Q-1)
XYZ Ltd. is a leading company in FMCG sector and has a large number of coffee chains across India. The company uses ERP system for all its business operations and for recording sales at each outlet. The company has customized ERP, which is connected to a central server. 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, it is reliable and no unauthorized disclosure of the same is made. Further, it is also presumed that the virtual business organization is up and running all the time on 24×7 basis. However, in reality, the technology-enabled and technology-dependent organizations are more vulnerable to security threats in this highly connected world.
Read the above carefully and answer the following: *(5 × 4 = 20 Marks)*
(a) 'An ERP system is not only the integration of various organization processes; rather any system has to possess few key characteristics to qualify for a true ERP solution'. What are these characteristics?
(b) 'Access Control plays a key role in the implementation of information security policies'. Explain its detailed controls and objectives.
(c) Describe 'Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security' with respect to the Section 69B of Information Technology (Amendment) Act, 2008.
(d) Briefly explain the tasks that are to be performed during the post-implementation phase of an ERP package.

Q-2)
(a) A Company is offering a wide range of products and services to its customers. It relies heavily on its existing information system to provide up-to-date information. The company wishes to enhance its existing system. You being an information system auditor, suggest how the investigation of the present information system should be conducted so that it can be further improved upon. (6Marks)
(b) What should be the components of a good Security Policy? Explain in brief. (4 Marks)
(c) Discuss the set of major skills that is generally expected from an IS Auditor in your opinion? (4 Marks)

Q-3)
(a) What is Executive Information System? Briefly discuss its major characteristics. (6 Marks)
(b) What are the points that are required to be kept in mind by an IS Auditor while working with logical access control mechanisms? (6 Marks)
(c) Explain the advantages of continuous audit techniques in brief. (4 Marks)

Q-4)
(a) What are the major Risk management Strategies ? Explain in brief. (6 marks)
(b) ABC Company is committed to implement the data backup policy through proper planning. What are the major tips that should be followed by the company for the back up? (6 mark)
(c) Explain provisions for retention of Electronic Records ? (4 marks)

Q-5)
(a) Explain attributes of information ? (6 marks)
(b) Describe the contents of a disaster recovery and planning documents ? (6 marks)
(c) Explain Do phase with reference to ISMS ? (4 marks)

Q-6)

(a) Explain Role of following security officers : (6 marks)
- DSSO
- ITSO
- FMSO
- Line manager

(b) What is data privacy ? Explain the major techniques that are used to address privacy protection for IT system ? (6 marks)

(c) Explain characteristic of A good coded Program ? (4 marks)

7. Write short notes on any four of the following:
(a) Corrective Controls
(b) White Box Testing
(c) Delphi Technique for Risk Assessment
(d) HIPAA
(e) Phased Implementation (4 × 4 = 16 Marks)

1. (a) To qualify for a true ERP solution, a system has to possess the following characteristics :

♦ 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. This means that 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 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 it should 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) The detailed controls and objectives of access control are given as follows:

♦ Business requirement for access control: To control access to information;

♦ User access management: To prevent unauthorized access to information systems;

♦ User responsibilities: To prevent unauthorized user access;

♦ Network access control: To protect 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.

(c) [Section 69B] Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security:

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of sub- section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

(d) Major tasks that are to be performed during the post-implementation phase of an ERP package are given as follows:

♦ To develop the new job descriptions and organization structure to suit the post ERP scenario;

♦ To determine the skill gap between existing jobs and envisioned jobs;

- To assess training requirements, and create and implement a training plan;
- To develop and amend HR, financial and operational policies to suit the future ERP environment; and
- To develop a plan for workforce logistics adjustment.

ANS:
Q-3)

(a) Characteristic of EIS: -

- EIS is a CBIS that serves information to top managers
- Provides rapid access to both internal / external data
- It locates problem without need to learn query language
- Gives rapid access to timely information
- It provides extensive online usage like trend analysis, market conditions, etc
- DSS support can be easily given to EIS to support decision making.

(b) An IS auditor should keep the following points in mind while working with logical access control mechanisms.

- Reviewing the relevant documents relating to logical facilities and understanding the security risks faced by information processing system.
- Access paths into the system should be evaluated by the auditor to assess their sufficiency.
- Deficiencies must be identified and evaluated.
- By proper audit techniques, auditor must verify test controls over access paths to determine its effective functioning.
- He must verify whether the control objectives are achieved and must evaluate access control mechanism, analyze the test results, etc.
- The auditor should compare security policies and practices of other organizations with their organization and assess its adequacy.

