PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

MULTIPLE CHOICE QUESTIONS

1. Some of the tasks performed in an organization XYZ Pvt. Ltd. are as follows:

   I. Review the processes used by the IT organization to identify, assess, and monitor/mitigate risks within the IT environment.

   II. Review how organization management and IT personnel are interacting and communicating current and future needs across the organization.

   III. Assess the involvement of IT leadership in the development and on-going execution of the organization's strategic goals.

   IV. Evaluate the physical IT Assets of the company in terms of hardware and software.

   You are appointed as an Internal Auditor to XYZ Pvt. Ltd. Which of the option highlight the activities that fall under your work preview while evaluating audit activities?

   (a) I, II, III, IV

   (b) I, II

   (c) I and III

   (d) I, II, III

2. Mr. B wants to invest some money for future but he has no idea where to invest and how much to invest. He is seeking help from a specialized system which is helping him to find answers of all queries such as how much money can be invested in portfolio and which securities would be better for him. Identify the specialized software system used in such situation.

   (a) Expert System

   (b) Knowledge System

   (c) Financial System

   (d) Core Banking System

3. A manufacturing company ABC recently made some changes in terms of checking for periodic performance reporting with variance, flaw in cash count and bank reconciliation and monitoring expenditure against budgeted amount. Which of the following control is used by company in this situation?

(a) Compensatory control

(b) Corrective control

(c) Preventive control

(d) Detective Control

4. ABC is the manufacturing company having worth of ₹ 5000 million. While developing Business Continuity Plan, the company sets-up a committee for providing direction and guidance to the whole project team and responsible to make all the decisions related to recovery planning efforts. Which of the following phase of BCP the committee is working at?

(a) Pre-planning Activities

(b) Vulnerability Assessment and general definition of requirement

(c) Plan development

(d) Business Impact Analysis

5. Choose the incorrect statement out of the following.

(a) The Incremental model is a method of software development where the model is designed, implemented and tested incrementally until the product is finished.

(b) The steps involved in the preliminary investigation phase of SDLC are Identification of Problem, Identification of objectives, Delineation of scope, and Feasibility Study.

(c) Decision Tree, Flowchart, Data Flow Diagrams and Structured English are some of the widely-used Fact finding Tools under System Requirement Analysis sub phase of Preliminary investigation in SDLC.

(d) Operations Manual is a technical communication document intended to give assistance to people using a particular system and is usually written by technical writers.

6. XYZ is a bank that has association with two different service providers as their payment gateways. Mr. A is appointed as an auditor for XYZ bank. He is checking and auditing the details of online payments made by different users and third party customers. He is checking for material theft and unauthorized modification. Which type of risk he is working on?

(a) Control Risk

(b) Detection Risk

(c) Online payment risk

(d) Inherent risk

7. In Information TechnologyAct, 2000; Section 73 deals with ___________.

    (a) Penalty for misinterpretation

    (b) Penalty for breach of confidentiality and privacy

    (c) Penalty for publishing electronic signature certificate false in certain particulars

    (d) Protected system

8. The IT department of XYZ organization wants to make use of its infrastructure resources optimally within its boundaries by provisioning the infrastructure with application using concepts of grid and virtualization. Which of the following Cloud computing environment the organization is opting for?

    (a) Private Cloud

    (b) Hybrid Cloud

    (c) Public Cloud

    (d) Community Cloud

DESCRIPTIVE QUESTIONS

Chapter 1: Concepts of Governance and Management of Information Systems

9. Define Corporate Governance and discuss its best practices.

10. You are appointed as a functional head of IT Department and are a member of IT Steering Committee also. The IT Steering Committee provides overall direction to deployment of IT and information systems in the enterprises. Discuss its key functions.

Chapter 2: Information System Concepts

11. You have sent an electronic mail (e-mail) to one of your friend who is a non-technical person. Through your email, you want to make him understand the features provided by e-mail. What would be the features of e-mail that you would highlight upon?

12. Nowadays; Financial, wholesaling and retailing and public sectors etc. are moving towards a real-time business model where transaction and information sharing are near instantaneous. What do you think are the impacts of Information Technology (IT) on Information Systems of these different sectors?

Chapter 3: Protection of Information Systems

13. Every organization maintains a document that describes its information security controls and activities. Identify the document and discuss it in detail.

14. Operations management is responsible for the daily running of hardware and software facilities in an organization. Discuss the different controls performed by Operations management on different functions.

