PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

Multiple Choice Questions

Questions No.(s) 1 to 6 are based on the Case Scenario. Remaining two question no(s). 7 and 8 are independent questions.

VK Textile Cotton Fabrics Private Limited is an export unit established in the year 2016. Company manufactures Cotton Fabrics in India and exports it to some foreign countries also. In December 2019, the company acquired a manufacturing unit situated in Dubai (UAE). Presently, Company is going in the process of listing in Bombay Stock Exchange and National Stock Exchange for listing its securities. Mr. Sameer Jain joined the Company as Chief Executive Officer (CEO) with effect from 01st January 2020. After taking his duty charge; he held various meetings with the company's management and stakeholders and presented a unified proposal on future of the company in meeting which are as given below:

- Expansion of the company business in other foreign countries includes European, Gulf and Asia-Pacific Countries.
- Providing best quality products under reasonable prices i.e., Value for money for its customers worldwide.
- Spreading out e-commerce business activities and online presence worldwide.
- Proposing Sales Plan (Budget) Turnover setting for the incoming Financial Year (2020-2021) to ₹ 2500 Crores from present budgeted turnover of ₹ 800 Crores in the Current Financial Year (2019-2020) with the help of strong boost sales, marketing strategy and corporate branding.
- Recognition of International ISO Certification to adopt IS and Process Audit.
- Stringent implementation of IS security policy.
- Adoption of new and emerging IT technologies includes Cloud Computing, Mobile Computing, Green Computing etc. for the company.
- Adoption of best practices of Corporate and Business Governance and COBIT 5 framework.
- Undertaking of a Business Process Reengineering (BPR) project in support of a new and direct marking approach to its customers.
- Shifting to maintenance of all records and documents in electronic digitalized form.
- Reciprocal agreement for disaster recovery with another company called G.K. Global Textile and Cotton Fabrics Limited (already a listed entity in Bombay Stock Exchange) w.e.f. 25th February, 2020.

Based on the above case, answer the following questions (1 to 6):

1. VK Textile Cotton Fabrics Private Limited has decided to enter into a reciprocal agreement as one of the strategies of Disaster Recovery Planning. Which of the following risk treatment approach does it indicate?

   (a) Risk Transfer

   (b) Risk Avoidance

   (c) Risk Mitigation

   (d) Risk Acceptance

2. VK Textile Cotton Fabrics Private Limited has decided to enter into a reciprocal agreement as one of the strategies of Disaster Recovery Planning. Which of the following represents the greatest risk created by reciprocal agreement for Disaster Recovery made between two companies - G.K. Global Textile and Cotton Fabrics Limited?

   (a) The security infrastructure in each company may be different.

   (b) The recovery plan cannot be tested.

   (c) The resources may not be available when needed.

   (d) The development in any company may result in hardware and software incompatibility.

3. Suppose you are an IS auditor of VK Textile Cotton Fabrics Private Limited. Company undertakes a Business Process Reengineering (BPR) project in support of a new and direct marking approach to its customers through establishment of new innovative information support system. Which of the following would be your primary key concern about the new process?

   (a) Are key controls in place to protect assets and information resources?

   (b) Does it address the corporate customer requirements?

   (c) Does system meet the performance goals (time and resource)?

   (d) Are owners responsible for various processes have been identified?

4. Suppose you are appointed as an IS auditor of VK Textile Cotton Fabrics Private Limited. The activities that would be involved in Information Systems' Audit are as follows:

   (i) Planning

   (ii) Close

   (iii) Analysis

(iv) Reporting

(v) Fieldwork

(vi) Scoping

How will you conduct IS audit in correct order/manner?

(a) (ii), (i), (iv), (iii), (vi), (v)

(b) (iii), (ii), (i), (iv), (v), (vi)

(c) (i), (iii), (ii), (iv), (v), (vi)

(d) (vi), (i), (v), (iii), (iv), (ii)

5. VK Textile Cotton Fabrics Private Limited is planning to keep all records and documents in electronic form. Which of the following section of Information Technology Act 2000 provides that the documents, records or information which are to be retained for any specified period shall be deemed to have been retained if the same are retained in the electronic form?

