.

(iv) **Review methods, procedures and data communications**: Methods and procedures transform input data into useful output. A method is defined as a way of doing something; a procedure is a series of logical steps by which a job is accomplished. A procedure review is an intensive survey of the methods by which each job is accomplished, the equipment utilized and the actual location of the operations. Its basic objective is to eliminate unnecessary tasks or to perceive improvement opportunities in the present information system. The system analyst must review the types of data communication equipments including data interface, data links, modems, dial up and leased lines and multiplexers, The system analyst must also understand how the data-communications network is used in the present system so as to identify the need to revamp the network when the new system is installed.

(v) **Analyze outputs**: The outputs or reports should be scrutinized carefully by the system analysts in order to determine how well they will meet the organization's needs. The analysts must understand what information is needed and why, who needs it and when and where it is needed. Additional questions concerning the sequence of the data, how often the form reporting is used, how long it is kept on file, etc. must be investigated.

(vi) **Review internal controls**: A detailed investigation of the present information system is not complete until internal control is reviewed. Locating the control points helps the analyst to visualize the essential parts and framework of a system. An examination of the present system of internal controls may indicate weaknesses that should be removed in the new system. The adoption of advanced methods, procedures and equipments might allow much greater control over the data.

(vii) **Model the existing physical system and logical system**: As the logic of inputs, methods, procedures, data files, data communications, reports, internal controls and other important items are reviewed and analyzed in a top down manner; the process must be properly documented. The flow charting and diagramming of present information not only organizes the facts, but also helps disclose gaps and duplication in the data gathered. It allows a
thorough comprehension of the numerous details and related problems in the present operation.

(viii) **Undertake overall analysis of the present system:** The final phase of the detailed investigation includes the analysis of the present work volume; the current personnel requirements; the present benefits and costs and each of these must be investigated thoroughly.

(b) An IS Auditor might use SCARF to collect the following types of information:

- **Application system errors:** SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.

- **Policy and procedural variances:** Organizations have to adhere to the policies, procedures and standards of the organization and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.

- **System exception:** SCARF can be used to monitor different types of application system exceptions.

- **Statistical sample:** Some embedded audit routines might be statistical sampling routines, SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.

- **Snapshots and extended records:** Snapshots and extended records can be written into the SCARF file and printed when required.

- **Profiling data:** Auditor can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.

- **Performance measurement:** Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.

(c) The audit tools and techniques used by an IS Auditor to ensure that disaster recovery plan is in order, are given as follows:

(i) **Automated Tools:** Automated tools make it possible to review large computer systems for a variety of flaws in a short time period. They can be used to find threats and vulnerabilities such as weak access controls, weak passwords, lack of integrity of the system software, etc.

(ii) **Internal Control Auditing:** This includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance of laws and regulations.
(iii) **Disaster and Security Checklists**: A checklist can be used against which the system can be audited. The checklist should be based upon disaster recovery policies and practices, which form the baseline. Checklists can also be used to verify changes to the system from contingency point of view.

(iv) **Penetration Testing**: Penetration testing can be used to locate vulnerabilities.

Ans.7

(a) Business applications of Expert Systems for Management Support Systems are given as follows:

(i) **Accounting and Finance**: It provides tax advice and assistance, helping with credit authorization decisions, selecting forecasting models, providing investment advice.

(ii) **Marketing**: It provides establishing sales quotas, responding to customer inquiries, referring problems to telemarketing centers, assisting with marketing timing decisions, determining discount policies.

(iii) **Manufacturing**: It helps in determining whether a process is running correctly, analyzing quality and providing corrective measures, maintaining facilities, scheduling job-shop tasks, selecting transportation routes, assisting with product design and faculty layouts.

(iv) **Personnel**: It is useful in assessing applicant qualifications, giving employees assisting at filling out forms.

(v) **General Business**: It helps in assisting with project proposals, recommending acquisition strategies, educating trainees, evaluating performance.

(b) **Firewalls**

A firewall is a collection of components (Computers, routers and software) that mediate access between different security domains. All traffic between the security domains must pass through the firewall, regardless of the direction of the flow. Since the firewall serves as an access control point for traffic between security domains, they are ideally situated to inspect and block traffic and co-ordinate activities with network Intrusion Detection Systems (IDSs).

There are four primary firewall types from which to choose: packet filtering, stateful inspection, proxy servers, and application-level firewalls. Any product may have characterization of one or more firewall types. The selection of firewall type is dependent on many types of characteristics of the security zone, such as the amount of traffic, the sensitivity of the systems and data, and applications. Additionally, consideration should be given to the ease of firewall administration, degree of firewall monitoring support through automated logging and log analysis, and the capability to provide alerts for abnormal
activity. Typically, firewalls block or allow traffic based on rules configured by the administrator. Rule sets can be static or dynamic. A static rule set is an unchanging statement to be applied to packet header, such as blocking all incoming traffic with certain source addresses. A dynamic rule set often is the result of coordinating a firewall and an IDS. For example, an IDS that alerts on malicious activity may send a message to the firewall to block the incoming IP address. The firewall, after ensuring the IP is not on a ‘white list’, creates a rule to block the IP. After a specified period of time, the rule expires and traffic is once again allowed from that IP.

Firewalls are subject to failure. When firewalls fail, they typically should fail closed, blocking all traffic, rather than failing open and allowing all traffic to pass.

(c) Delphi Technique for Risk Evaluation

The Delphi Technique was first used by the Rand Corporation for obtaining a consensus opinion. Here, a panel of experts is appointed. Each expert gives his/her opinion in a written and independent manner. They enlist the estimate of the cost, benefits and the reasons why a particular system should be chosen, the risks and the exposures of the system. These estimates are then compiled together. The estimates within a pre-decided acceptable range are taken. The process may be repeated four times for revising the estimates falling beyond the range. Then a curve is drawn taking all the estimates as points on the graph. The median is drawn and this is the consensus opinion.

(d) Capability Maturity Model (CMM)

The CMM presents sets of recommended practices in a number of key process areas that have been shown to enhance software process capability. The CMM is based on knowledge acquired from software process assessments and extensive feedback from both industry and government.

The capability maturity model for software provides software organizations with guidance on how to gain control of their processes for developing and maintaining software and how to evolve toward a culture of software engineering and management excellence. The CMM was designed to guide software organizations in selecting process improvement strategies by determining current process maturity and identifying the few issues most critical to software quality and process improvement. By focusing on a limited set of activities and working aggressively to achieve them, an organization can steadily improve its organization-wide software process to enable continuous and lasting gains in software process capability.

(e) Authentication of Electronic Records: [Section 3] of ITAA 2008

Section 3 of ITAA 2008 provides the conditions subject to which an electronic record may be authenticated by means of affixing digital signature, which is given below:
(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation -
For the purposes of this subsection, “Hash function” means an algorithm mapping or translation of one sequence of bits into another, generally smaller set known as “Hash Result” such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.
Q-1

(a) ABC Industries Ltd., a company engaged in a business of manufacture and supply of automobile components to various automobile companies in India, had been developing and adopting office automation systems, at random and in isolated pockets of its departments.

The company has recently obtained three major supply contracts from International Automobile companies and the top management has felt that the time is appropriate for them to convert its existing information system into a new one and to integrate all its office activities. One of the main objectives of taking this exercise is to maintain continuity of business plans even while continuing the progress towards e-governance.

(a) When the existing information system is to be converted into a new system, what are the activities involved in the conversion process? (5 Marks)

(b) What are the types of operations into which the different office activities can be broadly grouped under office automation systems? (5 Marks)

(c) What is meant by Business Continuity Planning? Explain the areas covered by Business Continuity. (5 Marks)

Q-2

(a) You are entrusted with the duty of implementing an ERP in your office. You have taken care of all the preparations during the implementation. However, during post implementation, there will be a need for course correction many times. What can be the reasons for them? (4 Marks)

(b) Why does an organization implement an ERP package and evaluate the various available ERP packages for assessing suitability? Mention the various evaluation criteria that are required to assess suitability of an ERP package on implementation. (4 Marks)
(c) “The information system insurance policy should be a multiperil policy, designed to provide various types of coverage.” Discuss the comprehensive list of items considered for coverage.  

(8 Marks)

Q-3

(a) As an IS auditor, suggest a method to test the correctness of a particular module of source code and justify your answer.  

(4 Marks)

(b) What are the aspects to be included when a documented audit program is developed?  

(4 Marks)

(c) “Once the information is classified on various levels, the organization has to decide about the implementation of different data integrity controls.” Do you agree? If yes, explain about data integrity and its policies.  

(8 Marks)

Q-4

(a) “Technology risk assessment needs to be a mandatory requirement for project to identify single point’s failures.” – Justify.  

(4 Marks)

(b) What do you understand from Type I and Type II reports from a Service auditor?  

(4 Marks)

(c) To get a good documentation of the working papers of an auditor, what are the points to be considered while gathering and organizing information and also mention the principles to be followed for writing the documentation?  

(8 Marks)

Q-5

(a) What does Information Technology (Amendment) Act, 2008 say about  

(i) Attributes of Electronic Records in Section 11 and  

(ii) Secure Electronic Signature (Substituted vide ITAA 2008) in Section 15?  

(4 Marks)

(b) What do you understand from the term ‘database’? How is it implemented in three different levels?  

(4 Marks)

(c) System maintenance is an important phase during the implementation of the system. If so, what are the three categories in which maintenance can be undertaken? As an IS auditor
of the organization, how will you evaluate the effectiveness and efficiency of the system maintenance process?

(8 Marks)

Q-6

(a) As a person in-charge of System Development Life Cycle, you are assigned a job of developing a model for a new system, which combines the features of a prototyping model and the waterfall model. Which will be the model of your choice and what are its strengths and weaknesses?

(8 Marks)

(b) From the perspective of IS audit, what are the advantages of System Development Life Cycle?

(4 Marks)

(c) How will you define a software process? What do you mean by its capability, performance and maturity?

(4 Marks)

Q-7 Write short notes on any four of the following:

(a) Regression Testing
(b) Business Engineering
(c) Benefits of Expert Systems
(d) Section 41, ITAA 2008 – Acceptance of Digital Signature Certificate
(e) SysTrust and WebTrust Services

(4 x 4 =16 Marks)
Ans.1

(a) Conversion from existing information system to a new system involves the following activities:

(i) Defining the procedures for correcting and converting the data into the new application, determining ‘what data can be converted through software and what data manually’;

(ii) Performing data cleansing before data conversion;

(iii) Identifying the methods to assess the accuracy of conversion like record counts and control totals;

(iv) Designing exception reports showing the data which could not be converted through software; and

(v) Establishing responsibility for verifying and signing off and accepting overall conversion by the system owner.

(b) **Types of Operations:** The types of operations into which different office activities under Office Automation Systems can be broadly grouped, are discussed as under:

(i) **Document capture:** Documents originating from outside sources like incoming mails, notes, handouts, charts, graphs etc. need to be preserved.

(ii) **Document Creation:** This consists of preparation of documents, dictation, editing of texts etc. and takes up major part of the secretary’s time.

(iii) **Receipts and Distribution:** This basically includes distribution of correspondence to designated recipients.

(iv) **Filling, Search, Retrieval and Follow-up:** This is related to filling, indexing, searching of documents, which takes up significant time.

(v) **Calculations:** These include the usual calculator functions like routine arithmetic, operations for bill passing, interest calculations, working out the percentages and the like.

(vi) **Recording Utilization of Resources:** This includes, where necessary, record keeping in respect of specific resources utilized by office personnel.

All the activities mentioned have been made very simple and effective by the use of computers. The application of computers to handle the office activities is also termed as office automation.

