PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

Multiple Choice Questions

1. "Enterprise Governance" can be defined as the set of responsibilities and practices exercised __________with the goal of providing strategic direction to ensure that objectives are achieved and risks are managed appropriately.

   (a) only by the board

   (b) only by the executive management

   (c) by both board and executive management

   (d) by board, executive management, and end-user

2. In DBMS, the database implementation is done at the three levels- Physical, Logical and External. Which of the statement is true about these levels?

   (a) Physical Level involves the implementation of the database on the hard disk.

   (b) Physical Level defines the schema which is divided into smaller units known as sub-schemas.

   (c) Logical Level defines the schema which is divided into smaller units known as sub-schemas.

   (d) External Level deals with the nature of data stored and the scheme of the data.

3. A hacker Mr. C, duplicates the login procedure of an employee of an organization ABC Ltd.; captures the user's password and attempts for the system's crash. Name the type of the attack.

   (a) Subversive Threat

   (b) Wire Tapping

   (c) Sabotage

   (d) Spoofing

4. Mr. Rahul is a security administrator in a bank which executes many real-time processes like ATM processing. If fast recovery is critical for its business processes, which type of backup option should he refer to the management of the company?

   (a) Cold Site

   (b) Hot Site

(c) Warm Site

(d) Reciprocal Agreement

5. An Analyst while conducting the Technical Feasibility under System Development Life Cycle (SDLC) would not consider that _____________?

   (a) Does the proposed equipment have the technical capacity to hold the data required to use the new system?

   (b) Can the system be expanded if developed?

   (c) Is the procurement of the hardware and software for the class of applications being considered, cost effective?

   (d) Will the proposed system provide adequate responses to inquiries, regardless of the number or location of users?

6. Which of the following represents the correct sequence of the steps involved in Information System (IS) Audit? (1) Planning, (2) Fieldwork, (3) Scoping, (4) Reporting, (5) Analysis and (6) Close.

   (a) (3) – (1) – (2) – (5) – (4) – (6)

   (b) (3) – (1) – (6) – (2) – (4) – (5)

   (c) (3) – (2) – (4) – (5) – (1) – (6)

   (d) (1) – (2) – (3) – (4) – (5) – (6)

7. Mr. A is an employee of XYZ company. He sends an email through his laptop to the client and pretends to be the Managing Director of the company. He informs the client to pay future payments in the employee Mr. A's account. Under which section will A be punished?

   (a) Section 66A

   (b) Section 66B

   (c) Section 66C

   (d) Section 66D

8. Among the emerging technologies, the ones which are environmentally sustainable are the ones which will survive the test of time. Such technologies are being designated by a key term called as _________.

   (a) Cloud Computing

   (b) Green Computing

(c) Mobile Computing

(d) Hybrid Computing

Concepts of Governance and Management of Information Systems

9. When risks are identified and analysed; it is not always appropriate to implement controls to counter them. Identify the possible Risk Management Strategies.

10. How can we say that COBIT 5 can be customized as per enterprise's specific requirement?

Information System Concepts

11. As an IT Expert, explain the importance of Information Systems from Strategic and Operational Perspective.

12. How Management Level Systems (MLS) differ from Strategic Level Systems (SLS)?

Protection of Information Systems

13. Discuss classification of Controls based on "Nature of Information Systems Resources".

14. Operating System is the computer control program that allows users and their applications to share and access common computer resources, such as processor, main memory, database and printers. Thus, protecting an Operating System access is crucial and should be dealt with utmost importance. Analyse the Operating Systems Access Controls that can be placed to safeguard Operating Systems.

Business Continuity Planning and Disaster Recovery Planning

15. List out the Objectives and Goals of Business Continuity Planning (BCP).

16. Determine the components of Business Continuity Management (BCM) Process.

Acquisition, Development and Implementation of Information Systems

17. As an Accountant, discuss the ways in which you can assist in various aspects during System development?

18. "A System Development Methodology is a formalized, standardized, well-organized and documented set of activities used to manage a system development project." Prepare a list of the common characteristics that all these system methodologies will have.