(a) Section 4

(b) Section 5

(c) Section 6

(d) Section 7

6. Which of the following emerging technology would have been adopted by VK Textile Cotton Fabrics Private Limited that promotes the practice of using computers and IT resources in a more efficient environmentally friendly and responsible way?

(a) Grid Computing

(b) Cloud Computing

(c) Virtualization

(d) Green Computing

7. Under the phase of Feasibility Study of System Development Life Cycle (SDLC), what possible dimension of the proposed web-based knowledge portal system of XYZ University is said to have been compromised in a situation if the students of the university are not able to access the e-resources available on university's website anytime?

(a) Technical Feasibility

(b) Resource Feasibility

(c) Behavioral Feasibility

(d) Economic Feasibility

8. Identify the Information System that would be useful for an organization in case it wishes to remotely access its documents for internal communication.

   (a) Electronic Message Communication System

   (b) Text Processing System

   (c) Teleconferencing and Videoconferencing System

   (d) Electronic Document Management System

DESCRIPTIVE QUESTIONS

Chapter 1: Concepts of Governance and Management of Information Systems

9. COBIT 5 explains various principles and enablers to act as a single business framework for the seamless Governance and Management of Enterprises IT. Discuss in detail the term "Enablers" in context of COBIT 5.

10. Discuss Information Systems Assurance. How COBIT 5 can play a role in achieving Information Systems assurance?

Chapter 2: Information System Concepts

11. Systems help to collect, store, and analyse data to produce the desired information for the functioning, betterment and expansion of any business. Classify the systems based on following parameters:

    (a) Interactive Behavior

    (b) Working/Output

12. In an organization PQR Ltd., Mr. A works as an Operational Manager who operates an Information system that helps him improving the operational efficiency of his organization. Identify the Information system he is working on and further discuss various activities that are performed by such a system.

Chapter 3: Protection of Information Systems

13. An internet connection along with providing benefits to an organization in terms of business competitiveness and time management, speed of operations etc. exposes it to harmful elements also. How can an organization be protected against these harmful elements?

14. In an enterprise ABC, the controls related to Operations management are responsible for the daily running of its hardware and software facilities. Discuss the functions over which these controls are implemented.

Chapter 4: Business Continuity Planning and Disaster Recovery Planning

15. The development of Business Continuity Planning (BCP) in an organization is prepared using a methodology having eight different phases. However, the extent of applicability of each phase can be tailored according to the respective organization. Elaborate these phases involved in the development of BCP.

16. In a BCP Audit; the auditor is expected to evaluate whether the processes of developing and maintaining are documented, communicated and tested plans for continuity of business operations are in place. List some BCP audit steps that an auditor will have to take regarding Building, Utilities and Transportation.

Chapter 5: Acquisition, Development and Implementation of Information Systems

17. Accountants are uniquely qualified to participate in systems development as they may combine knowledge of IT, business, accounting and internal control to ensure that new systems meet the needs of the user and possess adequate internal controls. Discuss the various aspects in which an accountant can help in system development.

18. Elaborate the major activities that are involved in Database Designing of System Designing phase of Systems Development Life Cycle.

Chapter 6: Auditing of Information Systems

19. (a) Explain the term Information Systems Audit.

    (b) Consider yourself to be an IS Auditor. Discuss the skill set that is expected to be acquired by you to undertake any Auditing assignment.

20. Application Controls refer to the transactions and data relating to each computer-based application system and are therefore, specific to each such application. Comprehend the various types of Application Controls. Also discuss the types of Audit Trails that exist.

Chapter 7: Information Technology Regulatory Issues

21. The MRA Marg police of Mumbai received an email at 9:30 am on 17th August 2011 challenging the local security agencies to prevent a terror attack in Mumbai. On detailed investigation, it was found that the IP address of the sender was traced to Patna in Bihar and the email was created 10 minutes before the email was sent. The sender while creating the new email-id had given two mobile numbers in the personal details' column. Both the numbers belonged to a photo frame-maker in Patna. Further probing led to the arrest of the email sender named Mr. X who was found to have criminal record having involved in terror related activities. The MRA Marg police registered a case of cyber-terrorism under the IT Act, 2000 against Mr. X. Identify and elaborate the Section under which Mr. X is held guilty.

