## 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 Technology Act, 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.

## 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.

## PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

## QUESTIONS

### Concepts of Governance and Management of Information Systems

1. List out the key functions of the IT Steering Committee.
2. 'IT has to provide critical inputs to meet the information needs of all the stakeholders'. Define IT Governance and list out its benefits.
3. Briefly describe the key management practices provided by COBIT 5 for ensuring IT compliances.

### Information System Concepts

4. 'There are various constraints, which come in the way of operating a Management Information Systems (MIS)'. Explain any four such constraints in brief.
5. "A business manager should have adequate knowledge to operate Information Systems effectively". Elaborate this statement.
6. Discuss few examples of business applications of Expert Systems.

### Protection of Information Systems

7. Discuss Application and Monitoring System Access Controls.
8. Discuss some Financial Controls Techniques.
9. Discuss about User Access Resource Management Controls.

### Business Continuity Planning and Disaster Recovery Planning

10. Why do you think an organization needs to maintain a BCP Manual?
11. What does the methodology emphasize upon while developing a Business Continuity Plan (BCP)?
12. Explain the phase "Business Impact Assessment (BIA)" under Business Continuity plan methodology?

### Acquisition, Development and Implementation of Information Systems

13. Discuss the roles of the following during SDLC (System Development Life Cycle).
    (a) Steering Committee
    (b) Database Administrator
    (c) Project Leader
    (d) Information Systems (IS) Auditor

14. Discuss the activities involved during the System Designing phase under SDLC (Systems Development Life Cycle).
15. Discuss the categories of tests that a programmer performs on a program unit during the phase System Testing under System Development Life Cycle (SDLC).

**Auditing of Information Systems**

16. As an auditor, what do you think are the disadvantages and limitations of using Continuous Audit Techniques?
17. Discuss the types of Managerial Controls and their scope, in brief.
18. Discuss Boundary Controls and their Audit Trails under Application Controls.

**Information Technology Regulatory Issues**

19. Identify and explain the Section of IT Act, 2000; that explains the situation(s) under which any computer or computer resources shall become liable to confiscation?
20. What do you understand by the term "IT Infrastructure Library (ITIL)"? Discuss its volumes in brief.

**Emerging Technologies**

21. Under Green Computing, discuss guidelines to conserve energy?
22. Discuss the limitations of Mobile Computing.
23. Discuss different instances of Infrastructure as a Service (IaaS) model in Cloud Computing.

**Short Note Based Questions**

24. Write short notes on following:
    (a) COBIT Components
    (b) Benefits of Office Automation Systems (OAS)
    (c) Examples of Segregation of Duties (SoD)
    (d) Features of Agile Manifesto
    (e) Detection Risk

**Questions based on Case Study**

25. ABC is a company that provides tourism related services worldwide to its customers worldwide. Though its operations are all online, however, the current information infrastructure is not sufficient to sustain itself in the competitive environment. Thus, the management realizes that they need to develop a "Smart Tourism – IT infrastructure", which involves development of semantic based information system using Web 3.0 technologies, in cloud and mobile computing environment, for which a high-level IT

Steering Committee comprising IS Auditor as one of the members is appointed. The company also intends to develop a document for Disaster Recovery Plan after upgrading information infrastructure.

Read the above and answer the following questions:

(a) What are the main objectives that an organization can achieve through Information Systems Auditing?

(b) What are the various areas to be incorporated in the Disaster Recovery Planning Document? Indicate any ten such areas.

(c) What do you mean by Web 3.0 Technology? Explain briefly two major components of Web 3.0 technology.

## SUGGESTED ANSWERS/HINTS

**1.** 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 between IT and its users; and
- To report to the Board of Directors on IT activities on a regular basis.

**2.** **IT Governance:** IT Governance refers to the system in which directors of the enterprise evaluate, direct and monitor IT management to ensure effectiveness, accountability and compliance of IT.

Benefits of IT Governance are as follows:

- Increased value delivered through enterprise IT;
- Increased user satisfaction with IT services;

- Improved agility in supporting business needs;
- Better cost performance of IT;
- Improved management and mitigation of IT-related business risk;
- IT becoming an enabler for change rather than an inhibitor;
- Improved transparency and understanding of IT's contribution to the business;
- Improved compliance with relevant laws, regulations and policies; and
- More optimal utilization of IT resources.

**3.** COBIT 5 provides key management practices for ensuring IT compliance with external compliances as relevant to the enterprise. The practices are given as follows:

- **Identify External Compliance Requirements:** On a continuous basis, identify and monitor for changes in local and international laws, regulations, and other external requirements that must be complied with from an IT perspective.
- **Optimize Response to External Requirements:** Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated. Consider industry standards, codes of good practice, and best practice guidance for adoption and adaptation.
- **Confirm External Compliance:** Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual requirements.
- **Obtain Assurance of External Compliance:** Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.

**4.** Major constraints which come in the way of operating a Management Information System are as follows:

- Non-availability of experts, who can diagnose the objectives of the organization and provide a desired direction for installing operating system. This problem may be overcome by grooming internal staff, which should be preceded by proper selection and training.
- Experts usually face the problem of selecting the sub-system of MIS to be installed and operated upon. The criteria, which should guide the experts, depend upon the need and importance of a function for which MIS can be installed first.
- Due to varied objectives of business concerns, the approach adopted by experts for designing and implementing MIS is a non-standardized one.

- Non-availability of cooperation from staff is a crucial problem, which should be handled tactfully. This task should be carried out by organizing lecturers, showing films and also explaining to them the utility of the system. Besides this, some persons should also be involved in the development and implementation of the system.

**5.** To operate Information Systems (IS) effectively and efficiently, a business manager should have following knowledge about it:

- **Foundation Concepts –** It includes fundamental business, and managerial concepts e.g. 'what are components of a system and their functions', or 'what competitive strategies are required'.
- **Information Technologies (IT) –** It includes operation, development and management of hardware, software, data management, networks, and other technologies.
- **Business Applications –** It includes major uses of IT in business steps i.e. processes, operations, decision making, and strategic/competitive advantage.
- **Development Processes –** It comprise how end users and IS specialists develop and execute business/IT solutions to problems.
- **Management Challenges –** It includes 'how the function and IT resources are maintained' and utilized to attain top performance and build the business strategies.

**6.** Some of the business applications of Expert Systems are as follows:

- **Accounting and Finance -** It provides tax advice and assistance, helping with credit-authorization decisions, selecting forecasting models, providing investment advice.
- **Marketing -** It provides establishing sales quotas, responding to customer inquiries, referring problems to telemarketing centres, assisting with marketing timing decisions, determining discount policies.
- **Manufacturing -** It helps in determining whether a process is running correctly, analysing quality and providing corrective measures, maintaining facilities, scheduling job-shop tasks, selecting transportation routes, assisting with product design and faculty layouts.
- **Personnel -** It is useful in assessing applicant qualifications and assisting employees in filling out forms.
- **General Business -** It helps in assisting with project proposals, recommending acquisition strategies, educating trainees, and evaluating performance.

