PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

*Question No. **1** is compulsory.*

*Candidates are also required to answer any **five** questions*

*from the remaining **six** questions.*

Question 1

The XYZ Company is marketing several household consumable products. It has several branches throughout the country, which are well-connected with internet and intranet. Based on the reports and feedbacks, the company understands that the present system is not able to meet the requirements of its IS stakeholders. Hence, it wants to improve its IS performance and availability of services, to minimize its loss in terms of revenue loss, loss of reputation and to improve the customer satisfaction. It has felt the need for having reengineered business processes and implementing BCM for assessing the potential threats and managing the consequences. It wants to ensure to provide all users with a secure Information Processing environment. Further it wants to provide continuous assurance about the quality of data by employing continuous auditing technique SCARF. Hence, it engages a highly professional System Development Team to study the present system for designing and implementing a new system. The team follows and takes advantages of SDLC methods.

Read the above carefully and being a member of the team, answer the following:

(a) Briefly discuss the steps that involved in Business Process Design.

(b) Discuss the means for achieving Network Access Controls.

(c) Discuss:

(i) as to how an enterprise uses Training Process as a tool to initiate a culture of BCM in all the stakeholders and

(ii) what supports are needed for the development of a BCM culture.

(d) Discuss the types of information that can be collected by SCARF. ***(4 x 5 = 20 Marks)***

Answer

(a) Business Process Design involves a sequence of the steps described briefly below:

(i) Present Process Documentation: In this step, the present business process is analyzed and documented. The key deliverable of this step includes the well-defined short-comings of the present processes and the overall business requirements. This step includes the following activities:

- Understanding the business and the objectives for which it exists;
- Documenting the existing business processes; and
- Analysis of the documented processes.

(ii) Proposed Process Documentation: This step is to design the new process requirements for the system. The design is based on the new system requirements and the changes proposed. The activities include the following:

- Understanding of the business processes necessary to achieve the business objectives;
- Designing the new processes; and
- Documentation of the new process, preferably using CASE tools.

(iii) Implementation of New Process: This step is to implement largely the new as well as modified processes at the entity. The critical activities may include the following:

- Validating the new process;
- Implementing the new process; and
- Testing the new process.

(b) Network Access Control can be achieved through following means:

- **Policy on use of network services:** An enterprise wide policy applicable to internet service requirements aligned with the business need for using the Internet services is the first step. Selection of appropriate services and approval to access them should be part of this policy.
- **Enforced path:** Based on risk assessment, it is necessary to specify the exact path or route connecting the networks; e.g., internet access by employees will be routed through a firewall and proxy.
- **Segregation of networks:** Based on the sensitive information handling function; say a VPN connection between a branch office and the head-office, this network is to be isolated from the internet usage service.
- **Network connection and routing control:** The traffic between networks should be restricted, based on identification of source and authentication access policies implemented across the enterprise network facility.
- **Security of network services:** The techniques of authentication and authorization policy should be implemented across the organization's network.
- **Firewall:** Organizations connected to the Internet and Intranet often implements an electronic firewall to insulate their network from intrude. A Firewall is a system that enforces access control between two networks. To accomplish this, all traffic between the external network and the organization's Intranet must pass through the firewall. Only authorized traffic between the organization and the outside is allowed to pass through the firewall. The firewall must be immune to penetrate from both outside and inside the organization. In addition to insulating the organization's network from

external networks, firewalls can be used to insulate portions of the organization's Intranet from internal access also.