Chapter 4: Business Continuity Planning and Disaster Recovery Planning

15. What do you understand by the term "Business Impact Analysis(BIA)"? Explain in detail.

16. Discuss the key areas that are emphasized upon in any Disaster Recovery Planning (DRP) document of an organization.

Chapter 5: Acquisition, Development and Implementation of Information Systems

17. "Achieving the objectives of the system development is essential but many times, such objectives are not achieved as desired". List down the various User-related and Developer-related issues that may arise and hinder in achieving the desired results.

18. Integration Testing is an activity of software testing under System Testing phase of System Development Life Cycle (SDLC) in which individual software modules are combined and tested as a group. Discuss the different techniques of Integration Testing.

Chapter 6: Auditing of Information Systems

19. Continuous auditing enables auditors to shift their focus from the traditional "transaction" audit to the "system and operations" audit for which an auditor uses continuous audit techniques to perform the audit. Discuss the advantages as well as limitations of continuous audit techniques.

20. Discuss the Audit Trails under Programming Management Controls of Managerial Controls.

Chapter 7: Information Technology Regulatory Issues

21. Describe the section of Information Technology Act, 2000 that defines the "Power to make rules by Central Government in respect of Electronic Signature".

22. Before proceeding with the audit, which type of the information an auditor is expected to obtain at the audit location?

Chapter 8: Emerging Technologies

23. You are supposed to make a presentation on the working of Mobile Computing. What will be the content of your presentation?

24. Any Bring Your Own Device (BYOD) program that allows access to corporate network, emails, client data etc.; is one of the top security concerns for enterprises. Discuss various risks associated with BYOD.

Questions based on Case Study

25. ABC is the coffee-house having its chain outlets in many countries with their main server residing in California, USA. Mr. A, is one of the regular client of the coffeehouse outlet in Guruguram, India who visits the outlet on daily basis. Being a regular customer, the outlet privileges Mr. A with a premium customer card that offers him 10% discount on every bill across globe.

    One day, on Mr. A's visit to one of the coffee-house outlets in California, USA; he realises that the said premium card provided to him by the ABC coffee-house is invalid. On inquiring, he was made to understand that due to the earthquake in the city, the main server had been severely damaged and the link between their Information systems and the main Server has been suspended temporarily. The data residing on the main server was permanently lost as there was no back up policy that was adapted by the coffee-house.

    (a) Explain the various types of data back-ups that coffee-house should have taken up to prevent the loss of data.

    (b) ABC coffee-house wants to develop a software for the protection of its data of customer. The IT head of the company is under the process of testing of whole software. Discuss different testing techniques that IT head can adopt to test the software as whole.

    (c) The coffee-house decided to adapt cloud computing for future reference. Explain in detail the issues related to Implementation and adaption of Cloud Computing.

SUGGESTED ANSWERS/HINTS

MULTIPLE CHOICE ANSWERS

1. **(d)** I, II, III

2. **(a)** Expert System

3. **(d)** Detective Control

4. **(a)** Pre-planning Activities

5. **(c)** Decision Tree, Flowchart, Data Flow Diagrams and Structured English are some of the widely-used Fact finding Tools under System Requirement Analysis sub phase of Preliminary investigation in SDLC.

6. **(d)** Inherent Risk

7. **(c)** Penalty for publishing electronic signature certificate false in certain particulars

8. **(a)** Private Cloud

DESCRIPTIVE ANSWERS

9. Corporate Governance has been defined as the system by which business corporations are directed and controlled. The corporate governance structure specifies the distribution of rights and responsibilities among different participants in the corporation, such as, the Board, managers, shareholders and other stakeholders, and spells out the rules and procedures for making decisions on corporate affairs. Some of the best practices of corporate governance include the following:

- Clear assignment of responsibilities and decision-making authorities, incorporating a hierarchy of required approvals from individuals to the Board of Directors;
- Establishment of a mechanism for the interaction and cooperation among the board of directors, senior management and the auditors;
- Implementing strong internal control systems, including internal and external audit functions, risk management functions independent of business lines, and other checks and balances;
- Special monitoring of risk exposures where conflicts of interest are likely to be particularly great, including business relationships with borrowers affiliated with the bank, large shareholders, senior management, or key decision-makers within the firm (e.g. traders);
- Financial and managerial incentives to act in an appropriate manner offered to senior management, business line management and employees in the form of compensation, promotion and other recognition; and
- Appropriate information flows internally and to the public. For ensuring good corporate governance, the importance of overseeing the various aspects of the corporate functioning needs to be properly understood, appreciated and implemented.