**7.** The Application and Monitoring System Access Controls are as follows:

- **Information access restriction:** The access to information is prevented by application specific menu interfaces, which limit access to system function. A user

can access only to those items, s/he is authorized to access. Controls are implemented on the access rights of users. For example, read, write, delete, and execute. And ensure that sensitive output is sent only to authorized terminals and locations.

- **Sensitive system isolation:** Based on the critical constitution of a system in an enterprise, it may even be necessary to run the system in an isolated environment.

  Monitoring system access and use is a detective control, to check if preventive controls discussed so far are working. If not, this control will detect and report any unauthorized activities.

- **Event logging:** In Computer systems, it is easy and viable to maintain extensive logs for all types of events. It is necessary to review if logging is enabled and the logs are archived properly. An intruder may penetrate the system by trying different passwords and user ID combinations. All incoming and outgoing requests along with attempted access should be recorded in a transaction log. The log should record the user ID, the time of the access and the terminal location from where the request has been originated.

- **Monitor system use:** Based on the risk assessment, a constant monitoring of some critical systems is essential. Define the details of types of accesses, operations, events and alerts that will be monitored. The extent of detail and the frequency of the review would be based on criticality of operation and risk factors. The log files are to be reviewed periodically and attention should be given to any gaps in these logs.

- **Clock synchronization:** Event logs maintained across an enterprise network plays a significant role in correlating an event and generating report on it. Hence, the need for synchronizing clock time across the network as per a standard time is mandatory.

**8.** Financial Controls are generally defined as the procedures exercised by the system user personnel over source, or transactions origination, documents before system input. Some examples of financial control techniques are as below:

- **Authorization:** This entails obtaining the authority to perform some act typically accessing to such assets as accounting or application entries.

- **Budgets:** These estimates of the amount of time or money expected to be spent during a particular period, project, or event. The budget alone is not an effective control. Budgets must be compared with the actual performance, including isolating differences and researching them for a cause and possible resolution.

- **Cancellation of documents:** This marks a document in such a way to prevent its reuse. This is a typical control over invoices marking them with a “paid” or “processed” stamp or punching a hole in the document.

- **Dual control:** This entails having two people simultaneously access an asset. For example, the depositories of banks’ 24-hour teller machines should be accessed and

emptied with two people present, many people confuse dual control with dual access, but these are distinct and different. Dual access divides the access function between two people: once access is achieved, only one person handles the asset. With teller-machines, for example, two tellers would open the depository vault door together, but only one would retrieve the deposit envelopes.

- **Input/ Output verification:** This entails comparing the information provided by a computer system to the input documents. This is an expensive control that tends to be over-recommended by auditors. It is usually aimed at such non-monetary by dollar totals and item counts.
- **Safekeeping:** This entails physically securing assets, such as computer disks, under lock and key, in a desk drawer, file cabinet storeroom, or vault.
- **Sequentially numbered documents:** These are working documents with pre-printed sequential numbers, which enables the detection of missing documents.

**9.** The User Access Resource Management Controls are as follows:

- **User Registration:** Information about every user is documented. The following questions are to be answered:
  - Why is the user granted the access?;
  - Has the data owner approved the access?; and
  - Has the user accepted the responsibility? etc. The de-registration process is also equally important.
- **Privilege management:** Access privileges are to be aligned with job requirements and responsibilities. For example, an operator at the order counter shall have direct access to order processing activity of the application system. S/he will be provided higher access privileges than others. However, misuse of such privileges could endanger the organization's information security. These privileges are to be minimal with respect to their job functions.
- **User password management:** Passwords are usually the default screening point for access to systems. Allocations, storage, revocation, and reissue of password are password management functions. Educating users is a critical component about passwords, and making them responsible for their password.
- **Review of user access rights:** A user's need for accessing information changes with time and requires a periodic review of access rights to check anomalies in the user's current job profile, and the privileges granted earlier.

**10.** An incident or disaster affecting critical business operations can strike at any time. Successful organizations need to maintain a comprehensive BCP Manual, which ensures process readiness, data and system availability to ensure business continuity. A BCP manual is a documented description of actions to be taken, resources to be used and

procedures to be followed before, during and after an event that severely disrupts all or part of the business operations.

- The BCP is expected to anticipate various types of incident or disaster scenarios and provide reasonable assurance to senior management of enterprise about the capability of the enterprise to recover from any unexpected incident or disaster affecting business operations and continue to provide services with minimal impact.
- The BCP Manual is expected to specify the responsibilities of the BCM team, whose mission is to establish appropriate BCP procedures to ensure the continuity of enterprise's critical business functions. In the event of an incident or disaster affecting any of the functional areas, the BCM Team serves as liasioning teams between the functional area(s) affected and other departments providing support services.

**11.** The methodology for developing a Business Continuity Plan (BCP) can be sub-divided into eight different phases; the extent of applicability of each phase must be tailored to the respective organization. The methodology emphasizes on the following:

- Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
- Obtaining commitment from appropriate management to support and participate in the effort;
- Defining recovery requirements from the perspective of business functions;
- Documenting the impact of an extended loss to operations and key business functions;
- Focusing appropriately on disaster prevention and impact minimization, as well as orderly recovery;
- Selecting business continuity teams that ensure the proper balance required for plan development;
- Developing a business continuity plan that is understandable, easy to use and maintain; and
- Defining how business continuity considerations must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.

**12.** The Phase "Business Impact Assessment (BIA)" under Business Continuity Plan methodology enables the project team to:

- identify critical systems, processes and functions;
- assess the economic impact of incidents and disasters that result in a denial of access to systems services and other services and facilities; and

- assess the "pain threshold," that is, the length of time business units can survive without access to systems, services and facilities.

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

**13. (a) Steering Committee:** It is a special high power committee of experts to accord approvals for go-ahead and implementations. Some of the functions of Steering Committee are as follows:

- To provide overall directions and ensures appropriate representation of affected parties;
- To be responsible for all cost and timetables;
- To conduct a regular review of progress of the project in the meetings of steering committee, which may involve co-ordination and advisory functions; and
- To undertake corrective actions like rescheduling, re-staffing, change in the project objectives and need for redesigning.

**(b) Database Administrator:** The data in a database environment has to be maintained by a specialist in database administration so as to support the application program. The DBA handles multiple projects; ensures the integrity and security of information stored in the database and also helps the application development team in database performance issues. Inclusion of new data elements has to be done only with the approval of the database administrator.

**(c) Project Leader:** The project leader is dedicated to a project, who has to ensure its completion and fulfillment of objectives. S/he reviews the project status more frequently than a Project Manager and the entire project team reports to him/her.

**(d) Information Systems (IS) Auditor:** As a member of the team, IS Auditor ensures that the application development also focuses on the control perspective. S/he should be involved at the Design Phase and the final Testing Phase to ensure the existence and the operations of the Controls in the new software.

