

PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

Multiple Choice Questions

Questions No.(s) 1 to 5 are based on Case Scenario

ABC is a Domestic Airlines in India having its Reservation System that runs in a real-time environment maintaining their records in electronic form so that it becomes usable for subsequent reference. The details of electronic records are also maintained to facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic records.

The ABC Airlines has well implemented COBIT 5 business framework for the governance and management of enterprise Information Technology. The nature of transactions being online, cyber security is a must. To address such security issues like Confidentiality, Integrity and Availability; ABC has documented its Information Security controls and activities in a document referred as Information Security Policy. Accordingly; the control procedures, secure system and secure procedure are well implemented in the company.

Later, it was brought in notice of Top Management of ABC Airlines that there have been various computing resources in the System that are essential for performing certain operations in ABC Airlines, however these resources lay underutilized for most of the time. For its fair audit; ABC Airlines hires an IS Auditor, Mr. A who is expected to be competent with regards to standards, practices and organizational processes world-wide. Mr. A along with his team members prepared a checklist to investigate and focus on the areas like – Optimum utilisation of computing resources, proper documentation, record maintenance, log files, data backup procedures etc.

Based on the above scenario, answer the following questions:

1. To make use of non-utilized computing power of various resources in an effective manner, it was decided by top management of ABC Airlines that computing power of underutilized resources may be shared with needy organizations. Which technology is Top Management referring to?
 - (a) Cloud Computing
 - (b) Web 3.0
 - (c) Green Computing
 - (d) Grid Computing
2. ABC Airlines prepared an Information Security Policy that will include the following except _____.
 - (a) Definition of Information Security

- (b) Reasons for information security importance
 - (c) Specifications of Technologies and solutions
 - (d) Definition of all relevant information security responsibilities
3. During the audit, Mr. A refused to conduct audit of the electronic records stating that all the records must be provided to him in physical format. Can ABC Airlines defend its stand of maintaining electronic records and providing the same to Mr. A for the audit purpose?
- (a) No, the maintenance of the physical records is required to be maintained by ABC Airlines.
 - (b) Yes, under Section 7A of IT Act that is based on Audit of Documents etc. maintained in electronic form.
 - (c) Yes, under Section 7 of IT Act that is based on Retention of Electronic Records.
 - (d) Yes, under Section 7 of IT Act that is based on Audit of Documents etc. maintained in electronic form.
4. Mr. A made many recommendations in his report post audit. He recommended that though till date, there has not been any case of interruption so far. However, ABC Ltd. should develop a practical logistical plan known as Business Continuity Plan (BCP) to take care of recovery and restoration partially/fully in case of occurrence of any disaster. Which of the following will not form part of Business Continuity Plan Methodology?
- (a) Defining recovery requirements from the perspective of business functions.
 - (b) Disaster prevention and impact minimization as well as orderly recovery.
 - (c) Documenting the impact of an extended loss to key business functions.
 - (d) Clear distinction and non-integration between Systems Development process and business planning to keep plan viable over time.
5. The Airlines has well implemented COBIT 5 business framework for the governance and management of enterprise Information Technology. Choose the incorrect statement related to COBIT 5:
- (a) The COBIT 5 framework integrates the two disciplines - Governance and Management that encompass various activities, organizational structures and serve same purpose.
 - (b) COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT.
 - (c) COBIT 5 provides all the required processes and other enablers to support business value creation using IT.
 - (d) COBIT 5 framework can be implemented in all sizes of enterprises, whether commercial, not-for-profit or in the public sector.