10. The key functions of the IT Steering committee would include 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.

11. Various features of electronic mail (e-mail) are stated below:

- **Electronic Transmission-** The transmission of messages with email is electronic and message delivery is very quick, almost instantaneous. The confirmation of transmission is also quick and the reliability is very high.
- **Online Development and Editing -** The email message can be developed and edited online before transmission. The online development and editing eliminates the need for use of paper in communication. It also facilitates the storage of messages on magnetic media, thereby reducing the space required to store the messages.
- **Broadcasting and Rerouting** – e-mail permits sending a message to many target recipients. Thus, it is easy to send a circular to all branches of a bank using Email resulting in a lot of paper saving. The email could be rerouted to people having direct interest in the message with or without changing or and appending related information to the message.
- **Integration with other Information Systems** - The e-mail has the advantage of being integrated with the other information systems. Such integration helps in ensuring that the message is accurate and the information required for the message is accessed quickly.
- **Portability –** e-mail renders the physical location of the recipient and sender irrelevant. The email can be accessed from any Personal computer/tablet/smart phones equipped with the relevant communication hardware, software and link facilities.
- **Economical –** The e-mail is one of the most economical mode for sending and receiving messages. Since the speed of transmission is increasing, the time cost on communication media per page is falling further, adding to the popularity of email. The email is proving to be very helpful not only for formal communication but also for informal communication within the enterprise.

12. The impact of Information Technology (IT) on Information Systems of different sectors is explained below:

(i) **E-business –** This is also called electronic business and includes purchasing, selling, production management, logistics, communication, support services and inventory management using internet technologies. The primary components of E-business are infrastructure (computers, routers, communication media e.g. wire, satellite etc., software and programmers), electronic commerce and electronically linked devices and computer aided networks. The advantages of E-business are - 24 hour sale, lower cost of doing business, more efficient business relationship, eliminate middlemen, unlimited market place and access with broaden customer base, secure payment systems, easier business administration and online fast updating. This is so because it does not require land for store or shops and anyone from anywhere can do business anytime as information regarding products etc. is available on the web. Only investment is needed in the purchase of space on internet, designing and maintenance of website. Different types of business can be done e.g. it may be B2B (Business to Business), B2C (Business to Customer), C2C (Customer to Customer) and C2B (Customer to Business). Because of no limitations of time and space, people prefer to involve in E-business. Thus, we can say that IT has given new definition to business.

(ii) Financial Service Sector – The financial services sector (banks, building societies, life insurance companies and short term insurers) manages large amounts of data and processes enormous numbers of transactions every day. Owing to application of IT, all the major financial institutions operate nationally and have wide networks of regional offices and associated electronic networks. The associated substantial client databases are handled via large central mainframe systems that characterize the industry. IT has changed the working style of financial services and makes them easier and simpler for customers also. Now-a-days most of the services are offered by the financial services on internet, which can be accessed from anywhere and anytime that makes it more convenient to the customers. It also reduces their cost in terms of office staff and office building. It has been observed that automated and IT enabled service sectors reduces cost effectively. Through the use of internet and mobile phones; financial service sectors are in direct touch with their customers and with adequate databases it will be easier for service sectors to manage customer relationships. For example, through emails or SMS the customers can be made aware of launch of new policies; they can be informed on time the day of maturity of their policies etc.

In traditional banking system, the customer has to visit bank branch to deposit or withdraw money and get updated passbook from the respective counter. With the advancement of IT, the customer can do transactions by using internet banking, phone banking and the deposit or withdraw of money can also be done by using ATM (Automatic Teller Machine), internet or mobile banking. Banks also offers most of direct banking services free of charge to the customers. The customers can check the status of their accounts in different banks by using of direct banking. Retail banking in India has assured great importance recently with a number of retail banking products available to the consumer like real time account status, transfer of funds, bill payments and so on e.g. HDFC, SBI and ICICI are the banks in India that offer real time online transactions etc.