Auditing of Information Systems

19. "Existence of an Audit Trail is a key financial audit requirement since without an audit trail, the auditor may have extreme difficulty in gathering sufficient, appropriate audit evidence to validate the figures in the client's accounts." Determine the issues through which the performance of evidence collection and reliability of controls can be understood?

20. As an Information Systems (IS) Auditor, you should acquire a good understanding of the technology environment and related control issues. List out the key aspects that you would majorly emphasize upon.

Information Technology Regulatory Issues

21. Which section of IT Act, 2000 relates to "Delivery of Services by Service Provider". Discuss.

22. Discuss the guidelines recommended by Securities and Exchange Board of India (SEBI) to conduct audit of systems.

Emerging Technologies

23. What do you understand by the term "Community Cloud"? Discuss its characteristics.

24. Discuss the steps that can be incorporated in the work habits of computer users and businesses to minimize adverse impact on the global environment towards Green IT.

Questions based on Case Study

25. PQR is an Indian- based enterprise engaged in event management worldwide having offices at various locations in India and abroad. Most of the company's operations are performed online. However, the existing infrastructure system is facing several operational and security problems with growing volume of business. It realizes the existing information system must be upgraded for better delivery of services for improved customer satisfaction and to remain competitive in global market. To upgrade their existing system, the top management of the Company has appointed a high-level IT Steering Committee comprising IS Auditor as one of the members. The company also intends to develop a document for Disaster Recovery Procedure Plan after upgrading information infrastructure.

    Read the above and answer the following:

    (a) Describe the key functions of IT Steering Committee for overall development/upgradation?

    (b) Enterprise needs to take various steps to ensure that they comply with the Cyber Laws of India. List out the steps that they must take to ensure the compliance.

    (c) "System Maintenance" is a crucial aspect of Systems Development Life Cycle. Once the new Information Systems are implemented, most of them require at least some modification after development. The need for modification arises from a failure to anticipate/capture all the requirements during system analysis/design and/or from changing organizational requirements. Discuss various categories of System Maintenance.

SUGGESTED ANSWERS/HINTS

1. **(c)** by both board and executive management

2. **(a)** Physical Level involves the implementation of the database on the hard disk.

3. **(d)** Spoofing

4. **(b)** Hot Site

5. **(c)** Is the procurement of the hardware and software for the class of applications being considered, cost effective?

6. **(a)** (3) – (1) – (2) – (5) – (4) – (6)

7. **(d)** Section 66D

8. **(b)** Green Computing

9. When risks are identified and analyzed; it is not always appropriate to implement controls to counter them. Some risks may be minor, and it may not be cost effective to implement expensive control processes for them. Risk management strategies are explained below:

   - **Tolerate/Accept the risk**. One of the primary functions of management is managing risk. Some risks may be considered minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.
   - **Terminate/Eliminate the risk**. It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.
   - **Transfer/Share the risk**. Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risks associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organization. Risk also may be mitigated by transferring the cost of realized risk to an insurance provider.
   - **Treat/mitigate the risk.** Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects.
   - **Turn back.** Where the probability or impact of the risk is very low, then management may decide to ignore the risk.

10. COBIT 5 can be tailored to meet an enterprise's specific business model, technology environment, industry, location and corporate culture. Because of its open design, it can be applied to meet needs related to:

- Information security,
- Risk management,
- Governance and management of enterprise IT,
- Assurance activities,
- Legislative and regulatory compliance, and
- Financial processing or Corporate Social Responsibility (CSR) reporting.

Enterprises can select required guidance and best practices from specific publications and processes of COBIT 5. Further, the above examples show specific areas based on which best practices can be extracted from COBIT 5.

11. Relative Importance of Information Systems from Strategic/Operational Perspectives are as follows:

- An Information System can help in decision making, produce high quality of products and perform logistical functions, assist in determining scenarios such as unifications and achievements, and streamline the strategic planning process that can help top management to take corporate decision easily.
- In operations management, information systems design can apply to production control, research, development, and manufacturing to produce desired results of the products in terms of quality and cost. Information systems applications in the field of human resources management can help in retaining highly qualified employees by having important data concerning employees obtained after several processes used by human resource managers or personnel.
- Information systems also support logistical processes in various ways, such as real time inquiries to track an item from the point of shipment, receiving and storage of the item and inventory status of the item. Not only this, information systems can also provide the structure for programmers, database managers and data administrators to collaborate on new and existing projects.
- Information system is used in every aspect of business right from customer relationship management, marketing strategies, retailing, communication, product promotion, product development, forecast future sales to supply chain management etc. ERP, Data Mining tools, Data warehouse, Business intelligence, MIS, Internet, Intranet, Extranet etc. are the information systems and information technologies that support managers in every step of business.