6. Which of the following statement is incorrect w.r.t Decision Support Systems (DSS)?
- (a) A DSS includes one or more databases that contain both routine and non-routine data from both internal and external sources.
 - (b) The DSS is intended to make decisions for managers in solving semi-structured and unstructured problems in their own.
 - (c) The Model Base is the brain of the DSS as it performs data manipulations and computations with the data provided to it by the user and the database.
 - (d) DSS is an interactive software-based system intended to help decision makers to compile useful information from raw data, documents and personal knowledge.
7. During System Acquisition phase in SDLC, the top management of an enterprise should establish acquisition standards that address the security and reliability issues as per current state-of-the art development standards. Which of the following is not to be considered while focussing on acquisition standards?
- (a) Ensuring security, reliability, and functionality already built into a product.
 - (b) Ensuring managers' complete reviews of appropriate vendor, contract and licensing.
 - (c) Request for proposals soliciting bids when acquiring off-the-shelf or third-party software.
 - (d) To select the programming techniques and languages to be used for systems development.
8. Which of the following statement is incorrect w.r.t Auditing of Information Systems?
- (a) Audit trail attempts to ensure that a chronological record of all events that occurred in an organization are maintained.
 - (b) One of the audit techniques named Integrated Test Facility (ITF) is used to trap exceptions whenever the application system uses a DBMS.
 - (c) The Boundary Controls under Application Controls maintain the chronology of events that occur when a user attempts to gain access to and employ systems resources.
 - (d) While auditing, an auditor must check that risk assessment procedure adequately covers periodic and timely assessment of all assets and physical access threats.

DESCRIPTIVE QUESTIONS

Chapter 1: Concepts of Governance and Management of Information Systems

9. Under COBIT 5, the process "Monitor, Evaluate and Assess the System of Internal Control (MEA)" provides guidance on evaluating and assessing internal controls implemented in an enterprise. Discuss the key management practices for assessing and evaluating the system of internal controls.

10. Explain the concepts of Threat and Vulnerability.

Chapter 2: Information System Concepts

11. Discuss various characteristics of an effective Management Information Systems (MIS) through which it provides reports to management that can help them in making effective, structured types as applicable to decisions of day-to-day operations.
12. In today's dynamic business environment; timeliness, accurate, meaningful and action oriented information enhances an organization's ability and capacity to deal with and develop in mission, competition, performance and change. Irrespective of the type of business, Information remains the key vital asset of any business at all levels. Comment.

Chapter 3: Protection of Information Systems

13. Discuss various Application and Monitoring System Access Controls to be implemented in an Information System.
14. An Auditor Mr. A is a member of the system development team and suggested certain Boundary controls that needed to be put in place in Information Systems of an organization to ensure authentication to access computing resources. Discuss various techniques that can be used for Boundary Controls.

Chapter 4: Business Continuity Planning and Disaster Recovery Planning

15. Identify the document which acts as a guide to make a systematic approach for disaster recovery and to bring about awareness among the persons in scope about the business continuity aspects in an enterprise. Also, discuss the objective of such document in an enterprise.
16. Discuss different types of plans that need to be designed for an enterprise so that these can be appropriately implemented in case, any disaster occurs.

Chapter 5: Acquisition, Development and Implementation of Information Systems

17. As a part of SDLC team; Mr. A, an analyst must determine the needs and requirements based on which the proposed system is to be developed. Discuss various fact-finding techniques which he can adopt to accomplish his objective.
18. At the end of the Design phase of SDLC, an organization gets a reasonable idea of the types of hardware, software and services it needs to acquire for the system being developed. Discuss the major considerations that are valid for acquisition of both hardware and software from a vendor.

Chapter 6: Auditing of Information Systems

19. Discuss the major objectives that are achieved through Information Systems Auditing.

20. To establish whether Application Security controls are operating effectively or not; Layered approach is used wherein the audit is carried out at each layer of an application. Discuss various aspects that need to be considered regarding Application Security layers.

Chapter 7: Information Technology Regulatory Issues

21. Mr. A and Mr. X are employees of the company ABC Ltd. and do not share congenial relations with each other. In the absence of Mr. X, Mr. A manages to access Mr. X's official computer system and intentionally introduces computer virus into his computer through a contaminated USB drive. Later, Mr. X realises that his computer system has been infected with computer virus due to which critical information residing in his system has got destroyed. In the given situation, examine in the light of the IT Act 2000, whether Mr. A is liable for causing damage to Mr. X's computer system or not?
22. List down the various norms recommended by SEBI for the selection of Auditors.

Chapter 8: Emerging Technologies

23. As a Software as a Service (SaaS) provider under Cloud Computing, enlist the services that you may provide to your client.
24. Though Cloud Computing provides the facility to access shared resources and common infrastructure offering services to demand over the network, there are major issues related to its implementation. Discuss them.