(c) **Business Continuity Planning (BCP)** is the creation and validation of a practical logistical plan for how an organization will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption. The
logistical plan is called a Business Continuity Plan. Planning is an activity to be performed before the disaster occurs otherwise it would be too late to plan an effective response. The resulting outage from such a disaster can have serious effects on the viability of a firm’s operations, profitability, quality of service, and convenience. Business Continuity covers the following areas:

(i) **Business resumption planning** – The Operation’s piece of business continuity planning;

(ii) **Disaster recovery planning** – The technological aspect of BCP, the advance planning and preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of a disaster.

(iii) **Crisis Management** – The overall co-ordination of an organization’s response to a crisis in an effective timely manner, with the goal of avoiding or minimizing damage to the organization’s profitability, reputation or ability to operate.

(d) Procedure to apply for a license to issue electronic signature under Section 22, IT (Amendment) Act, 2008 is given follows:

1. Every application for issue of a license shall be in such form as may be prescribed by the Central Government.

2. Every application for issue of a license shall be accompanied by
   (i) a certification practice statement;
   (ii) a statement including the procedure with respect to identification of the applicant;
   (iii) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government; and
   (iv) such other documents, as may be prescribed by the Central Government.

Ans.2

(a) The need for course correction during Post-implementation of ERP may be because of the following reasons: (i) A change in the business environment requires a change in the Critical Success Factors (CSF), resulting in a new or changed set of Key Performance Indicators (KPI) necessitating reconfiguration. (ii) A review indicates a need for change in some processes. (iii) Vision changes in the ERP and improvements in hardware and communication technology necessitate changes. (iv) New additions to the business require extra functionality.

(b) ERP implementation in the organization brings together in one platform, different business functions, different personalities, procedures, ideologies and philosophies with an aim to pool knowledge base to effectively integrate and bring worthwhile and beneficial changes throughout the organization. Implementation of ERP is a risky effort since it involves
considerable amount of time, efforts and valuable resources. Even with all these, the success of an implementation is not guaranteed. The ability of the ERP package to manage and support dynamically changing business process is a critical requirement for the organization and therefore the package should be expandable and adaptable to meet these changes. The ERP implementation methodology involves several steps of which, one is evaluating the various available ERP packages to assess suitability. Evaluation of ERP packages are done based on the following criteria:

- Flexibility
- Comprehensive
- Integrated
- Beyond the company
- Best business practices
- New technologies
- Other factors:
  - Global presence of package
  - Local presence
  - Market Targeted by the package
  - Price of the package
  - Obsolescence of package
  - Ease of implementation of package
  - Cost of implementation
  - Post-implementation support availability.

(c) The information system insurance policy should cover the following items:

(i) **Hardware facilities** – The equipments should be covered adequately. Provision should be made for the replacement of all equipments with a new one by the same vendor.

(ii) **Software reconstruction** – In addition to the cost of media, programming costs for recreating the software should also be covered.

(iii) **Extra expenses** – The cost incurred for continuing the operations till the original facility is restored should also be covered.

(iv) **Business interruption** – This applies mainly to centers, performing outsourced jobs of clients. The loss of profit caused by the damaged computer media should be covered.
(v) **Valuable paper and records** – The actual cost of valuable papers and records stored in the insured premises should be covered.

(vi) **Errors and Omissions** – This cover is against the legal liability arising out of errors and omissions committed by system analysts, programmers and other information system personnel.

(vii) **Fidelity Coverage** – This coverage is for acts of employees, more so in the case of financial institutions, which use their own computers for providing services to clients.

(viii) **Media transportation** – The potential loss or damage to media while being transported to off-site storage/premises should be covered.

**Ans.3**

(a) The suggested method is **Unit Testing**, which is used for testing the correctness of a particular module of a source code. The idea is to write test cases for every non-trivial functions or method in the module so that each test case is separate from the others if possible.

**Justification:** It provides the following benefits:

(i) **Encourages Change:** Unit Testing allows the programmer to re-factor code at a later date, and make sure the module still works correctly (regression testing). This provides the benefit of encouraging programmers to make changes to the code since it is easy for the programmer to check if the piece is still working properly.

(ii) **Simplifies integration:** Unit testing helps to eliminate uncertainty in the pieces themselves and can be used in a bottom-up testing style approach. By testing the parts of a program first and then testing the sum of its parts will make integration testing easier.

(iii) **Documents the Code:** Unit testing provides a sort of ‘living document’ for the class being tested. Clients wishing to learn to use the class can look at the unit tests to determine how to use the class to fit their needs.

(b) A documented audit program would include the following aspects:

(i) Documentation of the information system auditor’s procedures for collecting, analyzing, interpreting and documenting information during the audit;

(ii) Objectives of the audit;

(iii) Scope, nature and degree of testing required achieving the audit objectives in each phase of the audit;

(iv) Identification of technical aspects, risks, processes and transactions, which should be examined; and

(v) Procedures for audit will be prepared prior to the commencement of audit work and modified, as appropriate, during the course of the audit.
(c) Yes, we agree with the statement given in the question. Data integrity is a reflection of the accuracy, correctness, validity and currency of the data. The primary objective in ensuring integrity is to protect the data against erroneous input from authored users.

Data Integrity Policies: These policies are given as follows:

(i) **Virus Signature updating** – Virus signatures must be updated immediately when they are made available from the vendor.

(ii) **Software testing**: All software must be tested in a suitable test environment before installation on production systems.

(iii) **Division of Environments** – The division of environment into Development, Test and Production is required for critical systems.

(iv) **Version Zero Software** – Version Zero Software (1.0, 2.0 and so on) must be avoided whenever possible to avoid undiscovered bugs.

(v) **Off-site Backup Storage** – Backups older than one month must be sent offsite for permanent storage.

(vi) **Quarter-End and year-End Backups** – These backups must be done separately from the normal schedule for accounting purposes.

(vii) **Disaster Recovery** – A comprehensive disaster recovery plan must be used to ensure continuity of the corporate business in the event of an outrage.

**Ans.4**

(a) Single point of failures have increased due to the continued growth in the complexity in the organization’s IS environment. Technology risk assessment is a mandatory requirement to identify single point failures because of the following benefits:

(i) A business-driven process to identity, quantify and manage risks while detailing failure, suggestions for improvement in technical delivery.

(ii) A framework that governs technical choice and delivery processes with cyclic check-points during the project life-cycle.

(iii) Interpretation and communication of potential risk impact and where appropriate, risk reduction to a perceived acceptable level.

(iv) Implementation of strict disciplines for active risk management during the project life cycle.

The technology risk assessment ensures that proactive management of risks occurs and that no single point of failure is inadvertently built into the overall architecture.

(b) **Service Auditor’s Reports**: One of the most effective ways, a service organization can communicate information about its controls is through a Service Auditor’s Report. There are two types of Service Auditor’s Reports, namely, Type I and Type II.
A Type I report describes the service organization’s description of Controls at a specific point in time. In a Type I report, the service auditor will express an opinion on (1) whether the service organization’s description of its controls presents fairly, in all material respects, the relevant aspects of the service organization’s controls that had been placed in operation as of a specific date and (2) whether the controls were suitably designed to achieve specified control objectives.

A Type II report not only includes the service organization’s description of Controls, but also includes detailed testing of the service organization’s controls over a minimum six month period.

In a Type II report, the service auditor will express an opinion on the same items in a Type I report, and also on (3) whether the controls that were tested, also operate with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.

(c) In order to get a good documentation of the working papers of an auditor, the following points are to be considered during gathering information:

(i) About the reader — Finding information about the reader by doing a task analysis. Three parts of the task viz. input, process, and output will have to be identified before one could develop an understanding of a reader.

(ii) About the subject — The three sources of information about a subject are people, paper and the object of the report.

Organizing information:

The points to be considered during organizing information are given as under:

(i) Selecting Information — Selecting ‘what the reader needs to know’, organizing the information into a useful sequence.

(ii) Organizing the documentation — Using the five organizational sequences: subject, difficulty, chronological, importance and analytical.

(iii) Dividing into sections — Dividing documentation into chapters or sections.

(iv) Dividing into subsections — Dividing sections or chapters into subsections.

Principles for writing the documentation:

Following principles should be kept in mind for writing the documentation:

• Writing in Active voice: Using active voice in documentation;

• Giving the consequences: Giving the consequences of the reader’s action;

• Writing from General to specific: Designing the documentation from general to specific;
• Consistency: Using style, order and format consistently; and
• Writing online documentation: Laying down guidelines for writing online document-
tation by using appropriate techniques to emphasize text.

Ans.5 (a)

(i) **Attributes of Electronic Records in Section 11 of Information Technology (Amendment) Act, 2008**

An electronic record shall be attributed to the originator:

(i) if it was sent by the originator himself.

(ii) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or

(iii) by an information system programmed by or on behalf of the originator to operate automatically.

(ii) **[Section 15] Secure Electronic Signature (substituted vide ITAA 2008)**

An electronic signature shall be deemed to be secure if:

(i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and

(ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed.

(b) **Database:** Database can be defined as a 'Super-file' which consolidates data records formerly stored in many data files. The data in a database is organized in such a way that access to the data is improved and redundancy is reduced.

**Implementation of Databases:** Three levels at which database can be implemented, are as under:

(i) **Physical Level:** It involves the implementation of the database on the hard disk. The management of storage and access is controlled by operating system.

(ii) **Logical Level:** It is designed by professional programs, who have complete knowledge of DBMS. The storage is logically divided into various tables having techniques for defining relationships with indexes.

(iii) **External Level:** The logical level defines schema, which is divided into smaller units known as sub-schemas and given to the managers, each sub-schema containing all relevant data needed by one manager.

(c) Three categories of system maintenance are as follows:

(i) **Corrective maintenance:** Emergency program fixes and routine debugging-logical errors.
(ii) **Adaptive maintenance**: Accommodation of change in the user environment.

(iii) **Perfective maintenance**: User enhancements, improved documentation and recording for improving processing efficiency.

**Auditor's Role in System Maintenance:**

The effectiveness and efficiency of the system maintenance process is evaluated with the following metrics:

(i) The ratio of actual maintenance cost per application/operation versus the average of all applications/processes;

(ii) Average time to deliver change requests;

(iii) The number of change requests for the system application that were related to bugs, critical errors and new functional specifications;

(iv) The number of production problems per application and per respective maintenance changes;

(v) The instances of divergence from standard procedures such as undocumented applications, unapproved and testing reductions;

(vi) The quantity of modules returned to development due to errors discovered in acceptance testing; and

(vii) Time elapsed to analyze and fix problems.

**Ans.6**

(a) As a person in-charge of system development life cycle, the spiral model will be the choice. The spiral model is a software development process, combining elements of both design and prototyping-in-stages, in an effort to combine/advantages of top-down and bottom-up concepts. It is a system development method, which combines the features of the prototyping model and the waterfall model. The spiral model is intended for large, expensive and complicated projects. Its major distinctiveness is given as follows:

(i) The new system requirements are defined in as much detail as possible. This usually involves interviewing a number of users representing all the external or internal users and other aspects of the existing system.

(ii) A preliminary design is created for the new system. This phase is the most important part of 'Spiral Model' in which all possible alternatives that can help in developing a cost effective project are analyzed and strategies are decided to use them. This phase has been added specially in order to identify and resolve all the possible risks in the project development. If risks indicate any kind of uncertainty in requirements, prototyping may be used to proceed with the available data and find out possible solution in order to deal with the potential changes in the requirements.
(iii) A first prototype of the new system is constructed from the preliminary design. This is usually a scaled-down system, and represents an approximation of the characteristics of the final product.

(iv) A second prototype is evolved by a fourfold procedure:

- evaluating the first prototype in terms of its strengths, weaknesses, and risks;
- defining the requirements of the second prototype;
- planning and designing the second prototype; and
- constructing and testing the second prototype.