22. List down the various norms recommended by SEBI for the following:

    (i) Systems Audit (ii) Audit Report Norms

Chapter 8: Emerging Technologies

23. Infrastructure as a Service (IaaS) is a service model under Cloud Computing that provides computing resources such as processing power, data communication, data storage and networks for cloud users etc. to run their application on-demand. Elaborate different instances of IaaS related to the aforesaid features.

24. Mobile Computing is a versatile and strategic technology that increases information quality and accessibility, enhances operational efficiency and improves management effectiveness. However, many issues are related with Mobile Computing. Discuss them.

SUGGESTED ANSWERS/HINTS

MULTIPLE CHOICE ANSWERS

1. (c) Risk Mitigation

2. (d) The development in any company may result in hardware and software incompatibility.

3. (a) Are key controls in place to protect assets and information resources?

4. (d) (vi), (i), (v), (iii), (iv), (ii)

5. (d) Section 7

6. (d) Green Computing

7. (c) Behavioral Feasibility

8. (d) Electronic Document Management System

DESCRIPTIVE ANSWERS

9. In context of COBIT 5; Enablers are factors that, individually and collectively, influence whether something will work in governance and management of enterprise IT. Enablers are driven by the goals cascade i.e. higher-level IT related goals defining 'what the different enablers should achieve'.

The COBIT 5 framework describes seven categories of enablers, which are as follows:

(i) Principles, Policies and Frameworks are the vehicle to translate the desired behavior into practical guidance for day-to-day management.

(ii) **Processes** describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.

(iii) **Organizational structures** are the key decision-making entities in an enterprise.

(iv) **Culture, Ethics and Behavior** of individuals and of the enterprise is very often underestimated as a success factor in governance and management activities.

(v) **Information** is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.

(vi) **Services, Infrastructure and Applications** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.

(vii) **People, Skills and Competencies** are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

10. **Information Systems Assurance:** In the rapidly changing digital world, enterprises are inundated with new demands, stringent regulations and risk scenarios emerging daily, making it critical to effectively govern and manage information and related technologies. This has resulted in enterprise leaders being under constant pressure to deliver value to enterprise stakeholders by achieving business objectives. This has made it imperative for management to ensure effective use of information and technology investments and related IT for not only supporting enterprise goals but also to maintain compliance with internally directed and externally imposed regulations. This dynamic changing environment enforces the usage of globally accepted good practices and frameworks and developing a holistic approach which meets the needs of stakeholders.

Using COBIT 5 for Information System Assurance

Auditors will have to understand the business processes of the enterprises and organization structure to be effective. This understanding of the business process must be coupled with understanding of the enterprise's policies, procedures and practices as implemented. Any enterprise executes its business operations through its staff who need to have defined job responsibilities, which are provided in the organization structure. The organization structure needs to have internal control structure. IT implementation in the enterprise makes it imperative that the internal control structure is built into the IT as deployed. Further, IT impacts the way business operations could be performed and internal controls are implemented. Hence, it is critical for auditors to understand the organization

structure of the enterprise being audited as relevant to the objectives and scope of the assignment.

- COBIT 5 has been engineered to meet expectations of multiple stakeholders. It is designed to deliver benefits to both an enterprise's internal stakeholders, such as the board, management, employees, etc. as well as external stakeholders - customers, business partners, external auditors, shareholders, consultants, regulators, etc.
- It is written in a non-technical language and is therefore, usable not only by IT professionals and consultants but also by senior management personnel, assurance providers; regulators for understanding and addressing IT related issues as relevant to them.
- Globally from the GRC perspective, COBIT has been widely used with COSO by management, IT professionals, regulators and auditors (internal/external) for implementing or evaluating Governance and management practices from an end-to-end perspective.
- COBIT has been used as an umbrella framework under which other standards and approaches, such as ITIL, ISO 27001 etc. have been integrated into overall enterprise governance.

11. (a) **Based on Interactive behavior:** Systems may be classified as **Open Systems** or **Closed System** based on 'how the system interacts with environment'.