- Information Systems have accelerated the pace of processing of enterprise information using IT and integrating all aspects of the operations of the business e.g. instead of gathering data manually and taking out hidden information from it by conducting meeting of executives, which is crucial in decision making for marketing strategies, customer relationship management etc., the same can be obtained by using the respective data mining tools and data warehouse.
- Information System also provides new platform to business world where space and time is no more obstacle. For example, selling and purchasing of products can be done on web any time and from anywhere.
- There are different kinds of systems depending upon the different interest, specialties and levels in an organization. The organization comprise of strategic, management, knowledge and operational levels, which is further divided into functional areas e.g. sales, marketing, manufacturing, finance, accounting and human resources. For example - the sales area uses operational level system to keep track of daily sales figures, a knowledge level systems designs the promotional displays of the organization, a management level system generates report of the monthly sales by territory and a strategic level system predicts the sale of the product in coming five years.

12. **Management-Level Systems (MLS)** support the middle managers in monitoring, decision-making and administrative activities and are helpful in answering questions like - Are things working well and in order? These provide periodic reports rather than instant information on operations. For example – A college control system gives report on the number of leaves availed by the staff, salary paid to the staff, funds generated by the fees, finance planning etc. These types of systems mainly answer “what if” questions. For example - What would be quality of teaching if college must achieve top ranking in academics? These types of questions can be answered only after getting new data from outside the organization, as well as data from inside which cannot be easily obtained from existing operational level systems.

    MLS supports managers in effective decision making by providing relevant and required information at the right time to the right people. Management Information System and Decision Support Systems are two major types of Management Level systems.

    - **Management Information Systems (MIS)** enables management at different levels in decision making and problem solving. They use results produced by the TPS, but they may also use other information.
    - **Decision Support System (DSS)** is a type of computerized information system that supports business and organizational decision-making activities. A properly-designed DSS is an interactive software-based system intended to help decision makers to compile useful information from raw data, documents, personal knowledge, and/or business models to identify and solve problems and make decisions.

Strategic Level Systems are for strategic managers to track and deal with strategic issues, assisting long-range planning. These systems support the senior level management to tackle and address strategic issues and long term trends, both inside organization and the outside world. These answer questions like what products should be launched to increase the profit and capture the market. It helps in long term planning. A principle area is tracking changes in the external conditions (market sector, employment levels, share prices, etc.) and matching these with the internal conditions of the organization. Executive Information Systems (EIS) serves the strategic level i.e. top level managers of the organization. ESS creates a generalized computing and communications environment rather than providing any pre-set applications or specific competence.

13. Classification of Controls based on "Nature of Information System Resources" is as follows:

- **Environmental Controls** are the controls relating to IT environment such as power, air-conditioning, Un-interrupted Power Supply (UPS), smoke detection, fire-extinguishers, dehumidifiers etc. These controls deal with the external factors in the Information System and preventive measures to overcome environmental exposures which are primarily due to elements of nature. Such common occurrences are Fire, Natural disasters-earthquake, volcano, hurricane, tornado, Power spike, Air conditioning failure, Electrical shock, Equipment failure, Water damage/flooding-even with facilities located on upper floors of high buildings. Water damage is a risk, usually from broken water pipes, and Bomb threat/attack. However, with proper controls, exposures can be reduced.
- **Physical Access Controls** are the controls relating to physical security of the tangible Information System resources and intangible resources stored on tangible media etc. Such controls include Access control doors, Security guards, door alarms, restricted entry to secure areas, visitor logged access, CCTV monitoring etc. These controls are personnel; hardware and software related and include procedures exercised on access to IT resources by employees/outsiders. These controls relate to establishing appropriate physical security and access control measures for IT facilities, including off-site use of information devices in conformance with the general security policy. These Physical security and access controls should address supporting services (such as electric power), backup media and any other elements required for the system's operation. Access should be restricted to authorized individuals where resources are located in public areas, they should be appropriately protected to prevent or deter loss or damage from theft or vandalism. Further, IT management should ensure zero visibility.
- **Logical Access Controls:** These are the controls relating to logical access to **information** resources such as operating systems controls, application software boundary controls, networking controls, access to database objects, encryption controls etc. Logical access controls are implemented to ensure that access to