Game development is a main area where the spiral model is used and needed, that is because of the size and the constantly shifting goals of those large projects.

**Strengths:**

(i) Enhance risk avoidance;

(ii) Useful in helping to select the best methodology to follow for development of a given software iteration based on project risk.

(iii) Can incorporate waterfall, prototyping and incremental methodologies as special cases in the framework, and provide guidance as to which combinations of these models best fits a given software iteration, based upon the type of project risk.

**Weaknesses:**

(i) Challenges to determine the exact composition of development methodologies to use for each iteration around the spiral.

(ii) Highly customized to each project and thus is quite complex, limiting reusability.

(iii) A skilled and experienced project manager required to determine how to apply it to any given project.

(iv) No established controls for moving from one cycle to another cycle. Without controls, each cycle may generate, more work for the next cycle.

(v) No firm deadlines cycles continue with no clean termination condition, so there is an inherent risk of not meeting budget or schedule.

(b) From the perspective of the IS Audit, following are the possible advantages:

(i) The IS Auditor can have clear understanding of the various phases of SDLC on the basis of the detailed documentation created during each phase of the SDLC.

(ii) The IS Auditor on the basis of the examination, can state in his report about the compliance by the IS Management of the procedures, if any, set by the management.
(iii) The IS Auditor, if has a technical knowledge and ability of the area of SDLC, can be a guide during the various phases of SDLC.

(iv) The IS Auditor can provide an evaluation of the methods and techniques used through the various development phases of the SDLC.

(c) **Software Process**: A software process can be defined as a set of activities, methods, practices and transformations that people use to develop and maintain software and the associated products. Examples include project plans, design documents, code, test cases and user manuals etc.

**Software process capability**: It describes the range of expected results that can be achieved by following a software process. It focuses on results expected from the next software project.

**Software process performance**: It represents the actual results achieved by following a software process. It focuses on the results achieved.

**Software process maturity**: It is the extent to which a specific process is explicitly defined, managed, measured, controlled and effective. It helps the organization in institutionalization of its software process via policies, standards and organizational structure.

**Ans.7**

(a) **Usage of Regression Testing**:

(i) All aspects of system remain functional after testing.

(ii) Change in one segment does not change the functionality of other segment.

**Objectives**:

(i) System documents remain current.

(ii) System test data and test conditions remain current.

(iii) Previously tested system functions properly without getting effected though changes are made in some other segment of application system.

**How to Use**:

- Test cases, which were used previously for the already tested segment is, re-run to ensure that the results of the segment tested currently and the results of same segment tested earlier, are same.

- Test automation is needed to carry out the test transactions (test condition execution) else the process is very time consuming and tedious.

- In this case of testing, cost/benefit should be carefully evaluated else the efforts spend on testing would be more and payback would be minimum.
(b) Business Engineering:

(i) Business Engineering has come out of merging of two concepts, namely Information Technology and Business Process Reengineering.

(ii) It is the rethinking of business processes to improve speed, quality and output of materials or services.

(iii) The emphasis of business engineering is the concept of process oriented business solutions enhanced by the client-server computing in Information Technology.

(iv) The main point is the efficient redesigning of company’s value added chains assisted by business models, developed by Information Technology.

(v) It is the development of business processes according to changing requirements.

(c) Benefits of Expert Systems: These are given as follows:

(i) Expert Systems preserve knowledge that might be lost through retirement, resignation or death of an acknowledged company expert.

(ii) Expert Systems put information into an active form so it can be summoned almost as a real life expert might be summoned.

(iii) Expert Systems assist novices in thinking the way experienced professional do.

(iv) Expert Systems are not subject to such human feelings as fatigue, being too busy, or being emotional.

(v) Expert Systems can be effectively used as a strategic tool, in the areas of marketing products, cutting costs and improving products.

(d) [Section 41], ITAA 2008: Acceptance of Digital Signature Certificate

(i) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a digital signature certificate

(a) to one or more persons;

(b) in a repository or otherwise demonstrates his approval of the digital signature certificate in any manner.

(ii) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that:

(a) the subscriber holds the private key corresponding to the public key listed in the digital signature certificate and is entitled to hold the same;

(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true.
(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

(e) **SysTrust and WebTrust**: SysTrust and WebTrust are two specific services developed by the AICPA that are based on the Trust Services Principles and criteria. SysTrust engagements are designed for the provision or advisory services or assurance on the reliability of a system. WebTrust engagements relate to assurance or advisory services on an organization’s system related to e-commerce. Only Certified Public Accountants (CPAs) may provide the assurance services of trust services that result in the expression of Trust Services, WebTrust or SysTrust opinion and in order to issue SysTrust or WebTrust reports, CPA firms must be licensed by the AICPA. The following principles and related criteria have been developed by the AICPA for use by practitioners in the performance of trust services engagements such as SysTrust and WebTrust.

(i) Security: The system is protected against unauthorized access (both physical and logical)

(ii) Availability: The system is available for operation and use as committed or agreed.

(iii) Processing integrity: System processing is complete, accurate, timely and authorized.

(iv) Online privacy: Personal information obtained as a result of e-commerce is collected, used, disclosed and retained as committed or agreed.

(v) Confidentiality: Information designated as confidential is protected as committed or agreed.
Q-1
ASK International proposes to launch a new subsidiary to provide e-consultancy services for organizations throughout the world, to assist them in system development, strategic planning and e-governance areas. The fundamental guidelines, programmes modules and draft agreements are all preserved and administered in the e-form only.

The company intends to utilize the services of a professional analyst to conduct a preliminary investigation and present a report on smooth implementation of the ideas of the new subsidiary. Based on the report submitted by the analyst, the company decides to proceed further with three specific objectives (i) reduce operational risk, (ii) increase business efficiency and (iii) ensure that information security is being rationally applied. The company has been advised to adopt BS 7799 for achieving the same.

(a) What are the two primary methods through which the analyst would have collected the data?

(b) To achieve their objectives, what are the points BS 7799 has to ensure?

(c) Suppose an audit policy is required, how will you lay down the responsibility of audit?

(d) To retain their e-documents for specified period, what are the conditions laid down by Section 7, Chapter III of Information Technology Act, 2000?

Q-2

(a) What are common threats to the computerized environment other than natural disasters, fire and power failure?

(b) How would you use Data Dictionary as a tool for file security and audit trails?

(c) The management of ABC Ltd. wants to design a detective control mechanism for achieving security policy objective in a computerized environment. As an auditor explain, how audit trails can be used to support security objectives.
Q-3
(a) How will you get over the impediments for the successful implementation of ERP? Mention any five.  
(10 marks)
(b) A company has decided to outsource a third party site for its alternate back-up and recovery process. What are the issues to be considered by the security administrator while drafting the contract?  
(5 marks)
(c) Explain the role of IS auditor in evaluating logical access controls.  
(5 marks)

Q-4
(a) Describe some of the advantages of continuous audit techniques.  
(5 marks)
(b) Define the following terms related to Information Technology Act, 2000:
   (i) Computer contaminant  
   (ii) Cyber cafe  
   (iii) Electronic form  
   (iv) Traffic data  
   (v) Asymmetric crypto system  
(5 marks)
(c) Give some important advantages of Information System in business  
(5 marks)
(d) What is COBIT? Give three vantage points from which the issue of control can be addressed by this framework.  
(5 marks)

Q-5
(a) What are the two primary questions to consider when evaluating the risk inherent in a business function in the context of the risk assessment methodologies? Give the purposes of risk evaluation.  
(5 marks)
(b) If you are the CEO of a company, what factors would be considered before undertaking implementation of an ERP system?  
(5 marks)
(c) Briefly describe any three of the characteristics of the types of information used in Executive Decision making.  
(5 marks)
(d) Discuss the benefits and limitations of unit testing.  
(5 marks)
(a) Two primary methods through which the analyst would have collected the data are given as follows:

(1) **Reviewing internal documents**: The analyst first tries to learn about the organization involved in or affected by the project. For example, to review an inventory system proposal, s/he will try to know ‘how the inventory department operates’ and ‘who are the managers and supervisors’. S/he will examine organization charts and written operating procedures.

(2) **Conducting interviews**: Written documents tell the analyst ‘how the system should operate’ but they may not include enough details to allow a decision to be made about the merits of a system proposal nor do they present users’ views about current operations. To learn these details, analysts use interviews. Preliminary investigation interviews involve only management and supervisory personnel.

(b) BS 7799 should ensure that:

(1) Security controls are justified.

(2) Policies and procedures are appropriate.

(3) Security awareness is good amongst staff and managers.

(4) All security relevant information processing and supporting activities are auditable and are being audited.

(5) Internal audit, incident reporting/ management mechanisms are being treated appropriately.

(6) Management actively focuses on information security and its effectiveness.

(7) Certification can also be used as a part of marketing initiative, providing assurance to business partners and other outsiders.

(c) The scope of information system auditing should encompass the examination and evaluation of the adequacy and effectiveness of the system of internal control and the quality of performance by the information system. Information System Audit will examine and evaluate the planning, organizing, and directing processes to determine whether reasonable assurance exists that objectives and goals will be achieved. Such evaluations, in the aggregate, provide information to appraise the overall system of internal control.

The audit policy should lay down the responsibilities as follows:

(1) The policy should lay out the periodicity of reporting and the authority to whom the reporting is to be made.
(2) A statements of professional proficiency may be included to state the minimum qualification and experience requirements of the auditors.

(3) All information system auditors will sign a declaration of fidelity and secrecy before commencing the audit work in a form that the inspection department may design.

(4) The policy may lay out the extent of testing to be done under the various phases of the audit like Planning, Compliance Testing, and Substantive Testing.

(5) A documented audit program would be developed including the following:
   - Documentation of the information system auditor’s procedures for collecting, analyzing, interpreting, and documenting information during the audit.
   - Objectives of the audit.
   - Scope, nature, and degree of testing required for achieving the audit objectives in each phase of the audit.
   - Identification of technical aspects, risks, processes, and transactions which should be examined.
   - Procedures for audit will be prepared prior to the commencement of audit work and modified, as appropriate, during the course of the audit.

(6) The policy should determine when and to whom the audit results would be reported and communicated. It would define the access rights to be given to the auditors.

(7) The Policy should outline the compliance testing areas.

(8) The auditor will carry out substantive testing wherever the auditor observes weakness in internal controls or where risk exposure is high. The auditor may also carry out such tests to gather additional information necessary to form an audit opinion.

(9) The Audit Policy would define the compulsory audit working papers to be maintained and their formats.

(d) Section 7, Chapter III of Information Technology Act, 2000/ Information Technology (Amendment) Act, 2008 provides that the documents, records or information which is to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form provided the following conditions are satisfied:

(i) The information therein remains accessible so as to be usable subsequently.

(ii) The electronic record is retained in its original format or in a format which accurately represents the information contained.

(iii) The details which will facilitate the identification of the origin, destination, dates and time of dispatch or receipt of such electronic record are available therein. This section does not apply to any information which is automatically generated solely for the
AAGAM PUBLISHERS

purpose of enabling an electronic record to be dispatched or received. Moreover, this section does not apply to any law that provides for the retention of documents, records or information in the form of electronic records.

Ans.2

(a) A few common threats to computerized environment other than natural disasters, fire and power failure are:

1. **Communication failure**: Failure of communication lines result in inability to transfer data which primarily travel over communication lines. Where the organization depends on public communication lines e.g. for e-banking, communication failure presents a significant threat that will have a direct impact on operations.

2. **Disgruntled Employees**: A disgruntled employee presents a threat since, with access to sensitive information of the organization, he may cause intentional harm to the information processing facilities or sabotage operations.

3. **Errors**: Errors which may result from technical reasons, negligence or otherwise can cause significant integrity issues. A wrong parameter setting at the firewall to “allow” attachments instead of “deny” may result in the entire organization network being compromised with virus attacks.