- An **Open System** interacts with other systems in its environment. For example; Information system is an open system because it takes input from the environment and produces output to the environment, which changes as per the changes in the environment.
- **Closed System** does not interact with the environment and does not change with the changes in environment. Consider a 'throw-away' type sealed digital watch, which is a system, composed of several components that work in a cooperative fashion designed to perform some specific task. This watch is a closed system as it is completely isolated from its environment for its operation.

(b) **Based on Working/Output:** Based on the working style and the output, the systems can be classified as **Deterministic** and **Probabilistic System**.

- A **Deterministic System** operates in a predictable manner. For example - software that performs on a set of instructions is a deterministic system.
- A **Probabilistic System** can be defined in terms of probable behavior. For example - inventory system is a probabilistic system where the average demand, average time for replenishment, etc. may be defined, but the exact value at any given time is not known.

12. Mr. A is working on a Transaction Processing System (TPS) that helps him in improving the operational efficiency of his organization PQR Ltd.

Transaction Processing Systems (TPS) - At the lowest level of management, TPS is an information system that manipulates data from business transactions. Any business activity such as sales, purchase, production, delivery, payments or receipts involves transaction and these transactions are to be organized and manipulated to generate various information products for external use. For example, selling of a product to a customer will give rise to the need of further information like customer billing, inventory status and increase in account receivable balance. TPS will thus record and manipulate transaction data into usable information.

The various activities performed by TPS are as follows:

- Capturing data to organize in files or databases;
- Processing of files/databases using application software;
- Generating information in the form of reports; and
- Processing of queries from various quarters of the organization.

A TPS may follow the periodic data preparation and batch processing (as in payroll application) or on-line processing (as in inventory control application). However, in industries and business houses, now-a-days on-line approach is preferred in many applications as it provides information with up-to-date status. However, the people involved in TPS usually are not able to take any management decision.

13. An Internet connection exposes an organization to the entire world. This brings up the issue of benefits the organization should derive along with the precaution against harmful elements. This can be achieved through the 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.

14. Operations management is responsible for the daily running of hardware and software facilities. Operations management typically performs controls over the following functions as mentioned below:

(a) **Computer Operations:** The controls over computer operations govern the activities that directly support the day-to-day execution of either test or production systems on the hardware/software platform available. Three types of controls fall under this category:

- **Operation controls:** These controls prescribe the functions that either human operators or automated operations facilities must perform.

- **Scheduling controls:** These controls prescribe how jobs are to be scheduled on a hardware/software platform.
- **Maintenance controls:** These controls prescribe how hardware is to be maintained in good operating order.

(b) **Network Operations:** This includes the proper functioning of network operations and monitoring the performance of network communication channels, network devices, and network programs and files. Data may be lost or corrupted through component failure. Communication lines viz. twisted pair, coaxial cables, fibre optics, microwave and satellite etc.; Hardware in terms of ports, modems, multiplexers, switches and concentrators etc.; Software - Packet switching software, polling software, data compression software etc.; and the transmission disruption/destruction or corruption between sender and receiver due to failure of any component.

(c) **Data Preparation and Entry:** Irrespective of whether the data is obtained indirectly from source documents or directly from say customers, keyboard environments and facilities should be designed to promote speed and accuracy and to maintain the well-being of keyboard operators.

(d) **Production Control:** This includes the major functions like- receipt and dispatch of input and output; job scheduling; management of service-level agreements with users; transfer pricing/charge-out control; and acquisition of computer consumables.

(e) **File Library:** This includes the management of an organization's machine-readable storage media like magnetic tapes, cartridges, and optical disks.

(f) **Documentation and Program Library:** This involves that documentation librarians ensure that documentation is stored securely; that only authorized personnel gain access to documentation; that documentation is kept up-to-date and that adequate backup exists for documentation. The documentation may include reporting of responsibility and authority of each function; Definition of responsibilities and objectives of each functions; Reporting responsibility and authority of each function; Policies and procedures; Job descriptions and Segregation of duties.

(g) **Help Desk/Technical support:** This assist end-users to employ end-user hardware and software such as micro-computers, spreadsheet packages, database management packages etc. and provided the technical support for production systems by assisting with problem resolution.

(h) **Capacity Planning and Performance Monitoring:** Regular performance monitoring facilitates the capacity planning wherein the resource deficiencies must be identified well in time so that they can be made available when they are needed.