(c) Some of the advantages of continuous audit techniques are as under: [IDT'S]

- Information to system staff on meeting of objectives: Continuous audit techniques provide information to systems staff by evaluating whether an application system meets the objectives of organization i.e., asset safeguarding; data integrity; etc.
- 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.
- Training for new users: Using the ITF, new users can submit their data to the application system, and obtain feedback on any mistakes they make through system's error reports.
- Surprise test capability: As evidences are to be collected from the system itself, the auditors can gather evidence without the presence of systems staff and the system users not being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.

Q-2)
(a)
The following areas should be studied in depth:

- Review historical aspects: A brief study of history of the organization is a starting point for an analysis of the present system. The system analyst should review what system changes have been occurred in the past and whether it was successful or not.
- Review data files maintained: The analyst should investigate the data files maintained by each department, where they are located, who uses them number of times they are used, etc. He should also review all on-line and off-line files maintained in the organization.
- 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 to accomplish a job. The analyst must analyze data-communications network in the present system to identify whether there is need to revise the network in new system or not.
- Review internal controls: A investigation is not complete until internal control is reviewed because it identifies weaknesses that should be removed from the new system.
- Analyze inputs: A detailed analysis of present inputs is important since they are basic source of data. Analyze should also be conducted to determine what is source input of present system. Further analyze whether output of one area is the input of other. Analyst must also understand the flow of input.
- Analyze outputs: The output should be scrutinized carefully by the system analysts to determine how well it meets the organization's needs. The analysts must understand what information is needed and why. Many times information obtained from reports are a carry-over from earlier days which have little or no relevance and therefore such reports should be eliminated.
- Model the existing physical system: All the important items in the existing system should be reviewed and analyzed and this process must be properly documented which allows a thorough understanding of numerous problems in the current system.
- Undertake overall analysis of present system: It is the final phase of analysis which includes thorough analysis of present work volume; user requirements; etc.

(b)
A good security policy should clearly state the following:

- Purpose and Scope of the Document,
- Security organization Structure,
- IT Operations management,
- IT Communications,
- Access control,
- Incident Handling,
- Physical and Environmental Security,
- Business Continuity Planning,
- System Development and Maintenance Controls,
- The Security Infrastructure,
- Security policy document maintenance and compliance requirements,
- Inventory and Classification of assets,
- Description of technologies and computing structure,
- Legal Compliances,
- Monitoring and Auditing Requirements.

(C) The set of skills that is generally expected from an IS auditor includes:

- Should possess sound knowledge of business operations, practices and compliance requirements,
- Knowledge of IT strategies, policy and procedure controls,
- Good knowledge of Professional Standards and Best practices of IT controls and security,
- An good understanding of information risks and controls,
- Ability to understand technical and manual controls relating to business continuity, and
- Should possess the requisite professional qualification and certifications.

Q-4)

(a) The strategies to manage risk fall into one or more of these four major categories:

1) Risk Avoidance: It means activity which possesses risk should not be done. E.g. not using internet over organization's system instead using a stand alone PC for internet usage.
2) Risk Mitigation / Reduction: It involves implementing controls to protect the system and to reduce the severity of the loss incase threat materialize. E.g. using an effective anti virus solution to protect against the risk of viruses and updating it on timely basis.
3) Risk Transfer: It involves another party to accept the risk i.e., sharing risk with partners or insurance coverage.
4) Risk Retention / Acceptance: All risks that are not identified or avoided or transferred are retained by default. These risks are called residual risk. Risk management aims to identify, select and implement the controls that are necessary to reduce residual risk to acceptable levels.

(b) Backup Tips

- Draw up a simple plan of responsibility during emergency i.e., who will do what in case of emergency.
- Be organized! Keep a record of what was backed up, when it was backed up and which backup media contains what data.
- Select the option to verify backup, the process will take a little longer but it's definitely worth the wait (i.e., verify which back up contains what data).
- Create a reference point to get proper updating of whether everything is working properly.
- There should be restriction on restoring data to owner or administrator only. This will help to reduce the risk of media being stolen.
- Create a step-by-step guideline (for eg: a flowchart) clearly outlining the sequence for the retrieval and restoring of data

(c)

Section 7 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 that it can 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.

Q-5)

(a) Attributes of information: -

- Decay: Information must be refreshed regularly otherwise its value will decay over time.
- Reliability: - Information should be obtained from the reliable sources. If wrong information is obtained and decision are taken based on that information then decision will eventually lead to failure. If information leads to correct decision then information is said to be reliable.
- Purpose: - Information must serve the purpose at the time of transaction else it is just a simple data i.e., it must help in problem solving, decision making, etc.
- Availability: - Timeliness of information is of very important. If information is not available in time then it is useless.
- Mode & Format: - Mode may be either visual or written. Format should be simple, relevant and important points should be highlighted but there should not be more data at a time.
- Transparency: - If information does not reveal directly what we want then it is not transparent & will hault our decision process. Thus, based on that information, if we are able to take decision directly then information is said to be transparent
- Adequacy: - Information available must be adequate to take decision. Further information must flow within organization.
- Completeness: - Information must be complete as possible because it helps to be in better position to take decision on the important matters