systems, data and programs is restricted to authorized users to safeguard information against unauthorized use, disclosure or modification, damage or loss. The key factors considered in designing logical access controls include confidentiality and privacy requirements, authorization, authentication and incident handling, reporting and follow-up, virus prevention and detection, firewalls, centralized security administration, user training and tools for monitoring compliance, intrusion testing and reporting.

14. The Operating System Access Controls are as follows:

- **Automated terminal identification:** This will help to ensure that a particular session could only be initiated from a particular location or computer terminal.
- **Terminal log-in procedures:** A log-in procedure is the first line of defense against unauthorized access. The log-in procedure does not provide unnecessary help or information, which could be misused by an intruder. When the user initiates the log-on process by entering user-id and password, the system compares the ID and password to a database of valid users. If the system finds a match, then log-on attempt is authorized. If password or user-id is entered incorrectly, then after a specified number of wrong attempts, the system should lock the user from the system.
- **Access Token:** If the log on attempt is successful, the Operating System creates an access token that contains key information about the user including user-id, password, user group and privileges granted to the user. The information in the access token is used to approve all actions attempted by the user during the session.
- **Access Control List:** This list contains information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compasses his or her user-id and privileges contained in the access token with those contained in the access control list. If there is a match, the user is granted access.
- **Discretionary Access Control:** The system administrator usually determines; who is granted access to specific resources and maintains the access control list. However, in distributed systems, resources may be controlled by the end-user. Resource owners in this setting may be granted discretionary access control, which allows them to grant access privileges to other users. For example, the controller who is owner of the general ledger grants read only privilege to the budgeting department while accounts payable manager is granted both read and write permission to the ledger.
- **User identification and authentication:** The users must be identified and authenticated in a foolproof manner. Depending on risk assessment, more stringent methods like Biometric Authentication or Cryptographic means like Digital Certificates should be employed.

- **Password management system:** An operating system could enforce selection of good passwords. Internal storage of password should use one-way hashing algorithms and the password file should not be accessible to users.
- **Use of system utilities:** System utilities are the programs that help to manage critical functions of the operating system e.g. addition or deletion of users. Obviously, this utility should not be accessible to a general user. Use and access to these utilities should be strictly controlled and logged.
- **Duress alarm to safeguard users:** If users are forced to execute some instruction under threat, the system should provide a means to alert the authorities.
- **Terminal time out:** Log out the user if the terminal is inactive for a defined period. This will prevent misuse in absence of the legitimate user.
- **Limitation of connection time:** Define the available time slot. Do not allow any transaction beyond this time. For example, no computer access after 8.00 p.m. and before 8.00 a.m. - or on a Saturday or Sunday.

15. The primary objective of a Business Continuity Plan (BCP) is to minimize loss by minimizing the cost associated with disruptions and enable an organization to survive a disaster and to re-establish normal business operations. To survive, the organization must assure that critical operations can resume normal processing within a reasonable time frame. The key objectives of the contingency plan should be to:

- Provide the safety and well-being of people on the premises at the time of disaster;
- Continue critical business operations;
- Minimize the duration of a serious disruption to operations and resources (both information processing and other resources);
- Minimize immediate damage and losses;
- Establish management succession and emergency powers;
- Facilitate effective co-ordination of recovery tasks;
- Reduce the complexity of the recovery effort; and
- Identify critical lines of business and supporting functions.

Therefore, the goals of the Business Continuity Plan should be to:

- Identify weaknesses and implement a disaster prevention program;
- minimize the duration of a serious disruption to business operations;
- facilitate effective co-ordination of recovery tasks; and
- reduce the complexity of the recovery effort.