(i) **Management of Outsourced Operations:** This has the responsibility for carrying out day-to-day monitoring of the outsourcing contract.

15. The phases that are involved in the development of Business Continuity Planning (BCP) are as follows:

- **Phase 1 – Pre-Planning Activities (Project Initiation):** This Phase is used to obtain an understanding of the existing and projected computing environment of the organization. This enables the project team to refine the scope of the project and the associated work program; develop project schedules; and identify and address any issues that could have an impact on the delivery and the success of the project.

  During this phase, a Steering Committee should be established. The committee should have the overall responsibility for providing direction and guidance to the Project Team. The committee should also make all decisions related to the recovery planning effort. The Project Manager should work with the Steering Committee in finalizing the detailed work plan and developing interview schedules for conducting the Security Assessment and the Business Impact Analysis. Two other key deliverables of this phase are the development of a policy to support the recovery programs; and an awareness program to educate management and senior individuals who will be required to participate in the project.

- **Phase 2 – Vulnerability Assessment and General Definition of Requirements:** It is preferable from an economic and business strategy perspective, to concentrate on activities that have the effect of reducing the possibility of disaster occurrence, rather than concentrating primarily on minimizing impact of an actual disaster. This phase addresses measures to reduce the probability of occurrence and include the following key tasks:

  - A thorough Security Assessment of the computing and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security; insurance; security planning and administration; application controls; and personal computers.
  - The Security Assessment will enable the project team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.
  - Present findings and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.
  - Define the scope of the planning effort.
  - Analyze, recommend and purchase recovery planning and maintenance

software required to support the development of the plans and to maintain the plans current following implementation.

- Develop a Plan Framework.
- Assemble Project Team and conduct awareness sessions.

- **Phase 3 – Business Impact Assessment (BIA):** A Business Impact Assessment (BIA) of all business units that are part of the business environment enables the project team to identify critical systems, processes and functions; assess the economic impact of incidents and disasters that result in a denial of access to systems services and other services and facilities; and assess the "pain threshold," that is, the length of time business units can survive without access to systems, services and facilities.

  The BIA Report should be presented to the Steering Committee. This report identifies critical service functions and the timeframes in which they must be recovered after interruption. The BIA Report should then be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities.

- **Phase 4 – Detailed Definition of Requirements:** During this phase, a profile of recovery requirements is developed. This profile is to be used as a basis for analyzing alternative recovery strategies. The profile is developed by identifying resources required to support critical functions identified in Phase 3. This profile should include hardware (mainframe, data and voice communications and personal computers), software (vendor supplied, in-house developed, etc.), documentation (DP, user, procedures), outside support (public networks, DP services, etc.), facilities (office space, office equipment, etc.) and personnel for each business unit. Recovery Strategies will be based on short term, intermediate term and long-term outages. Another key deliverable of this phase is the definition of the plan scope, objectives and assumptions.

- **Phase 5 – Plan Development:** During this phase, recovery plans components are defined and plans are documented. This phase also includes the implementation of changes to user procedures, upgrading of existing data processing operating procedures required to support selected recovery strategies and alternatives, vendor contract negotiations (with suppliers of recovery services) and the definition of Recovery Teams, their roles and responsibilities. Recovery standards are also be developed during this phase.

- **Phase 6 – Testing/Exercising Program:** The plan Testing/Exercising Program is developed during this phase. Testing/exercising goals are established, and alternative testing strategies are evaluated. Testing strategies tailored to the environment should be selected and an on-going testing program should be established.

- **Phase 7 – Maintenance Program:** Maintenance of the plans is critical to the success of an actual recovery. The plans must reflect changes to the environments that are supported by the plans. It is critical that existing change management processes are revised to take recovery plan maintenance into account. In areas, where change management does not exist, change management procedures will be recommended and implemented. Many recovery software products take this requirement into account.
- **Phase 8 – Initial Plan Testing and Implementation:** Once plans are developed, initial tests of the plans are conducted and any necessary modifications to the plans are made based on an analysis of the test results. Specific activities of this phase include defining the test purpose/approach; identifying test teams; structuring the test; conducting the test; analyzing test results; and modifying the plans as appropriate.