SUGGESTED ANSWERS/HINTS

MULTIPLE CHOICE ANSWERS

1. (d) Grid Computing
2. (c) Specifications of Technologies and solutions
3. (b) Yes, under Section 7A of IT Act that is based on Audit of Documents etc. maintained in electronic form.
4. (d) Clear distinction and non-integration between Systems Development process and business planning to keep plan viable over time.
5. (a) The COBIT 5 framework integrates the two disciplines - Governance and Management that encompass various activities, organizational structures and serve same purpose.
6. (b) The DSS is intended to make decisions for managers in solving semi-structured and unstructured problems in their own.

7. (d) To select the programming techniques and languages to be used for system development.
8. (b) One of the audit techniques named Integrated Test Facility (ITF) is used to trap exceptions whenever the application system uses a DBMS.

DESCRIPTIVE ANSWERS

9. The key management practices for assessing and evaluating the system of internal controls in an enterprise are given 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.

10. **Threat:** Any entity, circumstance, or event with the potential to harm the software system or component through its unauthorized access, destruction, modification, and/or denial of service is called a Threat. A threat is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organization.

Threat has capability to attack on a system with intent to harm. Every system has a data, which is considered as a fuel to drive a system, data is nothing but assets. Assets and threats are closely correlated. A threat cannot exist without a target asset. Threats are typically prevented by applying some sort of protection to assets.

Vulnerability: Vulnerability is the weakness in the system safeguards that exposes the system to threats. It may be a weakness in information system/s, cryptographic system (security systems), or other components (e.g. system security procedures, hardware design, internal controls) that could be exploited by a threat. Vulnerabilities potentially “allow” a threat to harm or exploit the system. For example, vulnerability could be a poor access control method allowing dishonest employees (the threat) to exploit the system to adjust their own records.

Simply, Vulnerability can be referred as the weakness of the software, which can be exploited by the attackers. Vulnerabilities can originate from flaws on the software’s design, defects in its implementation, or problems in its operation. Some experts also define ‘vulnerability’ as opening doors for attackers. Normally, vulnerability is a state in a computing system (or set of systems), which must have at least one condition, out of the following:

- ‘Allows an attacker to execute commands as another user’ or
- ‘Allows an attacker to access data that is contrary to the specified access restrictions for that data’ or
- ‘Allows an attacker to pose as another entity’ or
- ‘Allows an attacker to conduct a denial of service’.

11. Major characteristic of an effective MIS are given as follows:

- **Management Oriented** – It means that efforts for the development of the information system should start from an appraisal of management needs and overall business objectives. Such a system is not necessarily for top management only but may also meet the information requirements of middle level or operating levels of management as well.

- **Management Directed** – Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts. For system's effectiveness, it is necessary for management to devote their sufficient time not only at the stage of designing the system but for its review as well to ensure that the implemented system meets the specifications of the designed system.
- **Integrated** – The best approach for developing information systems is the integrated approach as all the functional and operational information sub-systems are tied together into one entity. An integrated Information system has the capability of generating more meaningful information to management as it takes a comprehensive view or a complete look at the interlocking sub-systems that operate within a company.
- **Common Data Flows** – It means the use of common input, processing and output procedures and media whenever required. Data is captured by the system analysts only once and as close to its original source as possible. Afterwards, they try to utilize a minimum of data processing procedures and sub-systems to process the data and strive to minimize the number of output documents and reports produced by the system. This eliminates duplication in data collections, simplifies operations and produces an efficient information system.
- **Heavy Planning Element** – An MIS usually takes one to three years and sometimes even longer period to get established firmly within a company. Therefore, a MIS designer must be present in MIS development and should consider future enterprise objectives and requirements of information as per the organization structure of the enterprise as per requirements.
- **Sub System Concept** – Even though the information system is viewed as a single entity, it must be broken down into digestible sub-systems, which can be implemented one at a time by developing a phased plan. The breaking down of MIS into meaningful sub-systems sets the stage for this phasing plan.
- **Common Database** – Database is the mortar that holds the functional systems together. It is defined as a "super-file", which consolidates and integrates data records formerly stored in many separate data files. The organization of a database allows it to be accessed by several information sub-systems and thus, eliminates the necessity of duplication in data storage, updating, deletion and protection.
- **Computerized** - Though MIS can be implemented without using a computer; the use of computers increases the effectiveness of the system. In fact, its use equips the system to handle a wide variety of applications by providing their information requirements quickly. Other necessary attributes of the computer to MIS are accuracy and consistency in processing data and reduction in clerical staff. These attributes make computer a prime requirement in management information system.