**14.** The System Designing phase under System Development Life Cycle (SDLC) include activities - Architectural Design; Design of the Data / Information Flow; Design of the Database; Design of the User-interface; Physical Design; and Design and acquisition of the hardware/system software platform', which are described briefly as follows:

- **Architectural Design:** Architectural design deals with the organization of applications in terms of hierarchy of modules and sub-modules. At this stage, we identify major modules; functions and scope of each module; interface features of each module; modules that each module can call directly or indirectly and Data received from / sent to / modified in other modules.
- **Design of Data/Information flow:** The design of the data and information flow is a major step in the conceptual design of the new system. In designing the data / information flow for the proposed system, the inputs that are required are - existing data / information flows, problems with the present system, and objective of the new system. All these have been identified in the analysis phase and documented in Software Requirements Specification (SRS).
- **Design of Database:** Design of the database involves determining its scope ranging from local to global structure. The scope is decided based on interdependence among organizational units. Conceptual Modeling, Data Modeling, Storage Structure Design and Physical Layout Design are the major activities involved in this activity.
- **User Interface Design:** It involves determining the ways in which users will interact with a system. The points that need to be considered while designing the user interface are - source documents to capture raw data, hard-copy output reports, screen layouts for dedicated source-document input, inquiry screens for database interrogation, graphic and color displays, and requirements for special input/output device.
- **Physical Design:** For the physical design, the logical design is transformed into units, which in turn can be decomposed further into implementation units such as programs and modules. During physical design, the primary concern of the auditor is effectiveness and efficiency issues. Some of the issues addressed here are type of hardware for client application and server application, Operating systems to be used, type of networking, processing – batch – online, real – time; frequency of input, output; and month-end cycles / periodical processing.
- **System's Operating Platform:** In some cases, the new system requires an operating platform including hardware, network and system software not currently available in an organization. For example – a DSS might require high-quality graphics output not supported by the existing hardware and software. The new hardware/system software platform required to support the application system will then have to be designed for requisite provisions.
- **Internal Design Controls:** From internal control point of view, this phase is also an important phase as all internal controls are placed in system during this phase. The key control aspects at this stage include some concerns like - Whether all control aspects have been properly covered?; Whether controls put in place in system, appear in the documentation done at this stage?; and Whether a separate review of design document has been done by internal auditor?

**15.** There are five categories of tests that a programmer typically performs on a program unit. Such typical tests are described as follows:

- **Functional Tests:** Functional Tests check 'whether programs do, what they are supposed to do or not'. The test plan specifies operating conditions, input values, and expected results, and as per this plan, programmer checks by inputting the values to see whether the actual result and expected result match.
- **Performance Tests:** Performance Tests should be designed to verify the response time, the execution time, the throughput, primary and secondary memory utilization and the traffic rates on data channels and communication links.
- **Stress Tests:** 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. These tests are designed to overload a program in various ways. The purpose of a stress test is to determine the limitations of the program. For example, during a sort operation, the available memory can be reduced to find out whether the program is able to handle the situation.
- **Structural Tests:** Structural Tests are concerned with examining the internal processing logic of a software system. For example, if a function is responsible for tax calculation, the verification of the logic is a structural test.
- **Parallel Tests:** In Parallel Tests, the same test data is used in the new and old system and the output results are then compared.

**16.** Some disadvantages and limitations of the use of the continuous audit system are as follows:

- 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.
- Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.

**17.** The types of Managerial Controls and their scope are as follows:

- **Top Management and Information Systems Management Controls:** Discusses the top management's role in planning, organizing, leading and controlling the information

systems function. Also, provides advice to top management in relation to long-run policy decision making and translates long-run policies into short-run goals and objectives.

- **System Development Management Controls:** Provides a contingency perspective on models of the information systems development process that auditors can use as a basis for evidence collection and evaluation.
- **Programming Management Controls:** Discusses the major phases in the program life cycle and the important controls that should be exercised in each phase.
- **Data Resource Management Controls:** Discusses the roles of the data administrator and database administrator and the controls that should be exercises in each phase.
- **Quality Assurance Management Controls:** Discusses the major functions that quality assurance management should perform to ensure that the development, implementation, operation, and maintenance of information systems conform to quality standards.
- **Security Management Controls:** Discusses the major functions performed by operations by security administrators to identify major threats to the IS functions and to design, implement, operate, and maintain controls that reduce expected losses from these threats to an acceptable level.
- **Operations Management Controls:** Discusses the major functions performed by operations management to ensure the day-to-day operations of the IS function are well controlled.

18. **Boundary Controls:** These maintain the chronology of events that occur when a user attempts to gain access to and employ systems resources.

- Identity of the would-be user of the system;
- Authentication information supplied;
- Resources requested;
- Action privileges requested;
- Terminal Identifier;
- Start and Finish Time;
- Number of Sign-on attempts;
- Resources provided/denied; and

**Accounting Audit Trail**

- Action privileges allowed/denied.

**Operations Audit Trail**

- Resource usage from log-on to log-out time.
- Log of Resource consumption.

**19.** Section 76 under IT Act, 2000 explains about the situation under which any computer or computer resources that shall become liable to confiscation.

**[Section 76] Confiscation**

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation:

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

**20.** The IT Infrastructure Library (ITIL) is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. ITIL describes procedures, tasks and checklists that are not organization-specific, used by an organization for establishing a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement.

The volumes of ITIL are as follows:

- **Service Strategy:** This provides guidance on clarification and prioritization of service-provider investments in services;
- **Service Design:** This provides good-practice guidance on the design of IT services, processes, and other aspects of the service management effort;
- **Service Transition:** This elate to the delivery of services required by a business into live/operational use, and often encompasses the "project" side of IT rather than Business As Usual (BAU);
- **Service Operation:** This provides best practice for achieving the delivery of agreed levels of services both to end-users and the customers (where "customers" refer to those individuals who pay for the service and negotiate the SLAs), and

- **Continual Service Improvement:** This aims to align and realign IT services to changing business needs by identifying and implementing improvements to the IT services that support the business processes.

**21.** Guidelines for Energy Conservation are as follows:

- 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 centers; and
- Adapt more of Web conferencing offers instead of travelling to meetings in order to go green and save energy.

**22.** Limitations of Mobile Computing are as follows:

- **Insufficient Bandwidth:** Mobile Internet access is generally slower than direct cable connections using technologies such as GPRS and Enhanced Data for GSM and more recently 4G networks. These networks are usually available within range of commercial cell phone towers. Higher speed wireless LANs are inexpensive but have very limited range.
- **Security Standards:** When working mobile, one is dependent on public networks, requiring careful use of Virtual Private Network (VPN). Security is a major concern while concerning the mobile computing standards on the fleet. One can easily attack the VPN through a huge number of networks interconnected through the line.
- **Power consumption:** When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power. Combined with the compact size of many mobile devices, this often means unusually expensive batteries must be used to obtain the necessary battery life. Mobile computing should also look into Greener IT in such a way that it saves the power or increases the battery life.