  The approach taken to test the plans depends in large part, on the recovery strategies selected to meet the recovery requirements of the organization. As the recovery strategies are defined, specific testing procedures should be developed to ensure that the written plans are comprehensive and accurate.

16. Some BCP audit steps that an auditor will have to take regarding Building, Utilities and Transportation are as follows:

- Does the disaster recovery/ business resumption plan have a provision for having a building engineer inspect the building and facilities soon after a disaster so that damage can be identified and repaired to make the premises safe for the return of employees as soon as possible?
- Does the disaster recovery/business resumption plan consider the need for alternative shelter, if needed? Alternatives in the immediate area may be affected by the same disaster.
- Review any agreements for use of backup facilities.
- Verify that the backup facilities are adequate based on projected needs (telecommunications, utilities, etc.). Will the site be secure?
- Does the disaster recovery/ business resumption plan consider the failure of electrical power, natural gas, toxic chemical containers, and pipes?
- Are building safety features regularly inspected and tested?
- Does the plan consider the disruption of transportation systems? This could affect the ability of employees to report to work or return home. It could also affect the ability of vendors to provide the goods needed in the recovery effort.

17. An accountant can help in various related aspects during system development; some of them are as follows:

    (i) **Return on Investment (RoI):** This defines the return; an entity shall earn on a particular investment i.e. capital expenditure. This financial data is a prime consideration for any capital expenditure entity decides to incur. The important data required for this analysis being the cost of project, the expected revenue/benefit for a given period. The analysis ideally needs to be done before the start of the development efforts for better decision making by management. For this analysis following data needs to be generated. This includes estimates for typical costs like - **Development Costs** for a computer based information system that include costs of the system development process like salaries of developers; **Operating Costs** including hardware/software rental or depreciation charges; salaries of computer operators and other data processing personnel, who will operate the new system and **Intangible Cost** that cannot be easily measured.

    (ii) **Computing Cost of IT Implementation and Cost Benefit Analysis:** For analysis of RoI, accountants need the costs and returns from the system development efforts. For correct generation of data, proper accounting needs to be done. Accountants shall be the person to whom management shall look for the purpose.

18. **Design of Database:** Design of the database involves determining its scope ranging from local to global structure. The scope is decided based on the interdependence among organizational units. The design of the database involves four major activities, which are as follows:

    - **Conceptual Modeling:** These describe the application domain via entities/objects, attributes of these entities/objects and static and dynamic constraints on these entities/objects, their attributes, and their relationships.
    - **Data Modeling:** Conceptual Models need to be translated into data models so that they can be accessed and manipulated by both high-level and low-level programming languages.
    - **Storage Structure Design:** Decisions must be made on how to linearize and partition the data structure so that it can be stored on some device. For example - tuples (row) in a relational data model must be assigned to records, and relationships among records might be established via symbolic pointer addresses.
    - **Physical Layout Design:** Decisions must be made on how to distribute the storage structure across specific storage media and locations for example, the cylinders, tracks, and sectors on a disk and the computers in a LAN or WAN.

19. (a) The Information Systems (IS) Audit of an Information System environment may include one or both of the following:

- Assessment of internal controls within the IS environment to assure validity, reliability, and security of information and information systems.
- Assessment of the efficiency and effectiveness of the IS environment.

The IS audit process is to evaluate the adequacy of internal controls with regard to both specific computer program and the data processing environment as a whole.

(b) The audit objective and scope has a significant bearing on the skill and competence requirements of an IS auditor. The set of skills that is generally expected to be with an IS auditor include:

- Sound knowledge of business operations, practices and compliance requirements;
- Should possess the requisite professional technical qualification and certifications;
- A good understanding of information Risks and Controls;
- Knowledge of IT strategies, policy and procedural controls;
- Ability to understand technical and manual controls relating to business continuity; and
- Good knowledge of Professional Standards and Best Practices of IT controls and security.

Therefore, the audit process begins by defining the scope and objectives to adapt the standards and benchmarks for developing information model for collecting and evaluating evidence to execute the audit.