12. The information can be categorized on the basis of its requirement by the Top, Middle and Lower level management, that are as follows:
- **Top level management** strives for the information that can help them in major policy decisions such as establishment of new plant, launching of new product etc. In other words, the top management requires strategic information that helps them in making strategy of an enterprise in terms of scope of products, targets of products i.e. customers, competition with market i.e. price, quality, long term planning etc. The information about the customers buying habits such as what combination of products and type of products they are likely to purchase together helps top managers to decide the launching of new products. Such information can help top management of company to decide to work on new products as well as the location where it has to be launched for maximum profit and sale which is one of the objectives and goals of the top management.
 - **Middle management** requires tactical information that helps in implementing decisions taken by the top management. For example - information of customers likely to purchase certain product in a particular location can help sales managers to fulfill their sales target efficiently. Tactical information is used for short term planning whereas strategy information is used for long term planning. For example, the offers of companies during festive seasons are a short term planning, which is done by having information about the customers buying capacity in that location.
 - **The lower management** requires operational information, which is required in day-to-day activities. The operational information mainly comprises of information about stock on hand, information about customer order pending, information about bill payable by customer etc. These are essential for smooth running of the daily activities of a business at primary level. For example, if a regular customer demands for a product other than the daily purchase then this information is important for salesman because it will help him in providing better service.
13. Various Application and Monitoring System Access Controls to be implemented in an Information System are as follows:
- **Information access restriction:** The access to information is prevented by application specific menu interfaces, which limit access to system function. A user is allowed to access only to those items, s/he is authorized to access. Controls are implemented on the access rights of users, for example - Read, Write, Delete, and Execute. This also ensures that sensitive output is sent only to authorized terminals and locations.
 - **Sensitive system isolation:** Based on the critical constitution of a system in an enterprise, it may even be necessary to run the system in an isolated environment. Monitoring system access and use is a detective control, to check if preventive

controls discussed so far are working. If not, this control will detect and report any unauthorized activities.

- **Event logging:** In Computer systems, it is easy and viable to maintain extensive logs for all types of events. It is necessary to review if logging is enabled and the logs are archived properly. 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.
 - **Monitor system use:** Based on the risk assessment, a constant monitoring of some critical systems is essential. Define the details of types of accesses, operations, events and alerts that will be monitored. The extent of detail and the frequency of the review would be based on criticality of operation and risk factors. The log files are to be reviewed periodically and attention should be given to any gaps in these logs.
 - **Clock synchronization:** Event logs maintained across an enterprise network plays a significant role in correlating an event and generating report on it. Hence, the need for synchronizing clock time across the network as per a standard time is mandatory.
14. Major Boundary Control techniques to be implemented in Information System are as follows:
- **Cryptography:** It deals with programs for transforming data into cipher text 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. 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, hashing of passwords and number of entry attempts.
 - **Personal Identification Numbers (PIN):** PIN is similar to a password assigned to a user by an institution a random number stored in its database independent to a user identification details, or a customer selected number. Hence, a PIN may be 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 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.

15. **Business Continuity Management (BCM) Policy** is a document which acts as a guide to make a systematic approach for disaster recovery and to bring about awareness among the persons in scope about the business continuity aspects in an enterprise.

The objective of the BCM policy is to provide a structure through which:

- Critical services and activities undertaken by the enterprise operation for the customer will be identified.
- Plans will be developed to ensure continuity of key service delivery following a business disruption, which may arise from the loss of facilities, personnel, IT and/or communication or failure within the supply and support chains.
- Invocation of incident management and business continuity plans can be managed.
- Incident Management Plans and Business Continuity Plans are subject to ongoing testing, revision and updation as required.
- Planning and management responsibility are assigned to a member of the relevant senior management team.