- **Transmission interferences:** Weather, terrain, and the range from the nearest signal point can all interfere with signal reception. Reception in tunnels, some buildings, and rural areas is often poor.
- **Potential health hazards:** People who use mobile devices while driving are often distracted from driving are thus assumed more likely to be involved in traffic accidents. Cell phones may interfere with sensitive medical devices. There are allegations that cell phone signals may cause health problems.
- **Human interface with device:** Screens and keyboards tend to be small, which may make them hard to use. Alternate input methods such as speech or handwriting recognition require training.

**23.** The different instances of Infrastructure as a Service (IaaS) model in Cloud Computing are as follows:

- **Network as a Service (NaaS):** NaaS, an instance of IaaS, provides users with needed data communication capacity to accommodate bursts in data traffic during data-intensive activities such as video conferencing or large file downloads. It is an ability given to the end-users to access virtual network services that are provided by the service provider over the Internet on a per-per-use basis.
- **Storage as a Service (STaaS):** STaaS, an instance of IaaS, provides storage infrastructure on a subscription basis to users who want a low-cost and convenient way to store data, synchronize data across multiple devises, manage off-site backups, mitigate risks of disaster recovery, and preserve records for the long-term. It is an ability given to the end users to store the data on the storage services provided by the service provider.
- **Database as a Service (DBaaS):** This is also related to IaaS and provides users with seamless mechanisms to create, store, and access databases at a host site on demand. It is an ability given to the end users to access the database service without the need to install and maintain it on the pay-per-use basis. The end users can access the database services through any Application Programming Interfaces (APIs) or Web User Interfaces provided by the service provider.
- **Backend as a Service (BaaS):** It is a type of IaaS, that provides web and mobile app developers a way to connect their applications to backend cloud storage with added services such as user management, push notifications, social network services integration using custom software development kits and application programming interfaces.
- **Desktop as a Service (DTaaS):** It is an instance of IaaS that provides ability to the end users to use desktop virtualization without buying and managing their own infrastructure. DTaaS is a pay-per-use cloud service delivery model in which the service provider manages the back-end responsibilities of data storage, backup, security and upgrades. The end-users are responsible for securing for managing their

own desktop images, applications, and security. These services are simple to deploy, highly secure and produce better experience on almost all devices.

**24. (a)** Components of COBIT are as follows:

- **Framework -** Organize IT governance objectives and good practices by IT domains and processes, and links them to business requirements;
- **Process Descriptions -** A reference process model and common language for everyone in an organization. The processes map to responsibility areas of plan, build, run and monitor.
- **Control Objectives -** Provide a complete set of high-level requirements to be considered by management for effective control of each IT process.
- **Management Guidelines -** Help assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes
- **Maturity Models -** Assess maturity and capability per process and helps to address gaps.

**(b)** Major benefits of Office Automation Systems (OAS) are as follows:

- Office Automation Systems improve communication within an organization and between enterprises.
- They reduce the cycle time between preparation of messages and receipt of messages at the recipients' end.
- They also reduce the costs of office communication both in terms of time spent by executives and cost of communication links.
- Office Automation Systems ensure accuracy of information and smooth flow of communication.

**(c)** Examples of Segregation of Duties (SoD) are as follows:

- Systems software programming group from the application programming group;
- Database administration group from other data processing activities;
- Computer hardware operations from the other groups;
- Systems analyst function from the programming function;
- Physical, data, and online security group(s) from the other IS functions; and
- IS Audit from business operations groups.

**(d)** Agile Manifesto is based on following 12 features:

- Customer satisfaction by rapid delivery of useful software;
- Welcome changing requirements, even late in development;
- Working software is delivered frequently (weeks rather than months);

- Working software is the principal measure of progress;
- Sustainable development, able to maintain a constant pace;
- Close, daily co-operation between business people and developers;
- Face-to-face conversation is the best form of communication (co-location);
- Projects are built around motivated individuals, who should be trusted;
- Continuous attention to technical excellence and good design;
- Simplicity;
- Self-organizing teams; and
- Regular adaptation to changing circumstances.

**(e)** **Detection Risk:** Detection risk is the risk that the IT auditor's substantive procedures will not detect an error which could be material, individually or in combination with other errors. For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high because logs for the whole period of the audit are not available at the time of the audit. The detection risk associated with lack of identification of disaster recovery plans is ordinarily low since existence is easily verified.

**25. (a)** Information Systems Auditing is the process of attesting objectives (those of the external auditor) that focus on asset safeguarding, data integrity and management objectives (those of the internal auditor) that include effectiveness and efficiency both. This enables organizations to better achieve four major objectives that are as follows:

- **Asset Safeguarding Objectives:** The information system assets (hardware, software, data information etc.) must be protected by a system of internal controls from unauthorised access.
- **Data Integrity Objectives:** It is a fundamental attribute of IS Auditing. The importance to maintain integrity of data of an organisation requires all the time. It is also important from the business perspective of the decision maker, competition and the market environment.
- **System Effectiveness Objectives**: Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet business and user requirements.
- **System Efficiency Objectives:** To optimize the use of various information system resources (machine time, peripherals, system software and labour) along with the impact on its computing environment.

**(b)** The Disaster Recovery Planning 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 centre 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.

**(c) Web 3.0:** The term Web 3.0, also known as the Semantic Web, describes sites wherein the computers will be generated raw data on their own without direct user interaction. Web 3.0 standard uses semantic web technology, drag and drop mash-ups, widgets, user behavior, user engagement and consolidation of dynamic web contents depending on the interest of the individual users. Web 3.0 technology uses the "Data Web" Technology, which features the data records that are publishable and reusable on the web through query-able formats. An example of typical Web 3.0 application is the one that uses content management systems along with artificial intelligence.

The two major components of Web 3.0 are as follows:

- **Semantic Web:** This provides the web user a common framework that could be used to share and reuse the data across various applications, enterprises, and community boundaries. This allows the data and information to be readily intercepted by machines, so that the machines can take contextual decisions on their own by finding, combining and acting upon relevant information on the web.
- **Web Services:** It is a software system that supports computer-to-computer interaction over the Internet. For example - the popular photo-sharing website Flickr provides a web service that could be utilized and the developers to programmatically interface with Flickr in order to search for images.

## PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

## QUESTIONS

### Concepts of Governance and Management of Information Systems

1. You are appointed as an Internal Auditor in XYZ enterprise. As an internal auditor, what shall be your perspective while evaluating IT Governance of an enterprise?
2. (a) Discuss Risk Management Strategies in detail.

   (b) What do you understand by "Information Systems Risks"? Discuss broadly the characteristics of risk.
3. (a) Discuss the seven categories of enablers of COBIT 5?

   (b) Discuss various key management practices for assessing and evaluating the system of internal controls in an enterprise.

### Information System Concepts

4. "Decision Support Systems (DSS) are widely used as part of an Organization's Accounting Information System". Give examples to support this statement.
5. What is Executive Information Systems (EIS)? Explain major characteristics of an EIS.
6. What do you mean by the term "Information"? Discuss different attributes of it.

### Protection of Information Systems

7. Discuss Data Resource Management Controls under Managerial Controls.
8. Why is there an emergence of Quality Assurance Management Controls in organizations?
9. As a senior manager of an organization ABC, what do you think are the major functions performed by you while performing Information Systems (IS) functions in the organization?