20. Various types of Application Controls are as follows:

- **Boundary Controls:** These establish interface between the user of the system and the system itself. The system must ensure that it has an authentic user. Users allowed using resources in restricted ways.
- **Input Controls:** These are responsible for bringing both the data and instructions into the information system. Input Controls are validation and error detection of data input into the system.
- **Communication Controls:** These are responsible for controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, audit trail controls, and existence controls.

- **Processing Controls:** These are responsible for computing, sorting, classifying and summarizing data. It maintains the chronology of events from the time data is received from input or communication systems to the time data is stored into the database or output as results.
- **Output Controls:** These are responsible to provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared and routed to users.
- **Database Controls:** These are responsible to provide functions to define, create, modify, delete and read data in an information system. It maintains procedural dataset of rules to perform operations on the data to help a manager to take decisions.

The two types of audit trails that should exist in each subsystem are as follows:

- An **Accounting Audit Trail** to maintain a record of events within the subsystem; and
- An **Operations Audit Trail** to maintain a record of the resource consumption associated with each event in the subsystem.

21. Section 66F of IT Act, 2000 is applicable in this case.

[Section 66F] **Punishment for cyber terrorism**

(1) Whoever -

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

(iii) introducing or causing to introduce any computer contaminant,

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or

likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,

commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

22. Mandatory audits of systems and processes bring transparency in the complex workings of SEBI, prove integrity of the transactions and build confidence among the stakeholders.

(i) Systems Audit: SEBI had mandated that exchanges shall conduct an annual system audit by a reputed independent auditor.

- The Audit shall be conducted according to the Norms, Terms of References (TOR) and Guidelines issued by SEBI.
- Stock Exchange/Depository (Auditee) may negotiate and the board of the Stock Exchange / Depository shall appoint the Auditors based on the prescribed Auditor Selection Norms and TOR. The Auditors can perform a maximum of 3 successive audits. The proposal from Auditor must be submitted to SEBI for records.
- Audit schedule shall be submitted to SEBI at-least 2 months in advance, along with scope of current audit & previous audit.
- The scope of the Audit may be extended by SEBI, considering the changes which have taken place during last year or post previous audit report.
- Audit has to be conducted and the Audit report be submitted to the Auditee. The report should have specific compliance/non-compliance issues, observations for minor deviations as well as qualitative comments for scope for improvement. The report should also take previous audit reports in consideration and cover any open items therein.
- The Auditee management provides their comment about the Non-Conformities (NCs) and observations. For each NC, specific time-bound (within 3 months) corrective action must be taken and reported to SEBI. The auditor should indicate if a follow-on audit is required to review the status of NCs. The report along with Management Comments shall be submitted to SEBI within 1 month of completion of the audit.

(ii) Audit Report Norms: These are given as follows:

- The Systems Audit Reports and Compliance Status should be placed before the Governing Board of the Stock Exchanges/Depositories and the system audit report along with comments of Stock Exchanges / Depositories should be communicated to SEBI.
- The Audit report should have explicit coverage of each Major Area mentioned in the TOR, indicating any Nonconformity (NCs) or Observations (or lack of it). For each section, auditors should also provide qualitative input about ways to improve the process, based upon the best practices observed.

23. The different instances of Infrastructure as a Service (IaaS) are as follows:

- **Network as a Service (NaaS):** NaaS, an instance of IaaS, provides users with needed data communication capacity to accommodate bursts in data traffic during data-intensive activities such as video conferencing or large file downloads. It is an ability given to the end-users to access virtual network services that are provided by the service provider over the Internet on a per-per-use basis. NaaS allows network architects to create virtual networks; virtual network interface cards (NICs), virtual routers, virtual switches, and other networking components. It further allows the network architect to deploy custom routing protocols and enables the design of efficient in-network services, such as data aggregation, stream processing, and caching. NaaS providers operate using three common service models: Virtual Private Network (VPN), Bandwidth on Demand (BoD) and Mobile Virtual Network (MVN).
- **Storage as a Service (STaaS):** STaaS, an instance of IaaS, provides storage infrastructure on a subscription basis to users who want a low-cost and convenient way to store data, synchronize data across multiple devises, manage off-site backups, mitigate risks of disaster recovery, and preserve records for the long-term. It is an ability given to the end users to store the data on the storage services provided by the service provider. STaaS allows the end users to access the files at any time from any place. STaaS provider provides the virtual storage that is abstracted from the physical storage of any cloud data center. STaaS is also a cloud business model that is delivered as a utility.
- **Database as a Service (DBaaS):** This is also related to IaaS and provides users with seamless mechanisms to create, store, and access databases at a host site on demand. It is an ability given to the end users to access the database service without the need to install and maintain it on the pay-per-use basis. The end users can access the database services through any Application Programming Interfaces (APIs) or Web User Interfaces provided by the service provider.
- **Backend as a Service (BaaS):** It is a type of IaaS, that provides web and mobile app developers a way to connect their applications to backend cloud storage with added services such as user management, push notifications, social network services