4. **Malicious Code**: Malicious code such as viruses and worms, which freely access the unprotected networks, may affect organizational and business networks that use these unprotected networks.

5. **Abuse of access privileges by employees**: The security policy of the company authorizes employees based on their job responsibilities to access and execute select functions in critical applications.

6. **Theft or destruction of computing resources**: Since the computing equipment forms the back-bone of information processing, any theft or destruction of the resources can result in compromising the competitive advantage of the organization.

7. **Downtime due to technology failure**: IS facilities may become unavailable due to technical glitches or equipment failure and hence the computing infrastructure may not be available for short or extended periods of time. However, the period for which the facilities are not available may vary in criticality depending on the nature of business and the critical business process that the technology supports.

(b) **Data Dictionary**

A data dictionary is a computer file that contains descriptive information about the data items in the files of a business information system. Thus, a data dictionary is a computer file about data. Each computer record of a data dictionary contains infor-
mation about a single data item used in a business information system. Data dictionary contains the information about the identity of the computer programs or individuals permitted to access the data item for the purpose of file maintenance, upkeep or inquiry. It also maintains the identity of the computer programs or individuals, not permitted to access the data items. Because of maintaining above mentioned information, a data dictionary is useful for the security e.g. to prohibit certain employees from gaining access to sensitive payroll data.

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.

(c) Audit Trail Audit trail are logs that can be designed to record activity at the system, application, and user level. It provides an important detective control to help and accomplish security objectives. Many operating systems allow management to select the level of auditing to be provided by the system. This determines which events will be recorded in the log. Audit trails can be used to support security objectives in three ways:

• Detecting unauthorized access to the system,
• Facilitating the reconstruction of events, and
• Promoting personal accountability.

1. Detecting unauthorized access to the system: Detecting unauthorized 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 attempting 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 unauthorized access was accomplished, or attempted and failed.

2. Reconstructing 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 to 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.

3. **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 behavior. Individuals are less likely to violate an organization’s security policy if they know that their actions are recorded in an audit log. Audit trail are used to measure the potential damage and financial loss associated with application errors, abuse of authority, unauthorized access by outside intruders. Audit logs also provide valuable evidence or accessing both the adequacies of controls in place and the need for additional controls.

**Ans.3**

(a) **Implementation of ERP** ERP implementation is a special event, which integrates different business functions, different personalities, procedures, ideologies and philosophies together, brings worthwhile and beneficial changes throughout the organization. It involves considerable amount of time, effort, and valuable resources. One can get over the impediments for successful implementation of ERP in the following manner:

- The success of an implementation mainly depends on how closely the implementation consultants, users and vendors work together to achieve the overall objectives of the organization. The consultants should understand the needs of the users, understanding the business realities and design the business solutions keeping in mind all these factors. It is the users who will be driving the implementation and therefore their active involvement at all stages of implementation is vital for the overall success of implementation.

- During the course of implementation, the standard packages may undergo changes which may be a simple one or a major functionality’ change. Implementing such change is known as customization. It is always better to satisfy user requirements and overall objectives within the available framework of the existing package because any change in any functional module will have an adverse impact on the functioning of the other modules of the package.

- The roles and responsibilities of an employee to be clearly identified, understood and configured in the system. The employees will have to accept new processes and procedures laid down in the ERP system. At the same time, these process and procedures have to be simple and user friendly.
• The ability of the ERP package to manage and support dynamically changing business processes is critical requirement for the organization and therefore the package should be expandable and adaptable to meet these changes.

• An ERP package after implementation is expected to improve the flow of information and formalize and standardize all the business processes and workflow that exist in an enterprise. It is worthwhile to remember that ERP is an enabling tool, which makes one to do his/her work better, naturally needs additional efforts. A well managed and implemented ERP can give 200% return on investment.

(b) If a third party site is to be used for backup and recovery purposes, security administrators must ensure that a contract is written to cover the following issues:

• How soon the site will be made available subsequent to a disaster,

• The number of organizations that will be allowed to use the site concurrently in the event of a disaster,

• The priority to be given to concurrent users of the site in the event of a common disaster,

• The period during which the site can be used,

• The conditions under which the site can be used,

• The facilities and services the site provider agrees to make available, and

• The number of organizations that will be allowed to use the site concurrently in the event of a disaster,

• The priority to be given to concurrent users of the site in the event of a common disaster,

• The period during which the site can be used,

• The conditions under which the site can be used,

• The facilities and services the site provider agrees to make available, and

• What controls will be in place and working at the off-site facility.

The above are the main issues that should be covered while drafting a contract. These issues are often poorly specified in reciprocal agreements. Moreover, they can be difficult to enforce under a reciprocal agreement because of the informal nature of the agreement.

(c) The role of an IS auditor in evaluating logical access controls is briefly discussed below:

• S/he reviews the relevant documents pertaining to logical facilities, risk assessment and evaluation techniques and understands the security risks facing the information processing system.
The potential access paths into the system is evaluated by the auditor and documented to assess their sufficiency.

Deficiencies and redundancies are identified and evaluated.

By supplying appropriate audit techniques, s/he verifies test controls over access paths to determine its effective functioning.

S/he evaluates the access control mechanism, analyzes the test results and other auditing evidences and verifies whether the control objective has been achieved.

The auditor also compares security policies and practices of other organizations with the policies of their organizations and assesses its adequacy.

What controls will be in place and working at the off-site facility.

The above are the main issues that should be covered while drafting a contract. These issues are often poorly specified in reciprocal agreements. Moreover, they can be difficult to enforce under a reciprocal agreement because of the informal nature of the agreement.

(c) The role of an IS auditor in evaluating logical access controls is briefly discussed below:

- S/he reviews the relevant documents pertaining to logical facilities, risk assessment and evaluation techniques and understands the security risks facing the information processing system.
- The potential access paths into the system is evaluated by the auditor and documented to assess their sufficiency.
- Deficiencies and redundancies are identified and evaluated.
- By supplying appropriate audit techniques, s/he verifies test controls over access paths to determine its effective functioning.
- S/he evaluates the access control mechanism, analyzes the test results and other auditing evidences and verifies whether the control objective has been achieved.
- The auditor also compares security policies and practices of other organizations with the policies of their organizations and assesses its adequacy.

Ans.4

(a) Some of the advantages of continuous audit techniques are given as follows:

(i) Timely, comprehensive and detailed auditing – Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analysed rather than examining the inputs and the outputs only.

(ii) Surprise test capability – As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff...
and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.

(iii) Information to system staff on meeting of objectives - Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency. (iv) Training for new users - Using the Integrated Test Facilities (ITFs) new users can submit data to the application system, and obtain feedback on any mistakes they make via the system’s error reports.

(b)  

(i) Computer Contaminant: It refers to any set of computer instructions that are designed:

- to modify, destroy, record, transmit data or program residing within a computer, computer system or computer network; or
- by any means to disrupt the normal operation of the computer, computer system, or computer network.

(ii) Cyber Cafe: It refers to any facility from where access to the Internet is offered by any person in the ordinary course of business to the members of the public.

(iii) Electronic Form: It refers to any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated microfiche or similar device.

(iv) Traffic Data: It refers to any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, data size, duration or type of underlying service or any other information.

(v) Asymmetric crypto system: It refers to a system of secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

(c) Some of the important advantages of information system in business are discussed as under:

(i) Information system will help managers in effective decision making to achieve the organizational goal.

(ii) Based on well designed information system, an organization will gain edge in the competitive environment.

(iii) Information systems help in taking right decision at the right time.
(iv) Innovative ideas for solving critical problems may come out from good information system.

(v) Knowledge gathered through information system may be utilized by managers in unusual situations.

(vi) If information system is viewed as a process, it can be integrated to formulate a strategy of action or operation.

(d) COBIT or Control Objectives for Information and Related Technology is a framework of generally applicable information systems, security and control practices for IT Control. The framework allows:

- management to benchmark the security and control practices of IT environments,
- users of IT services to be assured that adequate security and control exist, and
- auditors to substantiate their opinions on internal control and to advise on IT security and control matters.

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

1. Business objectives: To satisfy business objectives, information must conform to certain criteria that COBIT refers to as business requirements for information. The criteria are divided into seven distinct yet overlapping categories that map into the COSO objectives namely, effectiveness (relevant, pertinent, and timely), efficiency, confidentiality, integrity, availability, compliance with legal requirements, and reliability.

2. IT resources which include people, application systems, technology, facilities, and data.

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

Ans.5

(a) The two primary questions to consider when evaluating the risk inherent in a business function are given below:

(i) What is the probability that things can go wrong? (Probability). This view will have to be taken strictly on the technical point of view and has to focus on the available measures that can prevent such happening.
(ii) What is the cost if ‘what can go wrong’ does go wrong? (Exposure)

**Purposes of Risk Evaluation**

The purpose of risk evaluation is to:

- identify the probabilities of failures and threats,
- calculate the exposure i.e. the damage or loss to assets, and
- make control recommendations keeping the cost benefit analysis in mind.

(b) Various factors which should be considered before undertaking the implementation of an ERP system are:

(i) **Integrate financial information:** As the CEO tries to understand the company’s overall performance, he may find many different versions of the truth. Finance has its own set of revenue numbers, sales has another version, and the different business units may each have their own version of how much they contributed to revenue. ERP creates a single version of the truth that cannot be questioned because everyone is using the same system.

(ii) **Integrate customer order information:** ERP systems can become the place where the customer order lives from the time a customer service representative receives it until the loading dock ships the merchandise and finance department sends an invoice. By having this information in one software system, rather than scattered among many different systems that can’t communicate with one another, companies can keep track of orders more easily, and coordinate manufacturing, inventory and shipping among many different locations simultaneously.

(iii) **Standardize and speed up manufacturing processes:** Manufacturing companies—especially those with an appetite for mergers and acquisitions—often find that multiple business units across the company make the same transaction/report using different methods and computer systems. ERP systems come with standard methods for automating some of the steps of the manufacturing process. Standardizing those processes and using a single, integrated computer system can save time, increase productivity and reduce headcount.

(iv) **Reduce inventory:** ERP helps the manufacturing process flow more smoothly, and it improves visibility of the order fulfillment process inside the company. It can lead to reduced inventories of the materials used to make products (work-in-progress inventory), and it can help users to better plan deliveries to customers, thereby reducing the finished good inventory at the warehouses and shipping docks. To really improve the flow of the supply chain, one needs supply chain software, but ERP helps too.

(v) **Standardize HR information:** Especially in companies with multiple business units, HR may not have a unified, simple method for tracking employees’ time and communicating with them about benefits and services. ERP can fix that problem.
The characteristics of the types of information used in Executive Decision Making are:

1. **Lack of structure**: Many of the decisions made by executives are relatively unstructured. For instance, what general direction should the company take? Or what type of advertising campaign will best promote the new product line? These types of decisions are not as clear-cut as deciding how to debug a computer program or how to deal with an overdue account balance. Also, it is not always obvious which data are required or how to weigh available data for reaching a decision. For example, how does an executive assess the future direction of the economy if the six sources on which that person typically depends for information, each forecasts something different? Even the portfolio of decisions that need to be made by the executive is an open issue. Should time be spent, for instance, considering new businesses to enter or should the company concentrate on looking for new markets for existing products?

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

3. **Future Orientation**: Strategic-planning decisions are made in order to shape future events. As conditions change, organizations must change also. It is the executive’s responsibility to make sure that the organization keeps pointed toward the future. Some key questions about the future include: “How will future technologies affect what the company is currently doing? What will the competition (or the government) do next? What products will consumers demand five years from now? Where will the economy move next, and how might that affect consumer buying patterns?” As one can see, the answers to all of these questions about the future external environment are vital.