- **Encryption:** Encryption is the conversion of data into a secret code for storage in databases and transmission over networks. The sender uses an encryption algorithm and the original message called the clear text is converted into cipher text. This is decrypted at the receiving end. The encryption algorithm uses a key. The more bits in the key, the stronger are the encryption algorithms. Two general approaches are used for encryption viz. private key and public key encryption.
- **Call Back Devices:** It is based on the principle that the key to network security is to keep the intruder off the Intranet rather than imposing security measure after the criminal has connected to the intranet. The call- back device requires the user to enter a password and then the system breaks the connection. If the caller is authorized, the call back device dials the caller's number to establish a new connection. This limits access only from authorized terminals or telephone numbers and prevents an intruder masquerading as a legitimate user. This also helps to avoid the call forwarding and man-in-the middle attack.
- **Recording of Transaction Log**: An intruder may penetrate the system by trying different passwords and user ID combinations. All incoming and outgoing requests along with attempted access should be recorded in a transaction log. The log should record the user ID, the time of the access and the terminal location from where the request has been originated.

(c) (i) An enterprise with Business Continuity Management (BCM) uses training as a tool to initiate a culture of BCM in all the stakeholders by:

- Developing a BCM program more efficiently;
- Providing confidence in its stakeholders (especially staff and customers) in its ability to handle business disruptions;
- Increasing its resilience over time by ensuring BCM implications are considered in decisions at all levels; and
- Minimizing the likelihood and impact of disruptions.

(ii) Development of a BCM culture is supported by:

- Leadership from senior personnel in the enterprise;
- Assignment of responsibilities;
- Awareness raising;
- Skills training; and
- Exercising plans.

(d) Auditors might use System Control Audit Review File (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 must 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.

Question 2

(a) An important task for the auditor as a part of the preliminary evaluation is to gain a good understanding of the technology environment and related control issues. As the company auditor which aspects you will include in your consideration to understand the technology?

(6 Marks)

(b) What are the goals and metrics that can be used to measure specific success of a GRC program using COBIT 5? ***(6 Marks)***

(c) What are the benefits of mobile computing? ***(4 Marks)***

Answer

(a) An important task for the auditor as a part of his preliminary evaluation is to gain a good understanding of the technology environment and related control issues. This could include consideration of the following:

- Analysis of business processes and level of automation,
- Assessing the extent of dependence of the enterprise on Information Technology to carry on its businesses i.e. Role of IT in the success and survival of business,
- Understanding technology architecture which could be quite diverse such as a distributed architecture or a centralized architecture or a hybrid architecture,
- Studying network diagrams to understand physical and logical network connectivity,
- Understanding extended enterprise architecture wherein the organization systems connect seamlessly with other stakeholders such as vendors (SCM), customers (CRM), employees (ERM) and the government,
- Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems,
- And finally, Studying Information Technology policies, standards, guidelines and procedures.

(b) Specific success of a Governance, Risk and Compliance (GRC) program using COBIT 5 can be measured by using the following goals and metrics:

- The reduction of redundant controls and related time to execute (audit, test and remediate);
- The reduction in control failures in all key areas;
- The reduction of expenditure relating to legal, regulatory and review areas;
- Reduction in overall time required for audit for key business areas;
- Improvement through streamlining of processes and reduction in time through automation of control and compliance measures;
- Improvement in timely reporting of regular compliance issues and remediation measures; and
- Dashboard of overall compliance status and key issues to senior management on a real-time basis as required.

(c) Benefits of Mobile Computing include the following:

- It provides mobile workforce with remote access to work order details, such as work order location, contact information, required completion date, asset history relevant warranties/service contracts.
- It enables mobile sales personnel to update work order status in real-time, facilitating excellent communication.
- It facilitates access to corporate services and information at any time, from anywhere.

- It provides remote access to the corporate Knowledge base at the job location.
- It enables to improve management effectiveness by enhancing information quality, information flow, and ability to control a mobile workforce.