16. The components of the Business Continuity Management (BCM) process are as follows:

- **BCM – Process:** The management process enables the business continuity, capacity and capability to be established and maintained. The capacity and capability are established in accordance to the requirements of the enterprise.
- **BCM – Information Collection Process:** The activities of assessment process do the prioritization of an enterprise's products and services and the urgency of the activities that are required to deliver them. This sets the requirements that will determine the selection of appropriate BCM strategies in the next process.
- **BCM – Strategy Process:** Finalization of business continuity strategy requires assessment of a range of strategies. This requires an appropriate response to be selected at an acceptable level and during and after a disruption within an acceptable timeframe for each product or service, so that the enterprise continues to provide those products and services. The selection of strategy will take into account the processes and technology already present within the enterprise.
- **BCM – Development and Implementation Process:** Development of a management framework and a structure of incident management, business continuity and business recovery and restoration plans.
- **BCM – Testing and Maintenance Process:** BCM testing, maintenance and audit testify the enterprise BCM to prove the extent to which its strategies and plans are complete, current and accurate; and Identifies opportunities for improvement.
- **BCM – Training Process:** Extensive trainings in BCM framework, incident management, business continuity and business recovery and restoration plans enable it to become part of the enterprise's core values and provide confidence in all stakeholders in the ability of the enterprise to cope with minimum disruptions and loss of service.

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

(i) **Return on Investment (referred as 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, cost analysis is done that includes estimates for typical like Development Costs, Operating Costs and Intangible Costs.

(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.

(iii) **Skills expected from an Accountant:** An accountant, being an expert in accounting field must possess skills to understand the system development efforts and nuances of the same. S/he is expected to have various key skills, including understanding of the business objectives, expert book keeper, and understanding of system development efforts etc.

18. A System Development Methodology is a formalized, standardized, well-organized and documented set of activities used to manage a system development project. It refers to the framework that is used to structure, plan and control the process of developing an information system. Each of the available methodologies is best suited to specific kinds of projects, based on various technical, organizational, project and team considerations. The methodology is characterized by the following:

- The project is divided into several identifiable processes, and each process has a starting point and an ending point. Each process comprises several activities, one or more deliverables, and several management control points. The division of the project into these small, manageable steps facilitates both project planning and project control.
- Specific reports and other documentation, called Deliverables must be produced periodically during system development to make development personnel accountable for faithful execution of system development tasks.
- Users, managers, and auditors are required to participate in the project, which generally provide approvals, often called signoffs, at pre-established management control points. Signoffs signify approval of the development process and the system being developed.
- The system must be tested thoroughly prior to implementation to ensure that it meets users' needs as well as requisite functionalities.
- A training plan is developed for those who will operate and use the new system.
- Formal program change controls are established to preclude unauthorized changes to computer programs.
- A post-implementation review of all developed systems must be performed to assess the effectiveness and efficiency of the new system and of the development process.

19. The performance of evidence collection and understanding the reliability of controls involves issues like-

- **Data retention and storage:** A client's storage capabilities may restrict the amount of historical data that can be retained "on-line" and readily accessible to the auditor. If the client has insufficient data retention capacities, the auditor may not be able to review a whole reporting period transactions on the computer system. For example, the client's computer system may save data on detachable storage device by summarising transactions into monthly, weekly or period end balances.

- **Absence of input documents:** Transaction data may be entered into the computer directly without the presence of supporting documentation e.g. input of telephone orders into a telesales system. The increasing use of Electronic Data Interchange (EDI) will result in less paperwork being available for audit examination.
- **Non-availability of audit trail:** The audit trails in some computer systems may exist for only a short period. The absence of an audit trail will make the auditor's job very difficult and may call for an audit approach which involves auditing around the computer system by seeking other sources of evidence to provide assurance that the computer input has been correctly processed and output.
- **Lack of availability of printed output:** The results of transaction processing may not produce a hard copy form of output, i.e. a printed record. In the absence of physical output, it may be necessary for an auditor to directly access the electronic data retained on the client's computer. This is normally achieved by having the client provide a computer terminal and being granted "read" access to the required data files.
- **Audit evidence:** Certain transactions may be generated automatically by the computer system. For example, a fixed asset system may automatically calculate depreciation on assets at the end of each calendar month. The depreciation charge may be automatically transferred (journalised) from the fixed assets register to the depreciation account and hence to the client's income and expenditure account.
- **Legal issues:** The use of computers to carry out trading activities is also increasing. More organisations in both the public and private sector intend to make use of EDI and electronic trading over the Internet. This can create problems with contracts, e.g. when is the contract made, where is it made (legal jurisdiction), what are the terms of the contract and are the parties to the contract.