4. **Informal source**: Executives, more than other types of managers, rely heavily on informal sources for key information. For example, lunch with a colleague in another firm might reveal some important competitor strategies. Informal sources such as television might also feature news of momentous concern to the executive – news that he or she would probably never encounter in the company’s database or in scheduled computer reports. Besides business meals and the media, some other important information sources of information are meetings, tours around the company’s facilities to chat with employees, brainstorming with a trusted colleague or two, and social events.

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

(d) **Unit Testing**

In computer programming, unit testing is a method of testing the correctness of a particular module of source code. The idea is to write test cases for every non-trivial function or method in the module so that each test case is separate from the others if possible. This type of testing is mostly done by the developers.

**Benefits of Unit Testing**: The goal of unit testing is to isolate each part of the program and show that the individual parts are correct. It provides a written contract that the piece must satisfy. The benefits of Unit testing are:

- **Encourages change**: Unit testing allows the programmer to re-factor code at a later date, and make sure that the module still works correctly (regression testing). This provides the benefit of encouraging programmers to make changes to the code since it is easy for the programmer to check if the piece is still working properly.

- **Simplifies Integration**: Unit testing helps eliminate uncertainty in the pieces themselves and can be used in a bottom-up testing style approach. By testing the parts of a program first and then testing the sum of its parts will make integration testing easier.

- **Documents the code**: Unit testing provides a sort of “living document” for the class being tested. Clients wishing to learn to use the class, can look at the unit tests to determine how to use the class to fit their needs.

**Limitations**: The limitations of Unit testing are:

- Unit testing will not catch every error in the program.
- It only tests the functionality of the units themselves.
- It will not catch integration errors, performance problems and any other system-wide issues.
- Unit testing is only effective if it is used in conjunction with other software testing activities.
INFORMATION SYSTEMS CONTROL AND AUDIT

NOVEMBER 2009

QUESTION PAPER

Q-1

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

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

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

Read the above carefully and answer the following with justifications:

(a) To overcome the problems which the financial analysts are facing, what kind of software the company should select? 

(10 Marks)

(b) The company is advised that the adoption of BS7799 International Standard will help in overcoming the problems and achieving its goals. Discuss.

(5 Marks)

(c) How should the human resources be enriched for effective utilization of the proposed new systems and standards?

(5 Marks)

Q-2

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

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

(5 Marks)
(b) Explain the threats due to Cyber crimes. (5 Marks)

(c) Discuss ‘Physical and Environmental Security with Control and Objectives’ with respect to information Security Policy? (5 Marks)

(d) How does the Information Technology Act, 2000 enable the authentication of records using digital signatures? (5 Marks)

Q-3

(a) What analysis should be done for understanding the degree of potential loss (such as reputation damage, regulation effects) of an organization? Enumerate the tasks to be undertaken in this analysis. In what ways the information can be obtained for this analysis? (10 Marks)

(b) Describe Risk Management Process. (5 Marks)

(c) Explain the term “Cryptosystems”. Briefly discuss Data Encryption Standard. (5 Marks)

Q-4

(a) You have been asked to conduct an I.S. Audit for a bank. (i) How will you develop a documented audit program? (ii) What kind of working papers and documentation you will prepare? (10 Marks)

(b) Explain the basic types of Information Protection that an Organization can use. (5 Marks)

(c) Discuss the three processes of Access Control Mechanism, when an user requests for resources. (5 Marks)

Q-5

(a) How does the Information Technology Act, 2000 enable the objective of the Government in spreading e-governance? (5 Marks)

(b) Briefly discuss Black Box Testing. (5 Marks)

(c) Discuss anti-virus software and its types. (5 Marks)

(d) ABC Limited has recently migrated to real-time Integrated ERP System. As an IS Auditor, advice the company as to what kinds of businesses risks it can face? (5 Marks)
Ans.1

(a) As the financial analysts of the company are working in six different geographical locations and the financial data is stored on seven different systems, located worldwide, therefore they are facing several problems. Few of them are as under:

- Missing the access to the same data as well as timely access to information.
- Dated budget and actual numbers for each business unit reside in seven different systems, separating critical components of the profit and loss account thus failing the financial analysts to assess results.
- The field analysts are not able to retrieve the data themselves from one universal place and therefore they have to rely upon the home office for the same.

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

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

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

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

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

The company can use BS 7799 for the following reasons:

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

This is achieved by ensuring that:

- Security controls are justified.
- Policies and procedures are appropriate.
- Security awareness is good amongst staff and managers.
- All security relevant information processing and supporting activities are auditable and are being audited.
- Internal audit, incident reporting / management mechanisms are being treated appropriately.
- Management actively focuses on information security and its effectiveness.

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

- **Training Personnel**: A system can succeed or fail depending on the way it is operated and used. Therefore, the quality of training received by the personnel involved with the system in various capacities helps in the successful implementation of information system and standards. Thus, training is a major component of systems implementation. When a new system is acquired which often involves new hardware and software, both users and computer experts need training organized by the vendor through hands-on learning techniques.

- Training Systems Operators: The effective implementation of new systems and standards also depend on the computer-centre personnel, who are responsible for keeping the equipment running as well as for providing the necessary support services. Their training must ensure that they are able to handle all possible operations, both routine and extra-ordinary. As part of their training, operators should be given a trouble shooting list that identifies possible problems and remedies for them. Training also involves familiarization with run procedures, which involve working through the sequence of activities needed to use a new system on an on-going basis.

- User training: User training deals with the operation of the system itself. Training in data coding emphasizes the methods to be followed in capturing data from transactions or preparing data for decision support activities. **Users should be trained**
data handling activities such as editing data, formulating inquiries (finding specific records or getting responses to questions) and deleting records of data. From time to time, users will have to prepare disks, load paper into printers, or change ribbons on printers. Some training time should be devoted to such system maintenance activities. If a micro computer or data entry system uses disks, users should be instructed in formatting and testing disks.

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

**Ans.2**

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

(v) Hardware-Software System | Closed Deterministic System | The interaction among the various parts of the system is known with certainty and it does not interact with the environment and does not change with the change in the environment. Here the requirements of the hardware and software inventory are known with certainty. The operational state of these systems is predictable.

(b) Threats due to cyber crimes are given as follows:

- **Embezzlement**: It is unlawful misappropriation of money or other things of value, by the person to whom it was entrusted, for his/her own use or purpose.

- **Fraud**: It occurs on account of intentional misappropriation of information or identifies to deceive others, the unlawful use of credential card or ATM, or the use of electronic means to transmit deceptive information, to obtain either money or other valuable things. Fraudulent may be an employee of the company or outsider.

- **Theft of proprietary information**: It is the illegal capturing of other’s documentation or information. Usually it is done by electronic copying. The things illegally copied may be in the form of design, plans, blue prints, codes, computer programs, formulas, trade secrets, graphics, copyrighted material, data, forms, files and personal or financial information etc.

- **Denial of service**: This is the disruption or degradation of external services. This is usually caused by events like ping attacks, port scanning probes and excessive amount of incoming data.

- **Vandalism or sabotage**: It is the deliberate or malicious damage, defacement, destruction or other alteration of electronic files, data, web pages, and programs.

- **Computer virus**: They are hidden computer codes. They are destruction programs. They propagate by inserting themselves or modifying other programs.

- **Others**: Threat includes several other cases such as intrusions, breaches and compromises of the respondent’s computer networks.
(c) **Physical and Environmental Security**: This is the beginning point of any security plan. It is designed to prevent unauthorized access, damage and interference to business premises and information. This involves physical security perimeter, physical entry control, creating secure offices, rooms, facilities, providing physical access controls, providing protection devices to minimize risks ranging from fire to electromagnetic radiation, providing adequate protection to power supplies and data cables. Cost effective design and constant monitoring are two key aspects to maintain adequate physical security control.

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

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

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

(d) Chapter-II, Section 3 of IT Act, 2000 provides conditions subject to which an electronic record is authenticated by means of affixing digital signature.

- The digital signature is created in two distinct steps. First the electronic record is converted into a message digest by using a mathematical function known as “hash function” which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tampering with the contents of the electronic record will immediately invalidate the digital signature.
- Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the corresponding public key.

This will enable anybody to verify whether the electronic record is retained intact or has been tampered with; since it was fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message.

Ans.3

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

For BIA, the following tasks are to be undertaken:

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

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

1. Questionnaires,
2. Workshops,
3. Interviews, and
4. Examination of documents.

The BIA Report should be presented to the Steering Committee. This report identifies critical service functions and the timeframe in which they must be recovered after interruption. The BIA Report should be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities.

(b) Risk Management Process: The broad Risk Management Process comprises of the following:

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

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

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

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

**Data Encryption Standard (DES)**: It is a cipher. It is a mathematical algorithm for encrypting
and decrypting binary coded information. Encrypting of data converts it to an unintelligible
form called cipher. Decrypting cipher converts the data back to its original form called
plaintext. Encryption and Decryption operations are done by using a binary number called
a key. A key consists of 64(bits) binary digits. Among these 64 bits, 56 bits are used for
encryption/ decryption and remaining 8 bits are used for error detection.

Authorized users of the encrypted data must have the unique key that was used to encipher
the data in order to decrypt it. Selection of a different key causes the cipher that is produced
for any given set of inputs to be different. The cryptographic security of the data depends
on the security provided for the key used to encipher and decipher the data. A standard
algorithm based on a secure key thus provides a basis for exchanging encrypted computer
data by issuing the key used to encipher it to those authorized to have the data.

The encryption and decryption processes are depicted in the following diagram:
Some documentation distinguishes DES from its algorithms. It refers algorithms as DEA (Data Encryption Algorithm).

Ans.4 (a)

(i) The documented audit program is developed with the help of following activities:

- Documentation of the IS auditor’s procedures for collecting, analysing, interpreting, and documenting information during the audit.
- Objectives of the audit.
- Scope, nature, and degree of testing required to achieve the audit objectives in each phase of the audit.
- Identification of technical aspects, risks, processes, and transactions which should be examined.
- Procedures for audit will be prepared prior to the commencement of audit work and modified, as appropriate, during the course of the audit.

(ii) Audit Working Papers and Documentation

Working papers should record the audit plan, the nature, timing and extent of auditing procedures performed, and the conclusions drawn from the evidence obtained. All significant matters which require the exercise of judgment, together with the auditor’s conclusion thereon, should be included in the working papers. The form and content of the working papers are affected by matters such as:

- The nature of the engagement
- The form of the auditor’s report
- The nature and complexity of client’s business
- The nature and condition of client’s records and degree of reliance on internal controls.

In case of recurring audits, some working paper files may be classified as permanent audit files which are updated currently with information of continuing importance to succeeding audits, as distinct from the current audit files which contain information relating primarily to audit of a single period.

The permanent audit file normally includes:

- The organization structure of the entity.
- The IS policies of the organization.
- The historical background of the information system in the organization.
- Extracts of copies of important legal documents relevant to audit.
• A record of the study and evaluation of the internal controls related to the information system.
• Copies of audit reports and observations of earlier years.
• Copies of management letters issued by the auditor, if any.

The current file normally includes:
• Correspondence relating to the acceptance of appointment and the scope of the work.
• Evidence of the planning process of the audit and audit programme.
• A record of the nature, timing, and extent of auditing procedures performed, and the results of such procedures.
• Copies of letters and notes concerning audit matters communicated to or discussed with the client, including material weaknesses in relevant internal controls.
• Letters of representation and confirmation received from the client.
• Conclusions reached by the auditor concerning significant aspects of the audit, including the manner in which the exceptions and unusual matters, if any, disclosed by the auditor’s procedures were resolved and treated.
• Copies on the data and system being reported on and the related audit reports.