(iii) Wholesaling and Retailing – Retail business uses IT to carry out basic functions including systems for selling items, capturing the sales data by item, stock control, buying, management reports, customer information and accounting. The laser scanners used in most grocery supermarkets and superstores to read product bar codes are among the most distinctive examples of modern computer technology. By using internet or mobile phones retailers can collect and exchange data between stores, distribution centres, suppliers and head offices.

IT can be used in wholesale for supply chain logistics management, planning, space management, purchasing, re-ordering, and analysis of promotions. Data mining and data warehousing applications helps in the analysis of market baskets, customer profiles and sales trends. E-commerce among partners (suppliers, wholesalers, retailers, distributors) helps in carrying out transactions.

(iv) Public sectors – It includes services provided by the government mainly hospitals, police stations, universities etc. IT/IS can be used here, to keep records of the cases, respective people involved it, other related documents and can consult the existing data warehouse or databases to take appropriate actions. For example, IS like ERP can be implemented in a university to keep record of its employees in terms of their designation, leaves availed, department, achievements that can be used further in analysing their performance. Owing to application of IT and IS, it becomes easy to file FIR of a case without going to police station personally and also important documents like passports can be made easily by applying online.

(v) Others – IT is efficiently used in entertainment industry (games, picture collection etc.), agriculture industry (information is just a mouse click away to the farmers), Tour industry (railway, hotel and airline reservations) and consultancy etc.

Thus, we can say that IT has changed the working style of business world drastically and make it simpler day-by-day with its advancement.

13. An **Information Security Policy** is a document that describes an organization's information security controls and activities. It is defined as the statement of intent by the management about how to protect a company's information assets. It is a formal statement of the rules, which give access to people to an organization's technology and information assets, and which they must abide.

- The policy does not specify technologies or specific solutions; it defines a specific set of intentions and conditions that help protect a company's information assets and its ability to conduct business. An Information Security Policy is the essential foundation for an effective and comprehensive information security program.
- It is the primary way in which management's information security concerns are translated into specific measurable and testable goals and objectives. It provides guidance to the people, who build, install, and maintain information systems. Information Security policy invariably includes rules intended to:
  - Preserve and protect information from any unauthorized modification, access or disclosure;
  - Limit or eliminate potential legal liability from employees or third parties; and
  - Prevent waste or inappropriate use of the resources of an organization.
- An information security policy should be in written form. It provides instructions to employees about "what kinds of behavior or resource usage are required and acceptable", and about "what is unacceptable".
- An Information Security policy also provides direction to all employees about how to protect organization's information assets, and instructions regarding acceptable (and unacceptable) practices and behavior.
- The policy does not need to be extremely extensive, but clearly state senior management's commitment to information security, be under change and version control and be signed by the appropriate senior manager. The policy should at least address the following issues:
  - a definition of information security,
  - reasons why information security is important to the organization, and its goals and principles,
  - a brief explanation of the security policies, principles, standards and compliance requirements,
  - definition of all relevant information security responsibilities; and
  - reference to supporting documentation.

  The auditor should ensure that the policy is readily accessible to all employees and that all employees are aware of its existence and understand its contents.

14. Operations management is responsible for the daily running of hardware and software facilities. Operations management typically performs controls over the functions as 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. The primary components in the communication sub-systems are given as follows:

- Communication lines viz. twisted pair, coaxial cables, fiber optics, microwave and satellite etc.
- **Hardware** – ports, modems, multiplexers, switches and concentrators etc.
- **Software** – Packet switching software, polling software, data compression software etc.
- Due to component failure, transmission between sender and receiver may be disrupted, destroyed or corrupted in the communication system.

(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 assists end-users to employ end-user hardware and software such as micro-computers, spreadsheet packages, database management packages etc. and provide 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. **Business Impact Analysis (BIA)** is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. The process of BIA determines and documents the impact of a disruption of the activities that support its key products and services. It enables the business continuity team to identify critical systems, processes and functions, assess the economic impact of incidents and disasters that result in a denial of access to the system, services and facilities, and assess the "pain threshold, "that is, the length of time business units can survive without access to the system, services and facilities. For each activity supporting the delivery of key products and services within the scope of its BCM program, the enterprise should:

- assess the impacts that would occur if the activity was disrupted over a period of time;
- identify the maximum time period after the start of a disruption within which the activity needs to be resumed;
- Identify critical business processes;
- assess the minimum level at which the activity needs to be performed on its resumption;
- identify the length of time within which normal levels of operation need to be resumed; and
- identify any inter-dependent activities, assets, supporting infrastructure or resources that have also to be maintained continuously or recovered over time.