Question 3

(a) *In spite of having various controls as well as counter measures in place, cyber frauds are happening and increasing on a continuous basis. Discuss any six types of Cyber Frauds.*

(6 Marks)

(b) *Write the objectives of Information Technology Act, 2000.* ***(6 Marks)***

(c) *Describe any four ways in which system maintenance can be categorized.* ***(4 Marks)***

Answer

(a) Some of the major cyber frauds are as follows:

- **Monetary cyber frauds:** These include non-delivery of paid products purchased through online auction etc.
- **Phishing:** It is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public.
- **Network Scanning**: It is a process to identify active hosts of a system, for purpose of getting information about IP addresses etc.
- **Virus/Malicious Code**: As per Section 43 of the Information Technology Act, 2000, "Computer Virus" means any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource.
- **Spam:** E-mailing the same message to everyone on one or more Usenet News Group or LISTSERV lists is termed as Spam. Spam can be used to spread computer viruses, Trojan horses or other malicious software with malicious intention.
- **Website Compromise/Malware Propagation:** It includes website defacements. Hosting malware on websites in an unauthorized manner.
- **Cracking:** Crackers are hackers who practice hacking of computer systems with malicious intentions.
- **Eavesdropping:** It refers to the listening of the private voice or data transmissions, often using a wiretap.

- **E-mail Forgery:** Sending e-mail messages that look as if someone else sent it is termed as E-mail forgery.
- **E-mail Threats:** Sending a threatening message to try and get recipient to do something that would make it possible to defraud him is termed as E-mail threats.
- **Scavenging:** This is regarding gaining access to confidential information by searching corporate records.
- **Hacking:** It refers to unauthorized access and use of computer systems, usually by means of personal computer and a telecommunication network. Normally, hackers do not intend to cause any damage.
- **Data Diddling:** Changing data before, during, or after it is entered into the system in order to delete, alter, or add key system data is referred as Data Diddling.
- **Data Leakage:** It refers to the unauthorized copying of company data such as computer files.
- **Denial of Service (DoS) Attack:** It refers to an action or series of actions that prevents access to a software system by its intended/authorized users; causes the delay of its time-critical operations; or prevents any part of the system from functioning.
- **Internet Terrorism:** It refers to the using Internet to disrupt electronic commerce and to destroy company and individual communications.
- **Logic Time Bombs:** These are the program that lies idle until some specified circumstances or a particular time triggers it. Once triggered, the bomb sabotages the system by destroying programs, data or both.
- **Masquerading or Impersonation:** In this case, perpetrator gains access to the system by pretending to be an authorized user.
- **Password Cracking:** Intruder penetrates a system's defense, steals the file containing valid passwords, decrypts them and then uses them to gain access to system resources such as programs, files and data.
- **Piggybacking:** It refers to the tapping into a telecommunication line and latching on to a legitimate user before s/he logs into the system.
- **Round Down:** Computer rounds down all interest calculations to 2 decimal places. Remaining fraction is placed in account controlled by perpetrator.
- **Social Engineering Techniques:** In this case, perpetrator tricks an employee into giving out the information needed to get into the system.
- **Super Zapping:** It refers to the unauthorized use of special system programs to bypass regular system controls and performs illegal acts.
- **Trap Door:** In this technique, perpetrator enters in the system using a back door that bypasses normal system controls and perpetrates fraud.

(b) The objectives of the Information Technology Act, 2000 are 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

(c) System Maintenance can be categorized in the following ways:

- **Scheduled Maintenance:** Scheduled maintenance is anticipated and can be planned for operational continuity and avoidance of anticipated risks. For example, the implementation of a new inventory coding scheme can be planned in advance, security checks may be promulgated etc.
- **Rescue Maintenance:** Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate troubleshooting 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 during the executions. 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 the 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 with the 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.

Question 4

(a) *How does Information Technology Act, 2000 define the term Electronic Signature? State under what conditions any electronic Signature or Electronic Authentication technique shall be considered reliable as per Section 3A of Information Technology Act, 2000.* ***(6 Marks)***

(b) *Discuss the key management practices that are required for aligning IT strategy with Enterprise strategy.* ***(6 Marks)***

(c) *What are the important characteristics of Computer Based Information System (CBIS)?* ***(4 Marks)***

Answer

(a) As per Information Technology Act, 2000; the definition of Electronic Signature is as follows:

"**Electronic Signature**" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature.