16. Various types of plans that need to be designed for an enterprise so that these can be appropriately implemented in case any disaster occurs include the following:

- **Emergency Plan:** The emergency plan specifies the actions to be undertaken immediately when a disaster occurs. Management must identify those situations that require the plan to be invoked e.g., major fire, major structural damage, and terrorist attack. The actions to be initiated can vary depending on the nature of the disaster that occurs. If an enterprise undertakes a comprehensive security review program, the threat identification and exposure analysis phases involve identifying those situations that require the emergency plan to be invoked. When the situations that evoke the plan have been identified, four aspects of the emergency plan must be articulated.
 - ◆ First, the plan must show 'who is to be notified immediately when the disaster occurs - management, police, fire department, medicos, and so on'.
 - ◆ Second, the plan must show actions to be undertaken, such as shutdown of equipment, removal of files, and termination of power.

- ◆ Third, any evacuation procedures required must be specified.
- ◆ Fourth, return procedures (e.g., conditions that must be met before the site is considered safe) must be designated. In all cases, the personnel responsible for the actions must be identified, and the protocols to be followed must be specified clearly.
- **Back-up Plan:** The Backup plan specifies the type of backup to be kept, frequency with which backup is to be undertaken, procedures for making backup, location of backup resources, site where these resources can be assembled and operations restarted, personnel who are responsible for gathering backup resources and restarting operations, priorities to be assigned to recovering the various systems, and a time frame for recovery of each system.
 - ◆ For some resources, the procedures specified in the backup plan might be straightforward. For example, microcomputer users might be admonished to make backup copies of critical files and store them off site.
 - ◆ In other cases, the procedures specified in the backup plan could be complex and somewhat uncertain. For example, it might be difficult to specify; exactly how an organization's mainframe facility will be recovered in the event of a fire.
 - ◆ The backup plan needs continuous updating as changes occur. For example, as personnel with key responsibilities in executing the plan leave the organization, the plan must be modified accordingly. Indeed, it is prudent to have more than one person knowledgeable in a backup task in case someone is injured when a disaster occurs. Similarly, lists of hardware and software must be updated to reflect acquisitions and disposals.
- **Recovery Plan:** Recovery plan should identify a recovery committee that will be responsible for working out the specifics 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. Again, the problem is that they will be required to undertake unfamiliar tasks. Periodically, they must review and practice executing their responsibilities so they are prepared should a disaster occur. If committee members leave the organization, new members must be appointed immediately and briefed about their responsibilities.
- **Test Plan:** The final component of a disaster recovery plan is a test plan. The purpose of the test plan is to identify deficiencies in the emergency, backup or recovery plans or in the preparedness of an organization and its personnel for facing a disaster. It must enable a range of disasters to be simulated and specify the criteria by which the emergency, backup, and recovery plans can be deemed satisfactory. Periodically, test plans must be invoked. Unfortunately, top managers are often unwilling to carry

out a test because daily operations are disrupted. They also fear a real disaster could arise as a result of the test procedures.

17. Various fact-finding techniques/tools that can be used by the system analyst for determining the needs and requirements of a proposed system are as below:
 - **Documents:** Document means manuals, input forms, output forms, diagrams of how the current system works, organization charts showing hierarchy of users and manager responsibilities, job descriptions for the people, who work with the current system, procedure manuals, program codes for the applications associated with the current system, etc. Documents are a very good source of information about user needs and the current system.
 - **Questionnaires:** Users and managers are asked to complete questionnaire about the information systems when the traditional system development approach is chosen. The main strength of questionnaires is that a large amount of data can be collected through a variety of users quickly. Also, if the questionnaire is skilfully drafted, responses can be analysed rapidly with the help of a computer.
 - **Interviews:** Users and managers may also be interviewed to extract information in depth. The data gathered through interviews often provide system developers with a larger picture of the problems and opportunities. Interviews also give analyst the opportunity to observe and record first-hand user reaction and to probe for further information.
 - **Observation:** In general, observation plays a central role in requirement analysis. Only by observing how users react to prototypes of a new system, the system can be successfully developed.
18. At the end of the Design phase of SDLC, the organization gets a reasonable idea of the types of hardware, software and services, it needs for the system being developed. Acquiring the appropriate hardware and software is critical for the success of the whole project. The following considerations are valid for both acquisition of hardware and software from a vendor:
 - **Vendor Selection:** This step is a critical step for success of process of acquisition of systems. It is necessary to remember that vendor selection is to be done prior to sending RFP (Request For Proposal). The result of this process is that 'RFP are sent only to selected vendors'. For vendor selection, following things are kept in mind including the background and location advantage of the vendor, the financial stability of vendor, the market feedback of vendor performance, in terms of price, services etc.
 - **Geographical Location of Vendor:** The issue to look for whether the vendor has local support persons. Otherwise, the proposals submitted by vendor not as per RFP requirements need to reject with no further discussion on such rejected proposals.