The enterprise should have a documented approach to conduct BIA. The enterprise should document its approach to assessing the impact of disruption and its findings and conclusions. The BIA Report should be presented to the Top Management. This report identifies critical service functions and the time frame 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. Developing the BCP also takes into account the BIA process.

16. The Disaster Recovery Planning (DRP) document may include the following areas:

- The conditions for activating the plans, which describe the process to be followed before each plan, are activated.
- Emergency procedures, which describe the actions to be taken following an incident which jeopardizes business operations and/or human life. This should include arrangements for public relations management and for effective liaisoning with appropriate public authorities e.g. police, fire, services and local government.
- Fall-back procedures, which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time-scale.
- Resumption procedures, which describe the actions to be taken to return to normal business operations.
- A maintenance schedule, which specifies, how and when the plan will be tested", and the process for maintaining the plan.
- Awareness and education activities, which are designed to create an understanding of the business continuity, process and ensure that the business continues to be effective.
- The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
- Contingency plan document distribution list.
- Detailed description of the purpose and scope of the plan.
- Contingency plan testing and recovery procedure.
- List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
- Checklist for inventory taking and updating the contingency plan on a regular basis.
- List of phone numbers of employees in the event of an emergency.
- Emergency phone list for fire, police, hardware, software, suppliers, customers, back-up location, etc.
- Medical procedure to be followed in case of injury.
- Back-up location contractual agreement, correspondences.
- Insurance papers and claim forms.

- Primary computer center hardware, software, peripheral equipment and software configuration.
- Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
- Alternate manual procedures to be followed such as preparation of invoices.
- Names of employees trained for emergency situation, first aid and life saving techniques.
- Details of airlines, hotels and transport arrangements.

17. Various User-related and Developer-related issues are as follows:

User Related Issues: It refers to those issues where user/customer is reckoned as the primary agent. Some of the aspects with regard to this problem are mentioned as follows:

- **Shifting User Needs:** User requirements for IT are constantly changing. As these changes accelerate, there will be more requests for Information systems development and more development projects. When these changes occur during a development process, the development team faces the challenge of developing systems whose very purpose might change since the development process began.
- **Resistance to Change:** People have a natural tendency to resist change, and information systems development projects signal changes - often radical - in the workplace. When personnel perceive that the project will result in personnel cutbacks, threatened personnel will dig in their heels, and the development project is doomed to failure.
- **Lack of Users' Participation:** Users must participate in the development efforts to define their requirements, feel ownership for project success, and work to resolve development problems. User participation also helps to reduce user resistance to change.
- **Inadequate Testing and User Training:** New systems must be tested before installation to determine that they operate correctly. Users must be trained to effectively utilize the new system.

Developer Related Issues: It refers to the issues and challenges regarding the developers. Some of the critical bottlenecks are mentioned as follows:

- **Lack of Standard Project Management and System Development Methodologies:** Some organizations do not formalize their project management and system development methodologies, thereby making it very difficult to consistently complete projects on time or within budget.
- **Overworked or Under-Trained Development Staff:** In many cases, system developers **often** lack sufficient educational background and requisite state of the art

skills. Furthermore, many companies do a little to help their development personnel stay technically sound, and more so a training plan and training budget do not exist.

18. Integration testing is an activity of software testing in which individual software modules are combined and tested as a group. It occurs after unit testing and before system testing with an objective to evaluate the validity of connection of two or more components that pass information from one area to another. Integration testing takes as its input modules that have been unit tested, groups them in larger aggregates, applies tests defined in an integration test plan to those aggregates, and delivers as its output the integrated system ready for system testing. This is carried out in the following two manners:

- **Bottom-up Integration:** It is the traditional strategy used to integrate the components of a software system into a functioning whole. It consists of unit testing, followed by sub-system testing, and then testing of the entire system. Bottom-up testing is easy to implement as at the time of module testing, tested subordinate modules are available. The disadvantage, however is that testing of major decision / control points is deferred to a later period.
- **Top-down Integration:** It starts with the main routine, and stubs are substituted, for the modules directly subordinate to the main module. An incomplete portion of a program code that is put under a function to allow the function and the program to be compiled and tested, is referred to as a stub. A stub does not go into the details of implementing details of the function or the program being executed.