[Section 3A (2) of IT Act, 2000] Electronic Signature

Any Electronic Signature or Electronic Authentication technique shall be considered reliable if-

(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and of no other person;

(b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(c) any alteration to the electronic signature made after affixing such signature is detectable;

(d) any alteration to the information made after its authentication by electronic signature is detectable; and

(e) it fulfills such other conditions which may be prescribed.

(b) The key management practices, which are required for aligning Information Technology (IT) Strategy with Enterprise Strategy are as below:

- **Understand enterprise direction:** Consider the current enterprise environment and business processes, as well as the enterprise strategy and future objectives. Consider also the external environment of the enterprise (industry drivers, relevant regulations, basis for competition.)
- **Assess the current environment, capabilities and performance:** Assess the performance of current internal business and IT capabilities and external IT services, and develop an understanding of the enterprise architecture in relation to IT. Identify issues currently being experienced and develop recommendations in areas that could benefit from improvement. Consider service provider differentiators and options and the financial impact and potential costs and benefits of using external services.
- **Define the target IT capabilities:** Define the target business and IT capabilities and required IT services. This should be based on the understanding of the enterprise environment and requirements; the assessment of the current business process and IT environment and issues; and consideration of reference standards, best practices and validated emerging technologies or innovation proposals.
- **Conduct a gap analysis:** Identify the gaps between the current and target environments and consider the alignment of assets with business outcomes to optimize investment in and utilization of the internal and external asset base. Consider the critical success factors to support strategy execution.
- **Define the strategic plan and road map:** Creates a strategic plan that defines, in co-operation with relevant stakeholders, how IT - related goals will contribute to the enterprise's strategic goals. This includes how IT will support IT-enabled investment programs, business processes, IT services and IT assets. IT should define the initiatives that will be required to close the gaps, the sourcing strategy, and the measurements to be used to monitor achievement of goals, then prioritize the initiatives and combine them in a high-level road map.
- **Communicate the IT strategy and direction:** Create awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy, through communication to appropriate stakeholders and users throughout the enterprise.

(c) The important characteristics of Computer Based Information Systems (CBIS) are as follows:

- All systems work for predetermined objectives and the system is designed and developed accordingly.

- In general, a system has several interrelated and interdependent subsystems or components. No subsystem can function in isolation; it depends on other subsystems for its inputs.
- 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'.
- The way a subsystem works with another subsystem is called Interaction. The different subsystems interact with each other to achieve the goal of the system.
- The work done by individual subsystems is integrated to achieve the central goal of the system. The goal of individual subsystem is of lower priority than the goal of the entire system.

Question 5

(a) State and explain any six key management practices for assessing and evaluating the System of Internal Controls in an enterprise. ***(6 Marks)***

(b) In the System Development phase, application programs re written, tested and documented. What are the characteristics required for a good coded application software?

(6 Marks)

(c) List any two advantages of each: [i] Private Cloud and [ii] Public Cloud. ***(4 Marks)***

Answer

(a) The key management practices for assessing and evaluating the system of internal controls in an enterprise are as follows:

- **Monitor Internal Controls:** Continuously monitor, benchmark and improve the IT control environment and control framework to meet organizational objectives.
- **Review Business Process Controls Effectiveness:** Review the operation of controls, including a review of monitoring and test evidence to ensure that controls within business processes operate effectively. It also includes activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing of controls, continuous controls monitoring, independent assessments, command and control centers, and network operations centers. This provides the business with the assurance of control effectiveness to meet requirements related to business, regulatory and social responsibilities.
- **Perform Control Self-assessments:** Encourage management and process owners to take positive ownership of control improvement through a continuing program of self- assessment to evaluate the completeness and effectiveness of management's control over processes, policies and contracts.