Working papers are the property of the auditor. The auditor may, at his discretion, make portions of, or extracts from his working papers available to the client. The auditor should adopt reasonable procedures for custody and confidentiality of his working papers and should retain them for a period of time sufficient to meet the needs of his practice and satisfy any pertinent legal and professional requirements of record retention.

(b) **Types of Information Protection** : The two basic types of information protection that an organization can use are given as follows:

1. Preventative Information Protection, and
2. Restorative Information Protection.

**Preventative Information Protection** : It is based on use of security controls, which itself is a group of three types of controls such as Physical, Logical, and Administrative.

Physical controls deal with Doors, Locks, Guards, Floppy Disk Access Locks, Cables locking systems to desks/walls, CCTV, Paper Shredders, Fire Suppression Systems,

Logical controls deal with Passwords, File Permissions, Access Control Lists, Account Privileges, Power Protection Systems, and Administrative controls deal with Security Awareness, User Account Revocation, and Policy,
**Restorative Information Protection** : If an organization cannot recover or recreate critical information systems in an acceptable time period, the organization will suffer and possibly have to go out of business. Hence, the key requirement of any restorative information system protection plan is that the information systems can be recovered. The claim of back program to backup data automatically cannot be reliable. It has so many problems. The restorative information protection program must address the following:

- Whether the recovery process has been evaluated and tested recently?
- The time taken for restoration,
- The quantum of productivity loss,
- The strict adherence of plan, and
- The time needed to input the data changes since the last backup.

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

- Identification
- Authentication
- Authorization

The access control mechanisms operate in the following sequence:

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

The mechanism accesses

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

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

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

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

- **Ticket oriented**: In this approach the access control mechanism assigns the users a ticket for each resource they are permitted to access. Ticket oriented approach operates via a row in the matrix. Each row along with the user resources holds the action privileges specific to that user.

- **List oriented**: In this approach, the mechanism associates with each resource a list of users who can access the resource and the action privileges that each user has with respect to the resource.

**Ans.5**

(a) In Information Technology Act 2000, chapter III is related with the objective of the government in spreading e-governance. It deals with the procedures to be followed for sending and receiving of electronic records. This chapter contains sections 4 to 10.

**Section 4** - This section provides the legal recognition of electronic records.

**Section 5** - This section provides the legal recognition of Digital Signatures.

**Section 6** - It lays down the foundation of Electronic Governance. It provides that the filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any license or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form.

Section 7 - This section provides that the documents, records or information which is to be retained for any specified period shall be deemed to have been retained in the electronic form with the following conditions:

(i) the information therein remains accessible so as to be usable subsequently,
(ii) it is retained in its original format,
(iii) the details such as origin, destination, dates and time of dispatch or receipt of such electronic record.

Section 8 - It provides for the publication of rules, regulations and notifications in the Electronic Gazette.

(b) **Black box testing**: Black box testing attempts to derive sets of inputs that will fully exercise all the functional requirements of a system. It is not an alternative to white box testing. This type of testing attempts to find errors in the following categories:

- incorrect or missing functions,
- interface errors,
• errors in data structures or external database access,
• performance errors, and
• initialization and termination errors.

Tests are designed to answer the following questions:
• How is the function’s validity tested?
• What classes of input will make good test cases?
• Is the system particularly sensitive to certain input values?
• How are the boundaries of a data class isolated?
• What data rates and data volume can the system tolerate?
• What effect will specific combinations of data have on system operation?

Some of the methods used for test cases are as follows:

• **Equivalence Partitioning**: This method divides the input domain of a program into classes of data from which test cases can be derived. Equivalence partitioning strives to define a test case that uncovers classes of errors and thereby reduces the number of test cases needed. It is based on an evaluation of equivalence classes for an input condition. An equivalence class represents a set of valid or invalid states for input conditions.

• **Boundary Value Analysis (BVA)**: This method leads to a selection of test cases that exercise boundary values. It complements equivalence partitioning since it selects test cases at the edges of a class. Rather than focusing on input conditions solely, BVA derives test cases from the output domain also.

• **Cause-Effect Graphing Techniques**: This technique provides a concise representation of logical conditions and corresponding actions. Causes (input conditions) and effects (actions) are listed for a module and represented in a cause-effect graph. This graph is converted to a decision table rules which are used to derive test cases.

(c) **Anti-virus Software**: It is a program that is used to detect viruses, and prevent their further propagation and harm. Three types of anti-virus software are briefly discussed below:

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

Active Monitor and Heuristic Scanner: This looks for critical interrupt calls and critical operating systems functions such as OS calls and BIOS calls, which resemble virus action.
Integrity Checkers: These can detect any unauthorized changes to files on the system. These can detect any unauthorized changes to the files on the system. The software performs a "take stock" of all files resident on the system and computes a binary check data called the Cyclic Redundancy Check (CRC). When a program is called for execution, the software computes the CRC again and checks with the parameter stored on the disk.

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

1. Single point of failure - All input data of an organization and transaction processing is within one application system.
2. Structural Changes - Significant personnel and organizational structural changes associate with reengineering or redesigning business processes.
3. Job Role Changes - Traditional roles of users are changed to empowered-based role. They have more chances to access enterprise information in real-time. This point of control shifts from the back-end financial processes to the front-end point of creation.
4. Online Real-Time - This environment requires a continuous business interaction. This warrants the capabilities of utilizing the ERP application and responds quickly to any problem that requires a re-entry of information (e.g., if field personnel are unable to transmit orders from handheld terminals, customer service staff may need the skills to enter orders into the ERP system correctly so the production and distribution operations will not be adversely impacted).
5. Change Management - It is challenging to bring together a highly integrated environment when different business processes have existed among business units for long. The level of user acceptance of the system has a significant influence on its success. Training and awareness of users is mandatory, to understand that their actions or inaction have a direct impact upon other users and in the performance of their day-to-day duties.
6. Distributed Computing Experience - Inexperience with implementing and managing this kind of environment may pose significant challenges.
7. Broad System Accessibility - Increased remote access by users and outsiders and high integration among application functions allow increased access to the application and data.
8. Dependency on External Assistance - Organization accustomed to in-house legacy systems may find that they have to rely on external help. Unless such external assistance is properly managed, it could introduce an element of security and resource management risk that may expose the organizations to a greater risk.
9. Program Interfaces and Data Conversions - Extensive interfaces and data conversions from legacy systems and other commercial software are necessary. The exposures of data integrity, security and capacity requirements for ERP are much higher.

10. Audit Expertise - Specialist expertise is required to effectively audit and control an ERP environment. The relative complexity of ERP systems has created specialization such that each specialist may know only a relatively small fraction of the entire ERP’s functionality in a particular core module, e.g. FI auditors, who are required to audit the entire organization’s business processes, have to maintain a good grasp of all the core modules to function effectively.

11. Single sign on - It reduces the security administration efforts associated with administering web-based access to multiple systems, but simultaneously introduces additional risks in that an incorrect assignment of access may result in inappropriate access to multiple systems.

12. Data content quality - As enterprise applications are opened to external suppliers and customers, the need for integrity in enterprise data becomes paramount.

13. Privacy and confidentiality - Regularity and governance issues surrounding the increased capture and visibility of personal information, i.e. spending habits.
Q-1

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

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

Read the above carefully and answer the following with justifications:

(a) What are the problems that the company is facing now? (5 Marks)

(b) Should the company go for ERP solution? If yes, will the company be able to share a common platform with its dealers to access servers and database to update the information of issues of mutual interest? (5 Marks)

(c) For the selection of ERP package, state the issues to be considered. (5 Marks)

(d) Suggest how to go about the implementation of ERP package. (5 Marks)

Q-2

(a) The top management of company has decided to develop a computer information system for its operations. Is it essential to conduct the feasibility study of system before implementing it? If answer is yes, state the reasons. Also discuss three different angles through which the feasibility study of the system is to be conducted. (10 Marks)

(b) “While reviewing a client’s control system, an information system auditor will identify three components of internal control.” State and briefly explain these three components. (5 Marks)
Q-3
(a) A company is engaged in the stores taking data activities. Whenever, input data error occurs, the entire stock data is to be reprocessed at a cost of Rs. 50,000. The management has decided to introduce a data validation step that would reduce errors from 12% to 0.5% at a cost of Rs. 2,000 per stock taking period. The time taken for validation causes an additional cost of Rs. 200. (i) Evaluate the percentage of costbenefit effectiveness of the decision taken by the management and (ii) suggest preventive control measures to avoid errors for improvement.

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

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

Q-4
(a) As a system auditor, what control measures will you check to minimize threats, risks and exposures in a computerized system?

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

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

Q-5
(a) When an organization is audited for the effective implementation of ISO 27001-(BS 7799: part II)-Information Security Management System, what are to be verified under.

(i) Establishing Management Framework

(ii) Implementation

(iii) Documentation.
(b) The Information Security Policy of an organization has been defined and documented as given below:

“Our organization is committed to ensure Information Security through established goals and principles. Responsibilities for implementing every aspect of specific applicable proprietary and general principles, standards and compliance requirements have been defined. This is reviewed at least once a year for continued suitability with regard to cost and technological changes.”

Identify the salient components that have not been covered in the above policy.  
(5 Marks)

(c) Briefly explain Asset Classification and Control under Information Security Management Systems.  
(5 Marks)

Q-6

(a) What purpose the information system audit policy will serve? Briefly describe the scope of information system audit.  
(10 Marks)

(b) State the duties of the subscriber of a digital signature as specified in Section 40 to 42 of Chapter VIII of Information Technology Act, 2000.  
(5 Marks)

(c) What are the conditions subject to which electronic record may be authenticated by means of affixing digital signature?  
(5 Marks)

Q-7 Write short notes on the following:  
(4x5=20 Marks)

(a) System Manual

(b) Control Objectives for Information related Technology (COBIT)

(c) Firewalls

(d) White Box Testing.
Ans.1

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

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

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

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

(c) While selecting the ERP package, the performance of following issues should be taken into account:

(i) Better inventory management and control.
(ii) Improved financial reporting and control.
(iii) Automation of certain tasks that were performed manually to increase productivity.
(iv) Improved production planning.
(v) Better information on stocks at various locations.
(vi) Using an integrated system as opposed to disparate systems at different locations, thereby eliminating errors of duplicate entries.

(vii) More accurate costing of products.

(viii) Better credit control.

(ix) Improved cash flow planning.

(x) Automatic quality control and tracking.

(xi) Better after-sales services.

(xii) Better information and reporting to top management.

(d) In the stated scenario, several steps involved in the implementation of a typical ERP package are enumerated below:

(i) Identifying the needs for implementing an ERP package.

(ii) Evaluating the ‘As Is’ situation of the business i.e., to understand the strength and weakness prevailing under the existing circumstances.

(iii) Deciding the ‘Would be’ situation for the business i.e., the changes expected after the implementation of ERP.

(iv) Reengineering the Business Process to achieve the desired results in the existing processes.

(v) Evaluating the various available ERP packages to assess suitability.

(vi) Finalizing of the most suitable ERP package for implementation.

(vii) Installing the required hardware and networks for the selected ERP package.

(viii) Finalizing the Implementation consultants who will assist in implementation.

(ix) Implementing the ERP package.

Ans.2

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

The feasibility study of the system is undertaken from three angles i.e. technical, economic and operational. The proposed system is evaluated from a technical viewpoint first and if technically feasible, its impact on the organization and staff is assessed. If a compatible technical and social system can be devised, it is then tested for economic feasibility.
**Technical feasibility**: It is concerned with hardware and software. Essentially, the analyst ascertains whether the proposed system is feasible with existing or expected computer hardware and software technology. The technical issues usually raised during the feasibility stage of investigation include the following:

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

(ii) Does the proposed equipment have the technical capacity to hold the data required to use the new system?

(iii) Will the proposed system provide an adequate response to inquires, regardless of the number or location of users ?