(b)

The disaster recovery and planning document may include the following areas:

- The conditions for activating the plans describing the process to be followed before activation.
- Emergency procedures, which describe the actions to be taken following an incident (ie., disaster) which jeopardizes business operations and/or human life which include effective liaison with appropriate public authorities e.g. police, fire, services and local government.
- Fallback procedures i.e., condition to be satisfied to move essential business activities to alternate temporary locations.
- Resumption procedures, which describe the actions to be taken to return to normal business operations.
- A schedule for testing and for maintaining the plan.
- The responsibilities of individuals describing who is responsible for executing the plan. Alternatives should be nominated as required.
- Contingency plan should be kept ready.
- Detailed description of the purpose and scope of the plan.
- List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
- List of phone numbers of employees in the event of an emergency.
- Emergency phone list of 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.
- Names of employees trained for emergency situation, first aid and life saving techniques.
  Details of airlines, hotels and transport arrangements

(c)

The Do phase:This phase consists of the following activities:

- Writing a risk treatment plan which describes budget within which controls should be implemented;
- Implementing the risk treatment plan;
- Implementing applicable security controls;
- Determining how to measure the effectiveness of controls;
- Carrying out awareness programs and training of employees; and Implementation of procedures for detecting and managing security incidents.

Q-6)

(a) Following is role of officers :

Divisional System Security Officer (DSSO): A System Security Officer (SSO) from each division will be appointed as a DSSO. The DSSO carries the same responsibilities as a SSO and in addition represent SSOs in their division to communicate requirements.

IT Security Officer (ITSO): The IT Security Officer reports to the ISMG on IT security matters. The ITSO is responsible for managing IT security programs.

Facilities Management Security Officer (FMSO): The Facilities Management Security Officer (FMSO) will report directly to Facilities Management on all security matters relating to facility. Their role is to ensure that controls are implemented and reviewed as necessary.

Line Managers: They have responsibility to take appropriate steps to ensure compliance with the aims and objectives of this policy

(b) Data privacy refers to the evolving relationship between technology and the privacy in sharing of data. Privacy problems exist wherever data are stored in digital form.

There are several technologies to address privacy protection of IT systems. These falls into two categories: communication and enforcement.

(i) Policy Communication

- P3P - The Platform for Privacy Preferences. It communicates privacy practices and compares individual preferences.

(ii) Policy Enforcement

- XACML - The extensible Access Control Markup Language together with its Privacy Profile is a standard which express its privacy policies in a machine-readable language, so that software can use to enforce the policy in enterprise.
- EPAL - The Enterprise Privacy Authorization Language is very similar to XACML, but is not yet a standard.
- WS-Privacy - "Web Service Privacy" communicates privacy policy in web services.

(c)

A good coded program should have the following characteristics:

- Reliability: It means program should be consistence over a period of time. However poor setting of parameters or hard coding of some data could result in the failure of a program after some time.
- Robustness: It refers to process of taking inputs and outputs in least likely situations.
- Accuracy: It refers to what program should do and should also take note of what it should not do.
- Efficiency: It means performance should not be affected due to increase in input values.
- Usability: It means user-friendly interface and easy-to-understand for any program.
- Readability: It refers to maintenance of the program even in the absence of the program developer

Q-7)

(a) Corrective Controls: Corrective controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. A Business Continuity Plan (BCP) is considered to be a significant corrective control. The main characteristics of the corrective controls are:

♦ Minimize the impact of the threat,
♦ Identify the cause of the problem,
♦ Remedy problems discovered by detective controls,
♦ Get feedback from preventive and detective controls,
♦ Correct error arising from a problem, and
♦ Modify the processing systems to minimize future occurrences of the problem.

Examples of Corrective Controls are: Contingency planning, Backup procedure, Rerun procedures, Treatment procedures for a disease, Change input value to an application system, and investigate budget variance and report violations.

(c) White Box Testing:

- White box testing uses an internal perspective of the system to design test cases based on internal structure.
- It requires programming skills to identify all paths through the software.
- The tester chooses test case inputs to exercise paths through the code and determines the appropriate outputs.
- It is applicable at the unit, integration and system levels of the testing process, it is typically applied to the unit.
- While, it normally tests paths within a unit, it can also test paths between units during integration, and between subsystems during a system level test.

(d) Delphi Technique for Risk Assessment:

- This technique was first used by the Rand Corporation for obtaining a consensus opinion.
- 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 by taking all the estimates as points on the graph.
- The median is drawn and this is the consensus opinion.

(d) HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) were enacted by the U.S. Congress in 1996. The major points of the act 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 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 in the US health care system. Security Rule issued under the Act is the key component of the Act.