  Once the main module testing is complete, stubs are substituted with real modules one by one, and these modules are tested with stubs. This process continues till the atomic modules are reached. Since decision-making processes are likely to occur in the higher levels of program hierarchy, the top-down strategy emphasizes on major control decision points encountered in the earlier stages of a process and detects any error in these processes. The difficulty arises in the top-down method, because the high-level modules are tested, not with real outputs from subordinate modules, but from stubs.

19. Some of the advantages of continuous audit techniques are given as under:

- **Timely, Comprehensive and Detailed Auditing -** Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analyzed rather than examining the inputs and the outputs only.
- **Surprise test capability -** As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.

- **Information to system staff on meeting of objectives -** Continuous audit **techniques** provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
- **Training for new users -** Using the ITFs, new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

The following are some limitations of the use of the continuous audit techniques:

- Auditors should be able to obtain resources required from the organization to support development, implementation, operation, and maintenance of continuous audit techniques.
- Continuous audit techniques are more likely to be used if auditors are involved in the development work associated with a new application system.
- Auditors need the knowledge and experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.
- Continuous auditing techniques are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.

20. Audit Trails under Programming Management Controls of Managerial Controls are as follows:

(a) Planning

- They should evaluate whether the nature of and extent of planning are appropriate to the different types of software that are developed or acquired.
- They must evaluate how well the planning work is being undertaken.

(b) Control

- They must evaluate whether the nature of and extent of control activities undertaken are appropriate for the different types of software that are developed or acquired.
- They must gather evidence on whether the control procedures are operating reliably. For example - they might first choose a sample of past and current software development and acquisition projects carried out at different locations in the organization they are auditing.

(c) Design

- Auditors should find out whether programmers use some type of systematic approach to design.

- Auditors can obtain evidence of the design practices used by undertaking interviews, observations, and reviews of documentation.

(d) Coding

- Auditors should seek evidence –
  - On the level of care exercised by programming management in choosing a module implementation and integration strategy.
  - To determine whether programming management ensures that programmers follow structured programming conventions.
  - To check whether programmers employ automated facilities to assist them with their coding work.

(e) Testing

- Auditors can use interviews, observations, and examination of documentation to evaluate how well unit testing is conducted. Auditors are most likely concerned primarily with the quality of integration testing work carried out by information systems professionals rather than end users.
- Auditor's primary concern is to see that whole-of-program tests have been undertaken for all material programs and that these tests have been well-designed and executed.

(f) Operation and Maintenance

- Auditors need to ensure effectively and timely reporting of maintenance needs occurs and maintenance is carried out in a well-controlled manner.
- Auditors should ensure that management has implemented a review system and assigned responsibility for monitoring the status of operational programs.

21. Section 10 of the Information Technology Act, 2000 defines the Power to make rules by Central Government in respect of Electronic Signature.

[Section 10] Power to make rules by Central Government in respect of Electronic Signature

The Central Government may, for the purposes of this Act, by rules, prescribe

(a) the type of Electronic Signature;

(b) the manner and format in which the Electronic Signature shall be affixed;

(c) the manner or procedure which facilitates identification of the person affixing the Electronic Signature;

(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to Electronic Signature.

22. Before proceeding with the audit, the auditor is expected to obtain the following information at the audit location:

- Location(s) from where Investment activity is conducted.
- IT Applications used to manage the Insurer's Investment Portfolio.
- Obtain the system layout of the IT and network infrastructure including: Server details, database details, type of network connectivity, firewalls other facilities/ utilities (describe).
- Are systems and applications hosted at a central location or hosted at different office?
- Previous Audit reports and open issues / details of unresolved issues from:
  - Internal Audit,
  - Statutory Audit, and
  - IRDA Inspection / Audit.
- Internal circulars and guidelines of the Insurer.
- Standard Operating Procedures (SOP).
- List of new Products/funds introduced during the period under review along with Insurance Regulatory and Development Authority of India (IRDA) approvals for the same.
- Scrip wise lists of all investments, fund wise, classified as per IRDA Guidelines, held on date.
- IRDA Correspondence files, circulars and notifications issued by IRDA.
- IT Security Policy.
- Business Continuity Plans.
- Network Security Reports pertaining to IT Assets.

23. The working of Mobile Computing is as follows:

- The user enters or access data using the application on handheld computing device.
- Using one of several connecting technologies, the new data are transmitted from handheld device to site's information system where files are updated and the new data are accessible to other system user.