(iv) Can the system be expanded if developed?

(v) Are there technical guarantees of accuracy, reliability, ease of access, the data security ?

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

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

**Table-1: Technical Issues**
Due to tremendous advancements in computer field these days, the technology is available for most business data processing systems but sometimes not within the constraints of the firm's resources or its implementation schedule. Therefore, trade offs are often necessary. A technically feasible system may not be economically feasible or may be so sophisticated that the firm's personnel cannot effectively operate it.

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

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

The procedure employed is the traditional cost-benefit study.

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

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

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

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

(i) **Accounting Controls**: These controls are extended to safeguard the client’s assets and ensure reliability of financial records.

(ii) **Operational Controls**: These deal with the day to day operations, functions and activities to ensure that the operational activities are contributing to business objectives.

(iii) **Administrative Control**: These are concerned with ensuring efficiency and compliance with management policies, including the operational controls.

(c) Following are the main testing techniques which involve the people working in the system areas:

(i) **White Box Testing**: White box testing is a test case design method that uses the control structure of the procedural design to derive test cases. Test cases can be derived to
   • guarantee that all independent paths within a module have been exercised at least once,
   • exercise all logical decisions on their true and false sides,
   • execute all loops at their boundaries and within their operational bounds, and
   • exercise internal data structures to ensure their validity

(ii) **Unit Testing**: In computer programming, a unit test is a method of testing the correctness of a particular module of source code. The idea is to write test cases for every non-trivial function or method in the module so that each test case is separate from the others if possible. This type of testing is mostly done by the developers.

(iii) **Requirements Testing**: These test conditions are generalized ones, which become test cases as the SDLC progresses until system is fully operational. The main usage of this testing technique is
   • to ensure that system performs correctly
   • to ensure that correctness can be sustained for a considerable period of time.
   • system can be tested for correctness through all phases of SDLC but in case of reliability the programs should be in place to make system operational.

(iv) **Regression Testing**: Under this testing technique, test cases, which were used previously...
Validation for the already tested segment are, re-run to ensure that the results of the segment tested currently and the results of same segment being tested earlier, are same. Test automation is needed to carry out the test transactions (test condition execution) else the process is very time consuming and tedious. In this case of testing, cost/benefit should be carefully evaluated else the efforts spend on testing would be more and payback would be minimum. The major objectives are as follows:

- System documents remain current.
- System test data and test conditions remain current.
- Previously tested system functions properly without getting effected though changes are made in some other segment of application system.

(v) Manual Support Testing: It involves testing of all the functions performed by the people while preparing the data and using these data from automated system. The major objectives of this testing technique are to

- verify that manual support documents and procedures are correct,
- determine that manual support responsibility is correct,
- determine that manual support people are adequately trained,
- determine that manual support and automated segment are properly interfaced.

(vi) Internal System Testing: This technique is used to ensure interconnection between application functions correctly. The major objectives of the testing are to ensure that

- proper parameters and data are correctly passed between the applications,
- documentation for involved system is correct and accurate,
- proper timing and coordination of functions exists between the application systems.

Ans.3 (a)

(i) The percentage of cost benefit effectiveness based on the information is calculated in the following table:
<table>
<thead>
<tr>
<th>S. No.</th>
<th>Particulars</th>
<th>Without validation Procedure</th>
<th>With Validation Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Cost of reprocessing the stock data</td>
<td>Rs. 50,000</td>
<td>Rs. 50,000</td>
</tr>
<tr>
<td>2.</td>
<td>Risk of data errors</td>
<td>12%</td>
<td>0.5%</td>
</tr>
<tr>
<td>3.</td>
<td>Expected processing cost</td>
<td>Rs. 6,000</td>
<td>Rs. 2,000</td>
</tr>
<tr>
<td>4.</td>
<td>Cost of validation procedure</td>
<td>Nil</td>
<td>Rs. 250</td>
</tr>
<tr>
<td>5.</td>
<td>Cost of delay due to validation</td>
<td>Nil</td>
<td>Rs. 200</td>
</tr>
<tr>
<td>6.</td>
<td>Total cost involved</td>
<td>Rs. 56,000</td>
<td>Rs. 52,450</td>
</tr>
<tr>
<td>7.</td>
<td>Net expected benefit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>in %</td>
<td></td>
<td>6.3%</td>
</tr>
</tbody>
</table>

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

**(ii) Preventive Control Measures**

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

(i) A clear-cut understanding about the vulnerabilities of the asset.

(ii) Understanding probable threats.

(iii) Provision of necessary controls for probable threats from materializing.

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

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

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

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

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Manual Control</th>
<th>Computerized Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrict unauthorized entry into the premises</td>
<td>Build a gate and post a security guard.</td>
<td>Use access control software, smart card, biometrics, etc.</td>
</tr>
<tr>
<td>Restricted</td>
<td>Keep the computer in a secured location and allow unauthorized entry into the software</td>
<td>Use access control, viz. User ID, password, smart card, etc.</td>
</tr>
<tr>
<td></td>
<td>only authorized person to use the applications.</td>
<td></td>
</tr>
</tbody>
</table>

**Table-2: Manual & Computerized Controls**

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

(i) Interview business users in each functional area covered by the system, and assess their satisfaction with, and overall use of, the system.

(ii) Interview security, operations and maintenance staff and, within the context of their particular responsibilities, assess their reactions to the system.

(iii) Based on the User Requirements Specification, determine whether the system’s requirements have been met. Identify the reasons(s) why any requirements are not to be provided, are yet to be delivered, or which do not work properly.

(iv) Confirm that the previous system has been decommissioned or establish the reasons(s) why it remains in use.

(v) Review system problem reports and change proposals to establish the number and nature (routine, significant, major) of problems, and changes being made to remedy them. The volume of system change activity can provide an indicator of the quality of systems development.

(vi) Confirm that adequate internal controls have been built into the system, that these are adequately documented, and that they are being operated correctly. Review the number and nature of internal control rejections to determine whether there are any underlying system design weaknesses.
(vii) Confirm that an adequate Service Level Agreement has been drawn up and implemented. Identify and report on any area where service delivery either falls below the level specified, or is inadequate in terms of what was specified.

(viii) Confirm that the system is being backed up in accordance with user requirements, and that it has been successfully restored from backup media.

(ix) Review the Business Case and determine whether:
- anticipate benefits have / are been achieved;
- any unplanned benefits have been identified;
- costs are in line with those estimated;
- benefits and costs are falling with the anticipated time-frame.

(x) Review trends in transaction throughput and growth in storage use to identify that the anticipated growth of the system is in line with the forecast.

(c) Any computerized environment is dependent on people. Though they play a critical role in success of an enterprise computing, it is a fact that threats always exist due to cyber crimes committed by people. The special skill sets of IT operational team, programmers; data administrator, etc. are key links in ensuring that the IT infrastructure delivers output as per user requirements. At the same time, social engineering risks target key persons to get sensitive information to exploit the information resources of the enterprise. Threats also arise on account of dependence on external agencies. IT computing services are significantly dependant on various vendors and service providers for equipment supply and support, consumables, systems and program maintenance, airconditioning, hot-site providers, utilities, etc. Following are some of the serious threats due to cyber crimes:

- **Embezzlement**: It is unlawful misappropriation of money or other things of value, by the person to whom it was entrusted (typically an employee), for his/ her own use or purpose.

- **Fraud**: It occurs on account of internal misrepresentation of information or identity to deceive others, the unlawful use of credit/ debit card or ATM, or the use of electronic means to transmit deceptive information, to obtain money or other things of value. Fraud may be committed by someone inside or outside the company.

- **Theft of proprietary information**: It is illegal to obtain of designs, plans, blueprints, codes, computer programs, formulas, recipes, trade secrets, graphics, copyrighted material, data, forms, files, lists, and personal or financial information, usually by electronic copying.

- **Denial of service**: There can be disruption or degradation of service that is dependent on external infrastructure. Problems may erupt through internet connection or e-
mail service that result in an interruption of the normal flow of information. Denial of service is usually caused by events such as ping attacks, port scanning probes, and excessive amounts of incoming data.

- Vandalism or sabotage: It is the deliberate or malicious, damage, defacement, destruction or other alteration of electronic files, data, web pages, and programs.
- Computer virus: Viruses are hidden fragments of computer codes which propagates by inserting themself into or modifying other programs.
- Other: Threat includes several other cases such as intrusion, breaches and compromises of the respondent’s computer networks (such as hacking or sniffing) regardless of whether damage or loss were sustained as a result.

Ans.4

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

(i) **Lack of integrity**: Control measures to ensure integrity include implementation of security policies, procedures and standards, use of encryption techniques and digital signatures, inclusion of data validation, editing, and reconciliation techniques for inputs, processes and outputs, updated antivirus software, division of job and layered control to prevent impersonation, use of disk repair utility, implementation of user identification, authentication and access control techniques, backup of system and data, security awareness programs and training of employees, installation of audit trails, audit of adequacy of data integrity.

(ii) **Lack of confidentiality**: Control measures to ensure confidentiality include use of encryption techniques and digital signatures, implementation of a system of accountability by logging and journaling system activity, development of a security policy procedure and standard, employee awareness and training, requiring employees to sign a non-disclosure undertaking, implementation of physical and logical access controls, use of passwords and other authentication techniques, establishment of a documentation and distribution schedule, secure storage of important media and data files, installation of audit trails, and audit of confidentiality of data.

(iii) **Lack of system availability**: Control measures to ensure availability include implementation of software configuration controls, a fault tolerant hardware and software for continuous usage and an asset management software to control inventory of hardware and software, insurance coverage, system backup procedure to be implemented, implementation of physical and logical access controls, use of passwords and other
authentication techniques, incident logging and report procedure, backup power supply, updated antivirus software, security awareness programmes and training of employees, installation of audit trails, audit of adequacy of availability safeguards.

(iv) Unauthorized users attempt to gain access to the system and system resources: Control measures to stop unauthorized users to gain access to system and system resources include identification and authentication mechanism such as passwords, biometric recognition devices, tokens, logical and physical access controls, smart cards, disallowing the sharing of passwords, use of encryption and checksum, display of warning messages and regular audit programs.

Data transmitted over a public or shared network may be intercepted by an unauthorized user, security breaches may occur due to improper use or bypass of available security features, strong identification and authentication mechanisms such as biometric, tokens, layered system access controls, documentation procedures, quality assurance controls and auditing.

(v) Hostile software e.g. virus, worm, Trojan horses, etc.: Establishment of polices regarding sharing and external software usage, updated anti-virus software with detection, identification and removal tools, use of diskless PCs and workstations, installation of intrusion detection tools and network filter tools such as firewalls, use of checksums, cryptographic checksums and error detection tools for sensitive data, installation of change detection tools, protection with permissions required for the ‘write’ function.

(vi) Disgruntled employees: Control measures to include installation of physical and logical access controls, logging and notification of unsuccessful logins, use of disconnect feature on multiple unsuccessful logins, protection of modem and network devices, installation of one time use only passwords, security awareness programs and training of employees, application of motivation theories, job enrichment and job rotation.

(vii) Hackers and computer crimes: Control measures to include installation of firewall and intrusion detection systems, change of passwords frequently, installation of one time use passwords, discontinuance of use of installed and vendor installed passwords, use of encryption techniques while storage and transmission of data, use of digital signatures, security of modem lines with dial back modems, use of message authentication code mechanisms, installation of programs that control change procedures, and prevent unauthorized changes to programs, installation of logging feature and audit trails for sensitive information.

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

(b) Four most commonly used techniques to access and evaluate risks are:

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

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

(i) Judgment and intuition: In many situations, the auditors have to use their judgment and intuition for risk assessment. This mainly depends on the personal and professional experience of the auditors and their understanding of the system and its environment. Together with it, systematic education and ongoing professional updating is also required.