integration using custom software development kits and application programming interfaces.

- **Desktop as a Service (DTaaS):** It is an instance of IaaS that provides ability to the end users to use desktop virtualization without buying and managing their own infrastructure. DTaaS is a pay-per-use cloud service delivery model in which the service provider manages the back-end responsibilities of data storage, backup, security and upgrades. The end-users are responsible for securing for managing their own desktop images, applications, and security. These services are simple to deploy, are highly secure, and produce better experience on almost all devices.

24. Some issues in Mobile Computing are as follows:

- **Security Issues:** Wireless networks in Mobile computing have relatively more security requirements than wired network. These are as follows.
  - **Confidentiality:** Preventing unauthorized users from gaining access to critical information of any particular user.
  - **Integrity:** Ensures unauthorized modification, destruction or creation of information cannot take place.
  - **Availability:** Ensuring authorized users getting the access they require.
  - **Legitimate:** Ensuring that only authorized users have access to services.
  - **Accountability:** Ensuring that the users are held responsible for their security related activities by arranging the user and his/her activities are linked when necessary.
- **Bandwidth:** Bandwidth utilization can be improved by logging bulk operations against short requests and compression of data before transmission. The technique of caching frequently accessed data items can play an important role in reducing contention in narrow bandwidth wireless networks. The cached data can help improve query response time. Since mobile clients often disconnect to conserve battery power the cached data can support disconnected operations
- **Location Intelligence:** As the mobile computers move, they encounter networks with different features. A mobile computer must be able to switch from infrared mode to radio mode as it moves from indoors to outdoors. Additionally, it should be capable of switching from cellular mode of operation to satellite mode as the computer moves from urban and rural areas. As computers are working in cells and are being serviced by different network providers, the physical distance may not reflect the true network distance. A small movement may result in a much longer path if cell or network boundaries are crossed. It will also lead to updating of the location dependent information as described above. This can increase the network latency as well as risk of disconnection. Service connections must be dynamically transferred to the nearest server. However, when load balancing is a priority this may not be possible.

- **Power Consumption:** Mobile Computers will rely on their batteries as the primary power source. Batteries should be ideally as light as possible but at the same time they should be capable of longer operation times. Power consumption should be minimized to increase battery life. Chips can be redesigned to operate at lower voltages. Power management can also help. Individual components be powered down when they are idle.
- **Revising the technical architecture:** Mobile users are demanding and are important to the business world. To provide complete connectivity among users; the current communication technology must be revised to incorporate mobile connectivity. Additionally, application and data architectures must also be revised to support the demands put upon them by the mobile connectivity.
- **Reliability, coverage, capacity, and cost:** At present wireless network is less reliable, have less geographic coverage and reduced bandwidth, are slower, and cost more than the wired-line network services. It is important to find ways to use this new resource more efficiently by designing innovative applications.
- **Integration with legacy mainframe and emerging client/server applications:** Application development paradigms are changing. As a result of the IT industry's original focus on mainframes, a huge inventory of applications using communications interfaces that are basically incompatible with mobile connectivity have been accumulated. Still the application development trend is geared towards wired network.
- **End-to-end design and performance:** Since mobile computing involves multiple networks (including wired) and multiple application server platforms, end-to-end technical compatibility, server capacity design, and network response time estimates are difficult to achieve.
- **Business challenges:** In addition to these technical challenges, mobile computing also faces business challenges. This is due to the lack of trained professionals to bring the mobile technology to the general people and development of pilot projects for testing its capabilities.