20. As an Information Systems (IS) Auditor, an important task for the auditor as a part of his/her preliminary evaluation is to gain a good understanding of the technology environment and related control issues. This could include consideration of the following:

- Analysis of business processes and level of automation,
- Assessing the extent of dependence of the enterprise on Information Technology to carry on its businesses i.e. Role of IT in the success and survival of business,
- Understanding technology architecture which could be quite diverse such as a distributed architecture or a centralized architecture or a hybrid architecture,
- Studying network diagrams to understand physical and logical network connectivity,

- Understanding extended enterprise architecture wherein the organization systems connect seamlessly with other stakeholders such as vendors (SCM), customers (CRM), employees (ERM) and the government,
- Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems,
- And finally, Studying Information Technology policies, standards, guidelines and procedures.

21. Section 6A of IT Act, 2000 deals with "Delivery of Services by Service Provider".

[Section 6A] Delivery of Services by Service Provider

(1) The appropriate Government may, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means authorize, by order, any service provider to setup, maintain and upgrade the computerized facilities and perform such other services as it may specify by notification in the Official Gazette.

Explanation –

For the purposes of this section, service provider so authorized includes any individual, private agency, private company, partnership firm, sole proprietor firm or any such other body or agency which has been granted permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector.

(2) The appropriate Government may also authorize any service provider authorized under sub-section (1) to collect, retain and appropriate such service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service.

(3) Subject to the provisions of sub-section (2), the appropriate Government may authorize the service providers to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.

(4) The appropriate Government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers under this section:

PROVIDED that the appropriate Government may specify different scale of service charges for different types of services.

22. The guidelines recommended by Securities and Exchange Board of India (SEBI) to conduct audit of systems are as follows:

- 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.

23. **Community Cloud:** The Community Cloud is the cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (eg. mission security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises. In this, a private cloud is shared between several organizations. This model is suitable for organizations that cannot afford a private cloud and cannot rely on the public cloud either.

Characteristics of Community Clouds are as follows:

- **Collaborative and Distributive Maintenance:** In this, no single company has full control over the whole cloud. This is usually distributive and hence better cooperation provides better results.
- **Partially Secure:** This refers to the property of the community cloud where few organizations share the cloud, so there is a possibility that the data can be leaked from one organization to another, though it is safe from the external world.

- **Cost Effective:** As the complete cloud if being shared by several organizations or community, not only the responsibility gets shared; the community cloud becomes cost effective too.

24. Some of steps for Green IT include the following:

Develop a sustainable Green Computing plan

- Involve stakeholders to include checklists, recycling policies, recommendations for disposal of used equipment, government guidelines and recommendations for purchasing green computer equipment in organizational policies and plans;
- Encourage the IT community for using the best practices and encourage them to consider green computing practices and guidelines.
- On-going communication about and campus commitment to green IT best practices to produce notable results.
- Include power usage, reduction of paper consumption, as well as recommendations for new equipment and recycling old machines in organizational policies and plans; and
- Use cloud computing so that multiple organizations share the same computing resources thus increasing the utilization by making more efficient use of hardware resources.

Recycle

- Dispose e-waste according to central, state and local regulations;
- Discard used or unwanted electronic equipment in a convenient and environmentally responsible manner as computers emit harmful emissions;
- Manufacturers must offer safe end-of-life management and recycling options when products become unusable; and
- Recycle computers through manufacturer's recycling services.

Make environmentally sound purchase decisions

- Purchase of desktop computers, notebooks and monitors based on environmental attributes;
- Provide a clear, consistent set of performance criteria for the design of products;
- Recognize manufacturer efforts to reduce the environmental impact of products by reducing or eliminating environmentally sensitive materials, designing for longevity and reducing packaging materials; and
- Use Server and storage virtualization that can help to improve resource utilization, reduce energy costs and simplify maintenance.