This stage may be referred to as 'technical validation', that is to check the proposals submitted by vendors, are technically complying with RFP requirements.

- **Presentation by Selected Vendors:** All vendors, whose proposals are accepted after "technical validation", can make presentation to the System Acquisition Team. The team evaluates the vendor's proposals by using techniques.
 - **Evaluation of Users Feedback:** The best way to understand the vendor systems is to analyse the feedback from present users. Present users can provide valuable feedback on system, operations, problems, vendor response to support calls.
19. Through Information Systems Auditing, organizations achieve following major objectives that are as follows:
- **Asset Safeguarding Objectives:** The information system assets (hardware, software, data information etc.) must be protected by a system of internal controls from unauthorised access.
 - **Data Integrity Objectives:** It is a fundamental attribute of IS Auditing. The importance to maintain integrity of data of an organisation requires all the time. It is also important from the business perspective of the decision maker, competition and the market environment.
 - **System Effectiveness Objectives:** Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet business and user requirements.
 - **System Efficiency Objectives:** To optimize the use of various information system resources (machine time, peripherals, system software and labour) along with the impact on its computing environment.
20. Application Security Controls are implemented in Layered manner which are divided into Operational Layer, Tactical Layer and Strategic Layer.
- (i) **Operational Layer:** The operational layer audit issues include:
- **User Accounts and Access Rights:** This includes defining unique user accounts and providing them access rights appropriate to their roles and responsibilities. Auditor needs to always ensure the use of unique user IDs, and these need to be traceable to individual for whom created. In case, guest IDs are used then test of same should also be there. Likewise, vendor accounts and third-party accounts should be reviewed.
 - **Password Controls:** In general, password strength, password minimum length, password age, password non-repetition and automated lockout after three attempts should be set as a minimum. Auditor needs to check whether there are applications where password controls are weak. In case such instances are found, then auditor may look for compensating controls against such issues.

- **Segregation of Duties:** As frauds due to collusions / lack of segregations increase across the world, importance of the Segregation of Duties also increases. Segregation of duties is a basic internal control that prevents or detects errors and irregularities by assigning to separate individuals' responsibility for initiating and recording transactions and custody of assets to separate individuals.
- (ii) **Tactical Layer:** At the tactical layer, security administration is put in place. This includes:
- Timely updates to user profiles, like creating/deleting and changing of user accounts. Auditor needs to check that any change to user rights is a formal process including approval from manager of the employee.
 - **IT Risk Management:** This function includes the following activities:
 - Assessing risk over key application controls;
 - Conducting a regular security awareness programme on application user;
 - Enabling application users to perform a self-assessment/complete compliance checklist questionnaire to gauge the users' understanding about application security;
 - Reviewing application patches before deployment and regularly monitoring critical application logs;
 - Monitoring peripheral security in terms of updating antivirus software;An auditor should understand the risk associated with each application and obtain a report on periodic risk assessment on the application or self-assessment/ compliance reports on the application.
 - **Interface Security:** This relates to application interfaced with another application in an organization. An auditor needs to understand that data flow to and from the application. Security of the interfaced data is also important, especially when unencrypted methods of transmission are used for data transmission.
 - **Audit Logging and Monitoring:** Regular monitoring the audit logs is required. The same is not possible for all transactions, so must be done on an exception reporting basis.
- (iii) **Strategic Layer:** At this layer, the top management takes action, in form of drawing up security policy, security training, security guideline and reporting. A comprehensive information security programme fully supported by top management and communicated well to the organization is of paramount importance to succeed in information security. The security policy should be supported and supplemented by

detailed standards and guidelines. These guidelines shall be used at the appropriate level of security at the application, database and operating system layers.