### Business Continuity Planning and Disaster Recovery Planning

10. (a) Discuss the maintenance tasks undertaken in the development of a Business Continuity Plan (BCP) in brief.

    (b) A company has decided to outsource its recovery process to a third-party site. What are the issues that should be considered by the security administrators while drafting the contract?
11. Discuss Differential Backup, its advantages and disadvantages.

12. An enterprise XYZ implemented a Business Continuity Plan and decided to get its plan audited. What factors should be verified while auditing or self-assessment of the enterprise's Business Continuity Management (BCM) program?

**Acquisition, Development and Implementation of Information Systems**

13. Discuss various System Changeover Strategies under System Implementation phase of System Development Life Cycle (SDLC).

14. Discuss various issues that should be considered while designing systems input.

15. Discuss the Waterfall Model, its strengths and weaknesses in brief.

**Auditing of Information Systems**

16. As an auditor, what do you think are the advantages of using Continuous Audit Techniques?

17. Why do we need to perform Audit of Information Systems?

18. What do you understand by the term "Audit Trails"? How Audit Trails can be used to support security objectives?

**Information Technology Regulatory Issues**

19. ABC Ltd. is a security market intermediary, providing depository services. Briefly explain the relevant requirements with respect to annual systems audit mandated by SEBI (Securities and Exchange Board of India) in this regard.

20. Describe the 'Tampering with Computer Source Documents' in the light of Section 65 of Information Technology Act 2000.

**Emerging Technologies**

21. Discuss emerging Bring Your Own Devices (BYOD) Threats.

22. Discuss the characteristics and advantages of Community Cloud in Cloud Computing.

**Short Note Based Questions**

23. Write short notes on following:

    (a) PDCA cyclic process

    (b) Role of IS Auditor in reviewing Physical Access Controls

    (c) Benefits of Governance of Enterprise IT (GEIT)

    (d) Information Technology General Controls (ITGC)

    (e) Business Continuity Plan (BCP) Manual

24. Differentiate between the following:
    (a) Explicit Knowledge and Tacit Knowledge
    (b) Program Debugging and Program Documentation
    (c) Manual Logging and Electronic Logging
    (d) Identity as a Service (IDaaS) and Security as a Service(SECaaS)
    (e) Control Risk and Detection Risk

**Questions based on the Case Studies**

25. XYZ Technical University, a newly formed university, decided to launch a web based knowledge portal to facilitate their students of distance education for different courses. It proposed to upload the course materials, e - lectures and e-reference books. It is expected to provide various resources easily on anytime and anywhere basis. Therefore, an initial study or investigation under all dimensions was done. As a part of this, the management of the university invited various technical experts for a capable and good solution as per the requirements and guidelines of the university. Also, the University decided to encourage people to collaborate and share information online through social networks.
    (a) According to you as an IS Auditor, what are the validation methods for approving the vendors' proposals?
    (b) The university will facilitate the communication system to interact with their students effectively and economically by using Electronic Mail systems. What are the features of the Electronic Mail System?

## SUGGESTED ANSWERS/HINTS

**1.** As an Internal Auditor in XYZ enterprise, the perspective while evaluating IT governance of an enterprise are as follows:

- **Leadership:** The following aspects need to be verified by the auditor:
    - Evaluate the relationship between IT objectives and the current/strategic needs of the organization and the ability of IT leadership to effectively communicate this relationship to IT and organizational personnel.
    - Assess the involvement of IT leadership in the development and on-going execution of the organization's strategic goals.
    - Determine how IT will be measured in helping the organization achieve these

goals.

- Review how roles and responsibilities are assigned within the IT organization and how they are executed.
- Review the role of senior management and the board in helping establish and maintain strong IT governance.

- **Organizational Structure:** The following aspects need to be assessed by the auditor:
  - Review how organization management and IT personnel are interacting and communicating current and future needs across the organization.
  - This should include the existence of necessary roles and reporting relationships to allow IT to meet the needs of the organization, while providing the opportunity to have requirements addressed via formal evaluation and prioritization. In addition, how IT mirrors the organization structure in its enterprise architecture should also be included.
- **Processes:** The following aspects need to be checked by the auditor:
  - Evaluate IT process activities and the controls in place to mitigate risks to the organization and whether they provide the necessary assurance regarding processes and underlying systems.
  - What processes are used by the IT organization to support the IT environment and consistent delivery of expected services?
- **Risks:** The following aspects need to be reviewed by the auditor:
  - Review the processes used by the IT organization to identify, assess, and monitor/mitigate risks within the IT environment.
  - Additionally, determine the accountability that personnel have within risk management and how well these expectations are being met.
- **Controls:** The following aspects need to be verified by the auditor:
  - Assess key controls that are defined by IT to manage its activities and the support of the overall organization.
  - Ownership, documentation, and reporting of self-validation aspects should be reviewed by the internal audit activity.
  - Additionally, the control set should be robust enough to address identified risks based on the organization's risk appetite and tolerance levels, as well as any compliance requirements.

- **Performance Measurement/Monitoring:** The following aspects need to be verified by the auditor:
  - Evaluate the framework and systems in place to measure and monitor organizational outcomes where support from IT plays an important part in the internal outputs in IT operations and developments.

**2. (a)** The Risk Management Strategies are as follows:

- **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.

**(b) Information Systems Risks:** Risk is the possibility of something adverse happening, resulting in potential loss/exposure. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Risk management involves identifying, measuring, and minimizing uncertain events affecting resources. Any Information system based on IT has its inherent risks. These risks cannot be eliminated but they can be mitigated by appropriate security. If controls are unavailable or inadequate or inappropriate, then there would be a control weakness, which must be reported to auditee management with appropriate recommendations to mitigate them.

The risks in IT environment are mitigated by providing appropriate and adequate IS Security. IS security is defined as "procedures and practices to assure that computer facilities are available at all required times, that data is processed completely and efficiently and that access to data in computer systems is restricted to authorized people".

Some of the common sources of risk are Commercial and Legal Relationships; Economic Circumstances; Human Behavior; Natural Events; Political Circumstances; Technology and Technical Issues; Management Activities and Controls, and Individual Activities.

Broadly, Risk has the following characteristics:

- Loss potential that exists as the result of threat/vulnerability process;
- Uncertainty of loss expressed in terms of probability of such loss; and
- The probability/likelihood that a threat agent mounting a specific attack against a system.

**3. (a)** The COBIT 5 framework describes seven categories of enablers, which are as follows:

- **Principles, Policies and Frameworks** are the vehicle to translate the desired behavior into practical guidance for day-to-day management.
- **Processes** describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
- **Organizational structures** are the key decision-making entities in an enterprise.
- **Culture, Ethics and Behavior** of individuals and of the enterprise is very often underestimated as a success factor in governance and management activities.
- **Information** is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
- **Services, Infrastructure and Applications** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.