- **Identify and Report Control Deficiencies:** Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.
- **Ensure that assurance providers are independent and qualified:** Ensure that the entities performing assurance are independent from the function, groups or organizations in scope. The entities performing assurance should demonstrate an appropriate attitude and appearance, competence in the skills and knowledge necessary to perform assurance, and adherence to codes of ethics and professional standards.
- **Plan Assurance Initiatives:** Plan assurance initiatives based on enterprise objectives and conformance objectives, assurance objectives and strategic priorities, inherent risk resource constraints, and sufficient knowledge of the enterprise.
- **Scope assurance initiatives:** Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.
- **Execute assurance initiatives:** Execute the planned assurance initiative. Report on **identified** findings. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control system residual risks.

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

- **Reliability:** It refers to the consistency with which a program operates 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 applications' strength to uphold its operations in adverse situations by taking into account all 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 take 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 per unit cost with respect to relevant parameters and it should not be unduly affected with the increase in input values.
- **Usability:** It refers to a user-friendly interface and easy-to-understand internal/external documentation.
- **Readability:** It refers to the ease of maintenance of program even in the absence of the program developer.

(c) **(i)** The advantages of Private Clouds include the following:

- It improves average server utilization;

- It allows usage of low-cost servers and hardware while providing higher efficiencies; thus, reducing the costs that a greater number of servers would otherwise entail.
- It provides a high level of security and privacy to the user.
- It is small in size and controlled and maintained by the organization.

(ii) The advantages of Public Clouds are as follows:

- It is widely used in the development, deployment and management of enterprise applications, at affordable costs.
- It allows the organizations to deliver highly scalable and reliable applications rapidly and at more affordable costs.
- There is no need for establishing infrastructure for setting up and maintaining the cloud.
- Strict Service-Level Agreements (SLAs) are followed.
- There is no limit for the number of users.

Question 6

(a) What are the factors influencing an organization towards control and audit of computers and the impact of the information systems?

(b) A company uses a third party site for backup and recovery purposes after having a written contract. Being a security administrator, you must ensure that the contract covers the security issues. List down the issues to be covered. ***(6 Marks)***

(c) What is asynchronous attack? Explain Subversive threats to an Information System.

(4 Marks)

Answer

(a) Factors influencing an organization towards controls and audit of computers and the impact of the information systems audit function on organizations are as below:

- **Organisational Costs of Data Loss:** Data is a critical resource of an organisation for its present and future process and its ability to adapt and survive in a changing environment.
- **Cost of Incorrect Decision Making:** Management and operational controls taken by managers involve detection, investigations and correction of the processes. These high-level decisions require accurate data to make quality decision rules.
- **Costs of Computer Abuse:** Unauthorised access to computer systems, malwares, unauthorised physical access to computer facilities and unauthorised copies of

sensitive data can lead to destruction of assets (hardware, software, data, information etc.)

- **Value of Computer Hardware, Software and Personnel***:* These are critical resources of an organisation, which has a credible impact on its infrastructure and business competitiveness.
- **High Costs of Computer Error:** In a computerised enterprise environment where many critical business processes are performed, a data error during entry or process would cause great damage.
- **Maintenance of Privacy:** Today, data collected in a business process contains private information about an individual too. These data were also collected before computers but now, there is a fear that privacy has eroded beyond acceptable levels.
- **Controlled evolution of computer Use:** Use of Technology and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.

The impact of information Systems on an organization are as follows:

- Information Systems play a vital role in an enterprise collaboration and management and strategic success of businesses that must operate in an inter-networked global environment and facilitate E-business and E-commerce operations.
- With the help of information systems; enterprises and individuals can use computers to collect, store, process, analyse, and distribute information.
- Three basics activities of an Information System – Input, Processing and Output helps enterprise in making decisions, control operations, analyse problems and create new products or services as an output that helps management in taking important decisions to carry out the business successfully.

(b) If a third-party site is to be used for backup and recovery purposes after having a written contract, security administrators must ensure that a contract covers issues such as -

- 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
- what controls will be in place and working at the off-site facility.