(ii) The Delphi Approach: This technique is used for obtaining a consensus opinion. A panel of experts is engaged and each expert is asked to give his opinion in a written and independent method. They enlist the estimate of the cost benefits and the reasons why a particular system is to be chosen, the risks and exposures of the system. These estimates are then compiled together. The estimates falling within a pre-decided acceptable range are taken. The process may be repeated four times for revising estimates falling beyond the range. Then a curve is drawn taking all the estimates as points on the graphs. The median is drawn and this is the consensus opinion.

(iii) The Scoring Approach: In this approach, the risks in the system and their respective exposures are listed. Weights are then assigned to the risks and to the exposures depending on the severity, impact of occurrence and costs involved. The product of the risk weight with the exposure weight of every characteristic gives the weighted score. The sum of these weighted score gives the risk and exposure score of the system. System risks and exposures are then ranked according to the scores.

(iv) Quantitative Techniques: Quantitative techniques involve the calculating of an annual loss exposure value based on the probability of the event and the exposure in terms of estimated costs. This helps the organization to select cost effective solutions. It is the assessment of potential damage in the event of occurrence of unfavorable events, keeping in mind how often such an event may occur.
(c) Audit tools and techniques used by a system auditor to ensure that the disaster recovery plan is in order, are briefly discussed below:

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

(i) Automated tools: They make it possible to review large computer systems for a variety of flaws in a short time period. They can be used to find threats and vulnerabilities such as weak access controls, weak passwords, and lack of integrity of the system software.

(ii) Internal Control auditing: This includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance for laws and regulations.

(iii) Disaster and Security Checklists: These checklists are used to audit the system. The checklists should be based upon disaster recovery policies and practices, which form the baseline. Checklists can also be used to verify changes to the system from contingency point of view.

(iv) Penetration Testing: It is used to locate vulnerabilities to the system.

Ans.5

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

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

(i) Establishing Management Framework: This would include the following activities:

- Define information security policy;
- Define scope of ISMS including functional, asset, technical, and locational boundaries;
- Make appropriate risk assessment;
- Identify areas of risk to be managed and degree of assurance required;
- Select appropriate controls;
- Prepare Statement of Applicability.

(ii) Implementation: Effectiveness of procedures to implement controls to be verified while reviewing security policy and technical compliance.
(iii) **Documentation:** The documentation shall consist of evidence of action undertaken under establishment of the following:

- Management control
- Management framework summary, security policy, control objective, and implemented control given in prepare Statement of Applicability
- Procedure adopted to implement control under Implementation clause
- ISMS management procedure
- Document Control: The issues focused under this clause would be
  - Ready availability
  - Periodic review
  - Maintain version control;
  - Withdrawal when obsolete
  - Preservation for legal purpose

- Records: The issues involved in record maintenance are as follows:
  - Maintain to evidence compliance to Part 2 of BS7799;
  - Procedure for identifying, maintaining, retaining, and disposing of such evidence;
  - Records to be legible, identifiable and traceable to activity involved.
  - Storage to augment retrieval, and protection against damage.

**A Policy** is a plan or course of action, designed to influence and determine decisions, actions and other matters. The security policy is a set of laws, rules, and practices that regulates how assets including sensitive information are managed, protected, and distributed within the user organization.

An information Security policy addresses many issues such as disclosure, integrity and availability concerns, who may access what information and in what manner, basis on which access decision is made, maximized sharing versus least privilege, separation of duties, who controls and who owns the information, and authority issues.

**Issues to address:** This policy does not need to be extremely extensive, but clearly state senior management’s commitment to information security, be under change and version control and besigned by the appropriate senior manager. The policy should at least address the following issues:

- a definition of information security,
- reasons why information security is important to the organization, and its goals and principles,
• a brief explanation of the security policies, principles, standards and compliance requirements,
• definition of all relevant information security responsibilities, and
• reference to supporting documentation.

The auditor should ensure that the policy is readily accessible to all employees and that all employees are aware of its existence and understand its contents. The policy may be a stand-alone statement or part of more extensive documentation (e.g. a security policy manual) that defines how the information security policy is implemented in the organization. In general, most if not all employees covered by the ISMS scope will have some responsibilities for information security, and auditors should review any declarations to the contrary with care. The auditor should also ensure that the policy has an owner who is responsible for its maintenance and that it is updated responding to any changes affecting the basis of the original risk assessment.

In the stated scenario of the question, the ISMS Policy of the given organization does not address the following issues:

(i) Definition of information security,
(ii) Reasons why information security is important to the organization,
(iii) A brief explanation of the security policies, principles, standards and compliance,
(iv) Reference to supporting documents.

(c) Asset Classification and Control

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

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

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

The detailed control and objectives thereof are as follows:

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

**Ans.6**

(a) **Purpose of the Audit Policy**

The purpose of the audit policy is to provide the guidelines to the audit team to conduct an audit of IT based infrastructure system. The audit is done to protect entire system from the most common security threats which includes the following:

- Access to confidential data
- Unauthorized access of the department computers
- Password disclosure compromise
- Virus infections
- Denial of service attacks
- Open ports, which may be accessed by outsiders
- Unrestricted modems, unnecessarily open ports

Audits may be conducted to ensure integrity, confidentiality and availability of information and resources. The IS Audit Policy should lay out the objective and the scope of the Policy.

An IS audit is conducted to:
• Safeguarding of Information System Assets/Resources
• Maintenances of Data Integrity
• Maintenance of System Effectiveness
• Ensuring System Efficiency
• Compliance with Information System related policies, guidelines, circulars, and any other instructions requiring compliance in whatever name called.

Scope of IS Audit

The scope of information system auditing should encompass the examination and evaluation of the adequacy and effectiveness of the system of internal control and the quality of performance by the information system. Information System Audit will examine and evaluate the planning, organizing, and directing processes to determine whether reasonable assurance exists that objectives and goals will be achieved. Such evaluation, in the aggregate, provides information to appraise the overall system of internal control.

The scope of the audit will also include the internal control system(s) for the use and protection of information and the information system, as under:

• Data
• Application systems
• Technology
• Facilities
• People

The information System auditor will consider whether the information obtained from the above reviews indicates coverage of the appropriate areas. The information system auditor will examine, among other, the following:

• Information system mission statement and agreed goals and objectives for information system activities.
• Assessment of the risks associated with the use of the information systems and approach to managing those risks.
• Information system strategy plans to implement the strategy and monitoring of progress against those plans.
• Information system budget and monitoring of variances.
• High level polices for information system use and the protection and monitoring of compliance with these polices.
• Major contract approval and monitoring of performance of the supplier.
• Monitoring of performance against service level agreements
• Acquisition of major systems and decisions on implementation.
• Impact of external influences on information system such as internet, merger of suppliers or liquidation etc.
• Control of self-assessment reports, internal and external audit reports, quality assurance reports or other reports on Information System.
• Business Continuity Planning, Testing thereof and Test results.
• Compliance with legal and regulatory requirements
• Appointment, performance monitoring and succession planning for senior information system staff including internal information system audit management and business process owners.

(b) The duties of the subscriber of a Digital Signature as specified in Section 40 to 42 of Chapter VII of IT Act- 2000 are as follows:

On acceptance of the Digital Signature Certificate the subscriber shall generate a key pair using a secure system.

A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate-
(i) to one or more persons;
(ii) in a repository, or otherwise demonstrates his approval of the Digital Signature certificate in any manner.

By accepting a Digital Signature Certificate, the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that –
(i) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;
(ii) all representations made by the subscriber to the Certificate Authority and all material relevant to the information contained in the Digital Signature Certificate are true;
(iii) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

The subscriber shall exercise all reasonable care to retain control of his private key corresponding to the public key. If such private key has been compromised (i.e., endangered or exposed), the subscriber must immediately communicate the fact to the Certifying Authority.

Otherwise, the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.
Chapter-II of IT Act, 2000 gives legal recognition to electronic records and digital signatures. It contains only section 3.

This Section deals with the conditions subject to which an electronic record may be authenticated by means of affixing digital signature which is created in two definite steps. First the electronic record is converted into a message digest by using a mathematical function known as “Hash function” which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tampering with the contents of the electronic record will immediately invalidate the digital signature. Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by any body who has the public key corresponding to such private key. This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message.

For the purposes of this sub-section, “hash function” means an algorithm mapping or translation of one sequence of bits into another, generally smaller set known as “hash result” such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible -

- to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
- that two electronic records can produce the same hash result using the algorithm.

Ans.7

(a) **System Manual**: The basic output of the system design is a description of the task to be performed, complete with layouts and flowcharts. This is called the job specifications manual or system manual. It contains:

(i) General description of the existing system.

(ii) Flow of the existing system.

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

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

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

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

(viii) Input layouts - the inputs to the new system are described and complete layouts of the input documents and input disks or tapes provided.

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

(x) Macro-logic - the overall logic of the internal flow will be briefly described by the systems analyst, wherever useful.

(xi) Files to be maintained - the specifications will contain a listing of the tape, disk or other permanent record files to be maintained, and the items of information to be included in each file. There must be complete layouts for intermediate or work file; these may be prepared later by the programmer.

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

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

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

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

(xvi) Glossary of terms used.

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

   (i) management to benchmark the security and control, practices of IT environments;
   (ii) users of IT services to be assured that adequate security and control exist, and
   (iii) auditors to substantiate their opinions on internal control and to advice on IT security and control matters.

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

(1) Business Objectives. To satisfy business objectives, information must conform to cer-
tain criteria the COBIT refers to as business requirements for information. The criteria are divided into seven distinct yet overlapping categories that map into the COSO objectives: effectiveness (relevant, pertinent, and timely), efficiency, confidentiality, integrity, availability, compliance with legal requirements and reliability.

(2) IT resources, while include people, application systems, technology, facilities, and data.

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

(c) **Firewall**: A firewall is a collection of components (computers, routers, and software) that mediate access between different security domains. All traffic between the security domains must pass through the firewall, regardless of the direction of the flow. Since the firewall serves as an access control point for traffic between security domains, they are ideally situated to inspect and block traffic and coordinate activities with network intrusion detection system (IDSs).

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

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

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

(d) **White Box Testing**

White box testing is a test case design method that uses the control structure of the procedural design to derive test cases. Test cases can be derived that

- guarantee that all independent paths within a module have been exercised at least once,
- exercise all logical decisions on their true and false sides,
- execute all loops at their boundaries and within their operational bounds, and
- exercise internal data structures to ensure their validity.

**The Nature of Software Defects**

Logic errors and incorrect assumptions are inversely proportional to the probability that a program path will be executed. General processing tends to be well understood while special case processing tends to be prone to errors.

We often believe that a logical path is not likely to be executed when it may be executed on a regular basis. Our unconscious assumptions about control flow and data lead to design errors that can only be detected by path testing. Typographical errors are random.

**Basis Path Testing**

This method enables the designer to derive a logical complexity measure of a procedural design and use it as a guide for defining a basis set of execution paths. Test cases that exercise the basis set are guaranteed to execute every statement in the program at least once during testing.

**Flow Graphs**

Flow graphs can be used to represent control flow in a program and can help in the derivation of the basis set. Each flow graph node represents one or more procedural statements. The edges between nodes represent flow of control. An edge must terminate at a node, even if the node does not represent any useful procedural statements. A region in a flow graph is an area bounded by edges and nodes. Each node that contains a condition is called a predicate node.

**Loop Testing**

This white box technique focuses exclusively on the validity of loop constructs. Four different classes of loops can be defined:

- Simple loops
- Nested loops
• Concatenated loops
• Unstructured loops

Other white box testing techniques include:
1. Condition testing which exercises the logical conditions in a program.
2. Data flow testing which selects test paths according to the locations of definitions and uses of variables in the program.