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

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

- **Monitor Internal Controls:** Continuously monitor, benchmark and improve the IT control environment and control framework to meet organizational objectives.
- **Review Business Process Controls Effectiveness:** Review the operation of controls, including a review of monitoring and test evidence to ensure that controls within business processes operate effectively. It also includes activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing of controls, continuous controls monitoring, independent assessments, command and control centers, and network operations centers. This provides the business with the assurance of control effectiveness to meet requirements related to business, regulatory and social responsibilities.
- **Perform Control Self-assessments:** Encourage management and process owners to take positive ownership of control improvement through a continuing program of self- assessment to evaluate the completeness and effectiveness of management's control over processes, policies and contracts.
- **Identify and Report Control Deficiencies:** Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.
- **Ensure that assurance providers are independent and qualified:** Ensure that **the** entities performing assurance are independent from the function, groups or organizations in scope. The entities performing assurance should demonstrate an appropriate attitude and appearance, competence in the skills and knowledge necessary to perform assurance, and adherence to codes of ethics and professional standards.
- **Plan Assurance Initiatives:** Plan assurance initiatives based on enterprise objectives and conformance objectives, assurance objectives and strategic priorities, inherent risk resource constraints, and sufficient knowledge of the enterprise.

- **Scope assurance initiatives:** Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.
- **Execute assurance initiatives:** Execute the planned assurance initiative. Report on identified findings. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control system residual risks.

**4.** Decision Support Systems (DSS) are widely used as a part of an organization's Accounting Information System. The complexity and nature of decision support systems vary. Many are developed in-house using either a general type of decision support program or a spreadsheet program to solve specific problems. Below are several illustrations:

- **Cost Accounting System:** The health care industry is well known for its cost complexity. Managing costs in this industry requires controlling costs of supplies, expensive machinery, technology, and a variety of personnel. Cost accounting applications help health care organizations calculate product costs for individual procedures or services. Decision support systems can accumulate these product costs to calculate total costs per patient. Health care managers may combine cost accounting decision support systems with other applications, such as productivity systems. Combining these applications allows managers to measure the effectiveness of specific operating processes
- **Capital Budgeting System:** Companies require new tools to evaluate high-technology investment decisions. Decision makers need to supplement analytical techniques, such as net present value and internal rate of return, with decision support tools that consider some benefits of new technology not captured in strict financial analysis. Example- Auto Man is a DSS designed to support decisions about investments in automated manufacturing technology that allows decision makers to consider financial, nonfinancial, quantitative, and qualitative factors in their decision-making processes.
- **Budget Variance Analysis System:** Financial institutions rely heavily on their budgeting systems for controlling costs and evaluating managerial performance. One institution uses a computerized decision support system to generate monthly variance reports for division comptrollers. The system allows these comptrollers to graph, view, analyze, and annotate budget variances, as well as create additional one-and five-year budget projections using the forecasting tools provided in the system. The decision support system thus helps the comptrollers create and control budgets for the cost-center managers reporting to them.

- **General Decision Support System:** Some planning languages used in decision support systems are general purpose and therefore have the ability to analyze many different types of problems. In a sense, these types of decision support systems are a decision-maker's tools. The user needs to input data and answer questions about a specific problem domain to make use of this type of decision support system. An example is a program called Expert Choice that supports a variety of problems requiring decisions. The user works interactively with the computer to develop a hierarchical model of the decision problem. The decision support system then asks the user to compare decision variables with each other. For instance, the system might ask the user how important cash inflows are versus initial investment amount to a capital budgeting decision. The decision maker also makes judgments about which investment is best with respect to these cash flows and which requires the smallest initial investment. Expert Choice analyzes these judgments and presents the decision maker with the best alternative.

5. **Executive Information Systems (EIS):** It is also referred to as an Executive Support System (ESS) that serves at the strategic level i.e. top level managers of the organization. ESS creates a generalized computing and communications environment rather than providing any preset applications or specific competence.

   Major characteristics of an EIS are as follows:

   - It is a Computer-based-information system that serves the information need of top executives.
   - EIS enables users to extract summary data and model complex problems without the need to learn query languages statistical formulas or high computing skills.
   - It provides rapid access to timely information and direct access to management reports.
   - EIS is capable of accessing both internal and external data.
   - EIS provides extensive online analysis tool like trend analysis, market conditions etc.
   - EIS can easily be given as a DSS support for decision making.

6. **Information:** Technically, Information means processed data. Information relates to description, definition, or perspective (what, who, when, where) and may be represented in the form of text, graph, pictures, voice, videos etc.

   Information is essential because it adds knowledge, helps in decision making, analyzing the future and taking action in time. Information products produced by an

information system can be represented by number of ways e.g. paper reports, visual displays, multimedia documents, electronic messages, graphics images, and audio responses.

Some of the important attributes of useful and effective information are as follows:

- **Availability -** Information is useless if it is not available at the time of need. Database is a collection of files which is collection of records and data from where the required information is derived for useful purpose.
- **Purpose/Objective -** Information must have purpose/objective at the time it is transmitted to a person or machine, otherwise it is simple data. The basic objective of information is to inform, evaluate, persuade, and organize. This indeed helps in decision making, generating new concepts and ideas, identify and solve problems, planning, and controlling which are needed to direct human activity in business enterprises.
- **Mode and format -** The mode of communicating information to humans should be in such a way that it is easily understandable by the people. The mode may be in the form of voice, text and combination of these two. Format should also be designed in such a way that it assists in decision making, solving problems, initiating planning, controlling and searching.
- **Current/Updated -** The information should be refreshed from time to time as it usually rots with time and usage. For example, the running score sheet of a cricket match available in Internet sites should be refreshed at fixed interval of time so that the current score will be available.
- **Rate -** The rate of transmission/reception of information may be represented by the time required to understand a particular situation. Useful information is the one which is transmitted at a rate which matches with the rate at which the recipient wants to receive. For example - the information available from internet site should be available at a click of mouse.
- **Frequency -** The frequency with which information is transmitted or received affects its value. For example - the weekly report of sales shows little change as compared to the quarterly and contribute less for accessing salesman capability.
- **Completeness and Adequacy -** The information provided should be complete and adequate in itself because only complete information can be used in policy making. For example - the position of student in a class can be find out only after having the information of the marks of all students and the total number of students in a class.

- **Reliability -** It is a measure of failure or success of using information for decision-making. If information leads to correct decision on many occasions, we say the information is reliable.
- **Validity -** It measures how close the information is to the purpose for which it asserts to serve. For example, the experience of employee supports in evaluating his performance.
- **Quality -** It means the correctness of information. For example, an over-optimistic manager may give too high estimates of the profit of product which may create problem in inventory and marketing.
- **Transparency -** It is essential in decision and policy making. For example, total amount of advance does not give true picture of utilization of fund for decision about future course of action; rather deposit-advance ratio is perhaps more transparent information in this matter.
- **Value of Information -** It is defined as the difference between the value of the change in decision behavior caused by the information and the cost of the information. In other words, given a set of possible decisions, a decision-maker may select one on basis of the information at hand. If new information causes a different decision to be made, the value of the new information is the difference in value between the outcome of the old decision and that of the new decision, less the cost of obtaining the information.