(c) **Asynchronous Attacks:** They occur in many environments where data can be moved asynchronously across telecommunication lines. Numerous transmissions must wait for the clearance of the line before data being transmitted. Data that is waiting to be transmitted are liable to unauthorized access called Asynchronous Attack. These attacks are hard to detect because they are usually very small pin like insertions.

Subversive Threats: An intruder attempts to violate the integrity of some components in the sub-system. Subversive attacks can provide intruders with important information about messages being transmitted and the intruder can manipulate these messages in many ways. An intruder attempts to violate the integrity of some components in the sub-system by:

- **Invasive tap:** By installing it on communication line, s/he may read and modify data.
- **Inductive tap:** It monitors electromagnetic transmissions and allows the data to be read only.

Question 7

*Write short notes on any **four** of the following:*

(a) Benefits of Expert System

(b) Inherent limitations of IS Audit

(c) Advantages of BYOD

(d) Role of IS Auditor in Physical Access Control

(e) Limitations of MIS ***(4 x 4 = 16 Marks)***

Answer

(a) The key benefits of Expert Systems are as follows:

- Expert Systems preserve knowledge that might be lost through retirement, resignation or death of an acknowledged company expert.
- Expert Systems put information into an active-form so it can be summoned almost as a real-life expert might be summoned.
- Expert Systems assist novices in thinking the way experienced professional do.
- Expert Systems are not subjected to such human fallings as fatigue, being too busy, or being emotional.
- Expert Systems can be effectively used as a strategic tool in the areas of marketing products, cutting costs and improving products.

(b) Inherent Limitations of Information Systems (IS) Audit are as follows:

- The nature of financial reporting;
- The nature of audit procedures;

- The need for the audit to be conducted within a reasonable period of time and at a reasonable cost.
- The matter of difficulty, time, or cost involved is not in itself a valid basis for the auditor to omit an audit procedure for which there is no alternative or to be satisfied with audit evidence that is less than persuasive.
- Fraud, particularly fraud involving senior management or collusion.
- The existence and completeness of related party relationships and transactions.
- The occurrence of non-compliance with laws and regulations.
- Future events or conditions that may cause an entity to cease to continue as a going concern.

(c) Advantages of Bring Your Own Device (BYOD) are as follows:

- **Happy Employees:** Employees love to use their own devices when at work. This also reduces the number of devices an employee must carry; otherwise he would be carrying his personal as well as organization provided devices.
- **Lower IT budgets:** Could involve financial savings to the organization since employees would be using the devices they already possess thus reducing the outlay of the organization in providing devices to employees.
- **IT reduces support requirement:** IT department does not have to provide end user support and maintenance for all these devices resulting in cost savings.
- **Early adoption of new Technologies:** Employees are generally proactive in adoption of new technologies that result in enhanced productivity of employees leading to overall growth of business.
- **Increased employee efficiency:** The efficiency of employees is more when the employee works on his/her own device. In an organization provided devices, employees have to learn and there is a learning curve involved in it.

(d) Auditing physical access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls. This involves the following:

- **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 exposures there from.
- **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.

- **Review of Documents:** It requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams.

(e) Major limitations of Management Information Systems(MIS) are as follows:

- The quality of the outputs of MIS is basically governed by the quality of input and processes.
- MIS is not a substitute for effective management, which means that it cannot replace managerial judgment in making decisions in 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 time, especially in fast changing and complex environment.
- MIS cannot provide tailor-made information packages suitable for every type of decision made by executives.
- MIS considers mainly quantitative factors thus it ignores the non-quantitative factors like morale and attitude of members of organization, which have an important bearing on the decision-making process of executives or senior management.
- MIS is less useful for making non-programmed decisions. Such types of decisions are not of the routine type and thus require information, which may not be available from existing MIS to executives.
- The effectiveness of MIS is reduced in enterprises, where the culture of hoarding information and not sharing with other holds.
- MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.