21. The situation pertains to Section 43 of IT Act, 2000 which is stated below -

[Section 43] Penalty and Compensation for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network, -

- (a) accesses or secures access to such computer, computer system or computer network or computer resource;
- (b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
- (c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
- (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
- (e) disrupts or causes disruption of any computer, computer system or computer network;
- (f) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;
- (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;
- (h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;
- (i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
- (j) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage,

he shall be liable to pay damages by way of compensation to the person so affected.

As per the Section 43(c) and 43(j) of IT Act, 2000; Mr. A will be held liable as he intentionally caused damage to computer system of Mr. X.

22. As per SEBI, various norms for selection of Auditors are as follows:

- Auditor must have minimum 3 years of experience in IT audit of Securities Industry participants e.g. stock exchanges, clearing houses, depositories etc. The audit experience should have covered all the Major Areas mentioned under SEBI's Audit Terms of Reference (TOR).
- The Auditor must have experience in/direct access to experienced resources in the areas covered under TOR. It is recommended that resources employed shall have relevant industry recognized certifications e.g. CISA (Certified Information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as (ISC).
- The Auditor should have IT audit/governance frameworks and processes conforming to industry leading practices like CoBIT.
- The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the Exchange/Depository. It should not have been engaged over the last three years in any consulting engagement with any departments/units of the entity being audited.
- The Auditor may not have any cases pending against its previous auditees, which fall under SEBI's jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.

23. The services provided by Software as a Service (SaaS) are as follows:

- (a) **Business Services:** SaaS providers provide a variety of business services to startup companies that includes ERP, CRM, billing, sales, and human resources.
- (b) **Social Networks:** Since the number of users of the social networking sites is increasing exponentially, cloud computing is the perfect match for handling the variable load.
- (c) **Document Management:** Most of the SaaS providers provide services to create, manage, and track electronic documents as most of the enterprises extensively use electronic documents.
- (d) **Mail Services:** To handle the unpredictable number of users and the load on e-mail services, most of the email providers offer their services as SaaS services.

24. Some of the well-identified implementation issues of Cloud Computing are as follows:

- **Threshold Policy:** In order to test if the program works, develops, or improves and implements; a threshold policy is of immense importance in a pilot study before moving the program to the production environment. This involves the checking how the policy enables to detect sudden increases in the demand and results in the

creation of additional instances to fill in the demand. Moreover, to determine how unused resources are to be de-allocated and turned over to other work needs to work out in the context. That is working out thresholds is really a matter of concern and would go a long way to assure the effectiveness.

- **Interoperability:** If a company outsources or creates applications with one cloud computing vendor, the company may find it difficult to change to another computing vendor that has proprietary Application Programming Interfaces (APIs) and different formats for importing and exporting data. This creates problems of achieving interoperability of applications between two cloud computing vendors. We may need to reformat/reorganize data or change the logic in applications.
- **Hidden Costs:** Like any such services in prevailing business systems, cloud computing service providers do not reveal 'what hidden costs are'. For instance, companies could incur higher network charges from their service providers for storage and database applications containing terabytes of data in the cloud. This outweighs costs they could save on new infrastructure, training new personnel, or licensing new software. In another instance of incurring network costs, companies, who are far from the location of cloud providers, could experience latency, particularly when there is heavy traffic.
- **Unexpected Behavior:** It is important to test the application in the cloud with a pilot study to check for unexpected behavior. Let's suppose that credit card validation application works well at our company's internal data centre. Examples of tests include how the application validates credit cards, and how, in the scenario of the buying crunch, it allocates resources and releases unused resources, turning them over to other work. If the tests show unexpected results of credit card validation or releasing unused resources, we will need to fix the problem before executing or obtaining cloud services from the cloud.
- **Software Development in Cloud:** To develop software using high-end databases, the most likely choice is to use cloud server pools at the internal data corporate centre and extend resources temporarily for testing purposes. This allows project managers to control costs, manage security and allocate resources to clouds for a project. The project managers can also assign individual hardware resources to different cloud types: Web development cloud, testing cloud, and production cloud. The cost associated with each cloud type may differ from one another. The cost per hour or usage with the development cloud is most likely lower than the production cloud, as additional features, such as SLA and security, are allocated to the production cloud. The managers can limit projects to certain clouds. For instance, services from portions of the production cloud can be used for the production configuration. Services from the development cloud can be used for development purpose only.