7. **Data Resource Management Controls:** Many organizations now recognize that data is a critical resource that must be managed properly and therefore, accordingly, centralized planning and control are implemented. For data to be managed; better users must be able to share data; data must be available to users when it is needed, in the location where it is needed, and in the form in which it is needed. Further it must be possible to modify data fairly easily and the integrity of the data be preserved. If data repository system is used properly, it can enhance data and application system reliability. It must be controlled carefully, however, because the consequences are serious if the data definition is compromised or destroyed. Careful control should be exercised over the roles by appointing senior, trustworthy persons, separating duties to the extent possible and maintaining and monitoring logs of the data administrator's and database administrator's activities.

   The control activities involved in maintaining the integrity of the database is as under:

   **(a) Definition Controls:** These controls are placed to ensure that the database always corresponds and comply with its definition standards.

**(b) Existence/Backup Controls:** These ensure the existence of the database by establishing backup and recovery procedures. Backup refers to making copies of the data so that these additional copies may be used to restore the original data after a data loss. Backup controls ensure the availability of system in the event of data loss due to unauthorized access, equipment failure or physical disaster; the organization can retrieve its files and databases. Various backup strategies are Dual recording of data; Periodic dumping of data; Logging input transactions; and Logging changes to the data.

**(c) Access Controls:** Access controls are designed to prevent unauthorized individual from viewing, retrieving, computing or destroying the entity's data. Controls are established in the following manner:

- User Access Controls through passwords, tokens and biometric Controls; and
- Data Encryption: Keeping the data in database in encrypted form.

**(d) Update Controls:** These controls restrict update of the database to authorized users in two ways:

- By permitting only addition of data to the database; and
- Allowing users to change or delete existing data.

**(e) Concurrency Controls:** These controls provide solutions, agreed-upon schedules and strategies to overcome the data integrity problems that may arise when two update processes access the same data item at the same time.

**(f) Quality Controls:** These controls ensure the accuracy, completeness, and consistency of data maintained in the database. This may include traditional measures such as program validation of input data and batch controls over data in transit through the organization.

**8.** The reasons for the emergence of Quality Assurance Management Controls in many organizations are as follows:

- Organizations are increasingly producing safety-critical systems and users are becoming more demanding in terms of the quality of the software they employ to undertake their work;
- Organizations are undertaking more ambitious projects when they build software;
- Users are becoming more demanding in terms of their expectations about the quality of software they employ to undertake their work;

- Organizations are becoming more concerned about their liabilities if they produce and sell defective software;
- Poor quality control over the production, implementation, operation, and maintenance of software can be costly in terms of missed deadlines, dissatisfied users and customer, lower morale among IS staff, higher maintenance and strategic projects that must be abandoned; and
- Improving the quality of Information Systems is a part of a worldwide trend among organizations to improve the quality of the goods and services they sell.

Quality Assurance (QA) personnel should work to improve the quality of information systems produced, implemented, operated, and maintained in an organization. They perform a monitoring role for management to ensure that –

- Quality goals are established and understood clearly by all stakeholders; and
- Compliance occurs with the standards that are in place to attain quality information systems.

**9.** The major functions that a senior manager must perform while performing Information Systems (IS) functions in the organization are as follows:

**(a) Planning –** This includes determining the goals of the information systems function and the means of achieving these goals. To achieve this – the plan is to be prepared with different types of Plans and the Role of a Steering Committee should be defined clearly.

**(b) Organizing –** There should be a prescribed IT organizational structure with documented roles and responsibilities and agreed job descriptions. This includes gathering, allocating, and coordinating the resources needed to accomplish the goals that are established during Planning function.

**(c) Leading –** This includes motivating, guiding, and communicating with personnel. The purpose of leading is to achieve the harmony of objectives; ie.. a person's or group's objectives must not conflict with the organization's objectives. The process of leading requires managers to motivate subordinates, direct them and communicate with them.

**(d) Controlling –** This includes comparing actual performance with planned performance as a basis for taking any corrective actions that are needed. This involves determining when the actual activities of the information system's functions deviate from the planned activities.

**10. (a)** The maintenance tasks undertaken in Development of Business Continuity Plan (BCP) are as follows:

- Determine the ownership and responsibility for maintaining the various BCP strategies within the enterprise;
- Identify the BCP maintenance triggers to ensure that any organizational, operational, and structural changes are communicated to the personnel who are accountable for ensuring that the plan remains up-to-date;
- Determine the maintenance regime to ensure the plan remains up-to-date;
- Determine the maintenance processes to update the plan; and
- Implement version control procedures to ensure that the plan is maintained up-to-date.

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

- how soon the site will be made available subsequent to a disaster;
- the number of organizations that will be allowed to use the site concurrently in the event of a disaster;
- the priority to be given to concurrent users of the site in the event of a common disaster;
- the period during which the site can be used;
- the conditions under which the site can be used;
- the facilities and services the site provider agrees to make available; and
- what controls will be in place and working at the off-site facility.

**11. 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.

For example - Suppose a differential backup job or task is to be done every night from Monday to Friday. On Monday, the first backup will be a full backup since no prior backups have been taken. On Tuesday, the differential backup will only backup the files that have changed since Monday and any new files added to the backup folders. On Wednesday, the files changed and files added since Monday's full backup

will be copied again. While Wednesday's backup does not include the files from the first full backup, it still contains the files backed up on Tuesday.

Advantages of Differential Backup are as follows:

- Much faster backups then full backups.
- More efficient use of storage space then full backups since only files changed since the last full backup will be copied on each differential backup run.
- Faster restores than incremental backups.

Disadvantages of Differential Backup are as follows:

- Backups are slower then incremental backups.
- Not as efficient use of storage space as compared to incremental backups. All files added or edited after the initial full backup will be duplicated again with each subsequent differential backup.
- Restores are slower than with full backups.
- Restores are a little more complicated than full backups but simpler than incremental backups. Only the full backup set and the last differential backup are needed to perform a restore.

**12.** An audit or self-assessment of the enterprise's Business Continuity Management (BCM) program should verify the following factors:

- All key products and services and their supporting critical activities and resources have been identified and included in the enterprise's BCM strategy;
- The enterprise's BCM policy, strategies, framework and plans accurately reflect its priorities and requirements (the enterprise's objectives);
- The enterprise' BCM competence and its BCM capability are effective and fit-for-purpose and will permit management, command, control and coordination of an incident;
- The enterprise's BCM solutions are effective, up-to-date and fit-for-purpose, and appropriate to the level of risk faced by the enterprise;
- The enterprise's BCM maintenance and exercising programs have been effectively implemented;
- BCM strategies and plans incorporate improvements identified during incidents and exercises and in the maintenance program;
- The enterprise has an ongoing program for BCM training and awareness;

- BCM procedures have been effectively communicated to relevant staff, and that those staff understand their roles and responsibilities; and
- Change control processes are in place and operate effectively.