Reduce Paper Consumption

- Reduce paper consumption by use of e-mail and electronic archiving;
- Use of “track changes” feature in electronic documents, rather than redline corrections on paper;
- Use online marketing rather than paper based marketing; e-mail marketing solutions that are greener, more affordable, flexible and interactive than direct mail; free and low-cost online invoicing solutions that help cut down on paper waste; and
- While printing documents; make sure to use both sides of the paper, recycle regularly, use smaller fonts and margins, and selectively print required pages.

Conserve Energy

- Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors;
- Develop a thin-client strategy wherein thin clients are smaller, cheaper, simpler for manufacturers to build than traditional PCs or notebooks and most importantly use about half the power of a traditional desktop PC;
- Use notebook computers rather than desktop computers whenever possible;
- Use the power-management features to turn off hard drives and displays after several minutes of inactivity;
- Power-down the CPU and all peripherals during extended periods of inactivity;
- Try to do computer-related tasks during contiguous, intensive blocks of time, leaving hardware off at other times;
- Power-up and power-down energy-intensive peripherals such as laser printers according to need;
- Employ alternative energy sources for computing workstations, servers, networks and data centres; and
- Adapt more of Web conferencing offers instead of travelling to meetings in order to go green and save energy.

25. (a) The IT Steering Committee provides overall direction to deployment of IT and information systems in the enterprises. The key functions of the committee would include of the following:

- To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives;
- To establish size and scope of IT function and sets priorities within the scope;
- To review and approve major IT deployment projects in all their stages;

- To approve and monitor key projects by measuring result of IT projects in terms of return on investment, etc.;
- To review the status of IS plans and budgets and overall IT performance;
- To review and approve standards, policies and procedures;
- To make decisions on all key aspects of IT deployment and implementation;
- To facilitate implementation of IT security within enterprise;
- To facilitate and resolve conflicts in deployment of IT and ensure availability of a viable communication system exists between IT and its users; and
- To report to the Board of Directors on IT activities on a regular basis.

(b) Enterprises need to take steps to ensure compliance with cyber laws. Some key steps for ensuring compliance are given below:

- Designate a Cyber Law Compliance Officer as required.
- Conduct regular training of relevant employees on Cyber Law Compliance.
- Implement strict procedures in HR policy for non-compliance.
- Implement authentication procedures as suggested in law.
- Implement policy and procedures for data retention as suggested.
- Identify and initiate safeguard requirements as applicable under various provisions of the Act such as: Sections 43A, 69, 69A, 69B, etc.
- Implement applicable standards of data privacy on collection, retention, access, deletion etc.
- Implement reporting mechanism for compliance with cyber laws.

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

- **Scheduled Maintenance:** Scheduled maintenance is anticipated and can be planned for operational continuity and avoidance of anticipated risks. For example, the implementation of a new inventory coding scheme can be planned in advance, security checks may be promulgated etc.
- **Rescue Maintenance:** Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate troubleshooting solution. A system that is properly developed and tested should have few occasions of rescue maintenance.
- **Corrective Maintenance:** Corrective maintenance deals with fixing bugs in the code or defects found during the executions. A defect can result from design errors, logic errors coding errors, data processing and system performance errors. The need for corrective maintenance is usually initiated by bug reports

drawn up by the end users. Examples of corrective maintenance include correcting a failure to test for all possible conditions or a failure to process the last record in a file.

- **Adaptive Maintenance:** Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system. The term environment in this context refers to the totality of all conditions and influences, which act from outside upon the system, for example, business rule, government policies, work patterns, software and hardware operating platforms. The need for adaptive maintenance can only be recognized by monitoring the environment.
- **Perfective Maintenance:** Perfective maintenance mainly deals with accommodating to the new or changed user requirements and concerns functional enhancements to the system and activities to increase the system's performance or to enhance its user interface.
- **Preventive Maintenance:** Preventive maintenance concerns with the activities aimed at increasing the system's maintainability, such as updating documentation, adding comments and improving the modular structure of the system. The long-term effect of corrective, adaptive and perfective changes increases the system's complexity. As a large program is continuously changed, its complexity, which reflects deteriorating structure, increases unless work is done to maintain or reduce it. This work is known as preventive change.