- Now both systems (handheld and site's computer) have the same information and are in sync.
- The process work the same way starting from the other direction.

The process is similar to the way a worker's desktop PC access the organization's applications, except that user's device is not physically connected to the organization's system. The communication between the user device and site's information systems uses different methods for transferring and synchronizing data, some involving the use of Radio Frequency (RF) technology.

24. Every business decision is accompanied with a set of threats and so is BYOD program too; it is not immune from them. As outlined in the Gartner survey, a BYOD program that allows access to corporate network, emails, client data etc. is one of the top security concerns for enterprises. Overall, these risks can be classified into four areas as outlined below:

- **Network Risks:** It is normally exemplified and hidden in "Lack of Device Visibility". When company-owned devices are used by all employees within an organization, the organization's IT practice has complete visibility of the devices connected to the network. This helps to analyze traffic and data exchanged over the Internet. As BYOD permits employees to carry their own devices (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the network. As network visibility is of high importance, this lack of visibility can be hazardous. For example, if a virus hits the network and all the devices connected to the network need be scanned, it is probable that some of the devices would miss out on this routine scan operation. In addition to this, the network security lines become blurred when BYOD is implemented.
- **Device Risks:** It is normally exemplified and hidden in "Loss of Devices". A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information. Data lost from stolen or lost devices ranks as the top security threats as per the rankings released by Cloud Security Alliance. With easy access to company emails as well as corporate intranet, company trade secrets can be easily retrieved from a misplaced device.
- **Application Risks:** It is normally exemplified and hidden in **"**Application Viruses and Malware". A related report revealed that most employees' phones and smart devices that were connected to the corporate network weren't protected by security software. With an increase in mobile usage, mobile vulnerabilities have increased concurrently. Organizations are not clear in deciding that "who is responsible for device security – the organization or the user".
- **Implementation Risks:** It is normally exemplified and hidden in "Weak BYOD Policy". The effective implementation of the BYOD program should not only cover the technical issues mentioned above but also mandate the development of a robust

implementation policy. Because corporate knowledge and data are key assets of an organization, the absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse. In addition to this, a weak policy fails to educate the user, thereby increasing vulnerability to the above-mentioned threats.

25. **(a)** Various types of data back-ups are as follows:

(i) **Full Backup:** A Full Backup captures all files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the backup set. At each backup run, all files designated in the backup job will be backed up again. This includes files and folders that have not changed. It is commonly used as an initial or first backup followed with subsequent incremental or differential backups. After several incremental or differential backups, it is common to start over with a fresh full backup again. Some also like to do full backups for all backup runs typically for smaller folders or projects that do not occupy too much storage space. The Windows operating system lets us to copy a full backup on several DVD disks. Any good backup plan has at least one full backup of a server.

(ii) **Incremental Backup:** An Incremental Backup captures files that were created or changed since the last backup, regardless of backup type. The last backup can be a full backup or simply the last incremental backup. With incremental backups, one full backup is done first and subsequent backup runs are just the changed files and new files added since the last backup.

(iii) **Differential Backup:** Differential backups fall in the middle between full backups and incremental backup. A Differential Backup stores files that have changed since the last full backup. With differential backups, one full backup is done first and subsequent backup runs are the changes made since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up. Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved. Restoring from a differential backup is a two-step operation: Restoring from the last full backup; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup probably includes files that were already included in earlier differential backups.

(iv) **Mirror back-up:** Mirror backups are, as the name suggests, a mirror of the source being backed up. With mirror backups, when a file in the source is deleted, that file is eventually also deleted in the mirror backup. Because of this, mirror backups should be used with caution as a file that is deleted by accident, sabotage or through a virus may also cause that same file in mirror to be deleted as well. Some do not consider a mirror to be a backup. Further, a mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

(b) **System Testing:** It is a process in which software and other system elements are tested as a whole. System testing begins either when the software as a whole is operational or when the well-defined subsets of the software's functionality have been implemented. The purpose of system testing is to ensure that the new or modified system functions properly. These test procedures are often performed in a non-production test environment. The types of testing that might be carried out are as follows:

- **Recovery Testing:** This is the activity of testing „how well the application is able to recover from crashes, hardware failures and other similar problems". Recovery testing is the forced failure of the software in a variety of ways to verify that recovery is liable to be properly performed, in actual failures.
- **Security Testing**: This is the process to determine that an Information System protects data and maintains functionality as intended or not. The six basic security concepts that need to be covered by security testing are – confidentiality, integrity, availability authentication, authorization, and non-repudiation. This testing technique also ensures the existence and proper execution of access controls in the new system.
- **Stress or Volume Testing**: Stress testing is a form of testing that is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results. Stress testing may be performed by testing the application with large quantity of data during peak hours to test its performance.
- **Performance Testing:** In the computer industry, software performance testing is used to determine the speed or effectiveness of a computer, network, software program or device. This testing technique compares the new system's performance with that of similar systems using well defined benchmarks.

(c) Some of the well-identified implementation issues of Cloud Computing are as follows:

- **Threshold Policy:** In order to test if the program works, develops, or improves and implements; a threshold policy is of immense importance in a pilot study before moving the program to the production environment. This involves the checking how the policy enables to detect sudden increases in the demand and results in the creation of additional instances to fill in the demand. Moreover, to determine how unused resources are to be de-allocated and turned over to other work needs to work out in the context. That is working out thresholds is really a matter of concern and would go a long way to assure the effectiveness. Let's suppose, we had a program that did credit card validation in the cloud, and we hit the crunch for the buying season. Higher demand would be detected and more instances would be created to fill that demand. As we moved out of the buying crunch, the need would be diminished and the instances of those resources would be de-allocated and put to other use.

- **Interoperability**: If a company outsources or creates applications with one cloud computing vendor, the company may find it difficult to change to another computing vendor that has proprietary Application Programming Interfaces (APIs) and different formats for importing and exporting data. This creates problems of achieving interoperability of applications between two cloud computing vendors. We may need to reformat/reorganize data or change the logic in applications. Although industry cloud computing standards do not exist for APIs or data import/export; IBM and Amazon Web Services have worked together to make interoperability happen.
- **Hidden Costs**: Like any such services in prevailing business systems, cloud computing service providers do not reveal “what hidden costs are”. For instance, companies could incur higher network charges from their service providers for storage and database applications containing terabytes of data in the cloud. This outweighs costs they could save on new infrastructure, training new personnel, or licensing new software. In another instance of incurring network costs, companies, who are far from the location of cloud providers, could experience latency, particularly when there is heavy traffic.
- **Unexpected Behavior**: It is important to test the application in the cloud with a pilot study to check for unexpected behavior. Examples of tests include how the application validates credit cards, and how, in the scenario of the buying crunch, it allocates resources and releases unused resources, turning them over to other work. If the tests show unexpected results of credit card validation or releasing unused resources, we will need to fix the problem before executing or obtaining cloud services from the cloud. Instead of waiting for an outage to occur, consumers should do security testing on their own checking how well a vendor can recover data. Apart from the common testing practices, what one needs primarily to do is to ask for old stored data and check how long it takes for the vendor to recover. Another area of security testing is to test a trusted algorithm to encrypt the data on the local computer, and then try to access data on a remote server in the cloud using the decryption keys. If we can't read the data once we have accessed it, the decryption keys are corrupted, or the vendor is using its own encryption algorithm. We may need to address the algorithm with the vendor. Another issue is the potential for problems with data in the cloud. To protect the data, one may want to manage his/her own private keys. Checking with the vendor on the private key management is no longer a simple as it appears so.

- **Software Development in Cloud**: To develop software using high-end databases, the most likely choice is to use cloud server pools at the internal data corporate center and extend resources temporarily for testing purposes. This allows project managers to control costs, manage security and allocate resources to clouds for a project. The project managers can also assign individual hardware resources to different cloud types: Web development cloud, testing cloud, and production cloud. The cost associated with each cloud type may differ from one another. The cost per hour or usage with the development cloud is most likely lower than the production cloud, as additional features, such as Service-Level Agreements (SLA) and security, are allocated to the production cloud. The managers can limit projects to certain clouds. For instance, services from portions of the production cloud can be used for the production configuration. Services from the development cloud can be used for development purpose only. To optimize assets at varying stages of the project of software development, the managers can get cost-accounting data by tracking usage by project and user.
- **Environment Friendly Cloud Computing**: One incentive for cloud computing is that it may be more environment friendly. First, reducing the number of hardware components needed to run applications on the company's internal data center and replacing them with cloud computing systems reduces energy for running and cooling hardware. By consolidating these systems in remote centers, they can be handled more efficiently as a group.