**13. System Change-Over Strategies:** Conversion or changeover is the process of changing over or shifting over from the old system (may be the manual system) to the new system. It requires careful planning to establish the basic approach to be used in the actual changeover, as it may put many resources/assets/operations at risk. The Four types of popular implementation strategies are described as follows:

- **Direct Implementation / Abrupt Change-Over:** This is achieved through an abrupt takeover – an all or no approach. With this strategy, the changeover is done in one operation, completely replacing the old system in one go. Direct Implementation, which usually takes place on a set date, often after a break in production or a holiday period so that time can be used to get the hardware and software for the new system installed without causing too much disruption.
- **Phased Changeover:** With this strategy, implementation can be staged with conversion to the new system taking place gradually. For example, some new files may be converted and used by employees whilst other files continue to be used on the old system i.e. the new is brought in stages (phases). If a phase is successful then the next phase is started, eventually leading to the final phase when the new system fully replaces the old one.
- **Pilot Changeover:** With this strategy, the new system replaces the old one in one operation but only on a small scale. Any errors can be rectified or further beneficial changes can be introduced and replicated throughout the whole system in good time with the least disruption. For example - it might be tried out in one branch of the company or in one location. If successful, then the pilot is extended until it eventually replaces the old system completely.
- **Parallel Changeover:** This is considered the most secure method with both systems running in parallel over an introductory period. The old system remains fully operational while the new systems come online. With this strategy, the old and the new system are both used alongside each other, both being able to operate independently. If all goes well, the old system is stopped and new system carries on as the only system.

**14.** Input design consists of developing specifications and procedures for data preparation, developing steps which are necessary to put transactions data into a usable form for processing, and data-entry, i.e., the activity of putting the data into the computer for

processing. Major areas that should be considered while designing systems input are as follows:

(i) **Content:** The analyst is required to consider the types of data that are needed to be gathered to generate the desired user outputs. Sometimes, the data needed for a new system are not available within the organization. Hence, the system designer has to prepare new documents for collecting such information.

(ii) **Timeliness:** In data processing, it is very important that data is inputted to computer in time because outputs cannot be produced until certain inputs are available. Hence, a plan must be established regarding when different types of inputs will enter the system.

(iii) **Media:** Various user input alternatives are available in the market such as workstations, magnetic disc, OCR, pen-based computers and voice input etc. A suitable medium may be selected depending on the application to be computerized.

(iv) **Format:** After the data contents and media requirements are determined, input formats are considered. While specifying the record formats, for instance, the type and length of each data field as well as any other special characteristics must be defined. Designing input formats often requires the assistance of a professional programmer or database administrator.

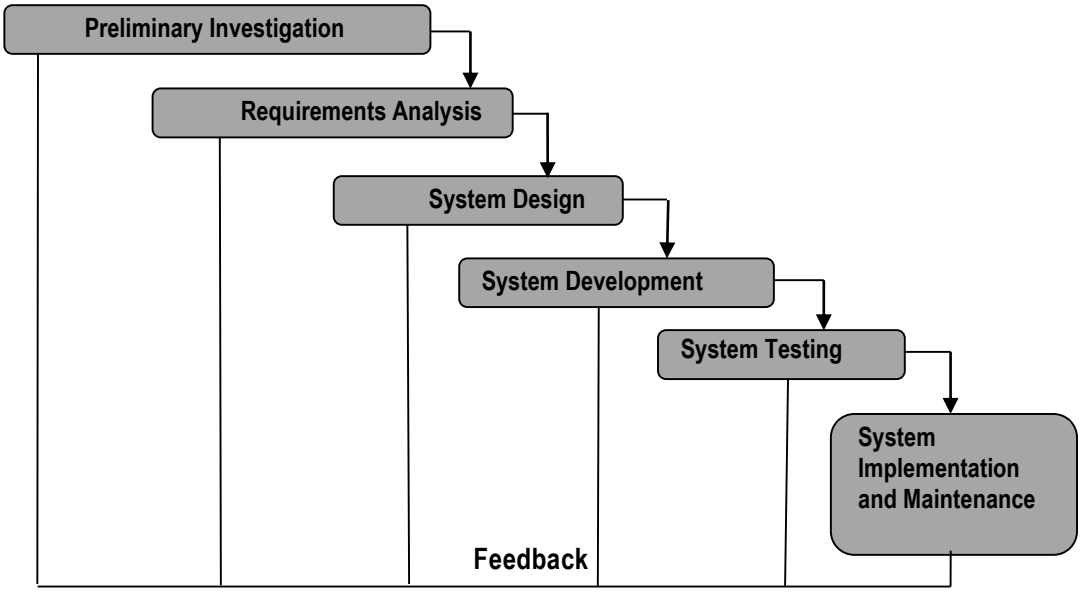
(v) **Input Volume:** Input volume refers to the amount of data that has to be entered in the computer system at any one time. For example, in some decision-support systems and many real-time transaction processing systems, input volume is light which involves data entry department using key-to-tape or key-to-disk systems.

15. **Waterfall Model:** The waterfall approach is a traditional development approach in which each phase is carried in sequence or linear fashion. These phases include requirements analysis, specifications and design requirements, coding, final testing, and release. In this traditional approach of system development, activities are performed in sequence. The tasks that are performed during each phase of the traditional approach is shown in the Fig. below. When the traditional approach is applied, an activity is undertaken only when the prior step is fully completed.

Major strengths of Waterfall Model are as follows:

- It is ideal for supporting less experienced project teams and project managers or project teams, whose composition fluctuates.
- The orderly sequence of development steps and design reviews help to ensure the quality, reliability, adequacy and maintainability of the developed software.

- Progress of system development is measurable.
- It enables to conserve resources.




Some of the weaknesses of the Waterfall Model are as follows:

- It is criticized to be inflexible, slow, costly, and cumbersome due to significant structure and tight controls.
- Project progresses forward, with only slight movement backward.
- There is a little to iterate, which may be essential in situations.
- It depends upon early identification and specification of requirements, even if the users may not be able to clearly define 'what they need early in the project'.
- Requirement inconsistencies, missing system components and unexpected development needs are often discovered during design and coding.
- Problems are often not discovered until system testing.
- System performance cannot be tested until the system is almost fully coded, and under capacity may be difficult to correct.
- It is difficult to respond to changes, which may occur later in the life cycle, and if undertaken it proves costly and are thus discouraged.
- It leads to excessive documentation, whose updation to assure integrity is an uphill task and often time-consuming.
- Written specifications are often difficult for users to read and thoroughly appreciate.

- It promotes the gap between users and developers with clear vision of responsibility.

**16.** Some of the advantages of using 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.

**17.** Audit of Information Systems is required due to following reasons:

- **Organisational Costs of Data Loss:** Data is a critical resource of an organisation for its present and future process and its ability to adapt and survive in a changing environment.
- **Cost of Incorrect Decision Making:** Management and operational controls taken by managers involve detection, investigations and correction of the processes. These high level decisions require accurate data to make quality decision rules.
- **Costs of Computer Abuse:** Unauthorised access to computer systems, malwares, unauthorised physical access to computer facilities and unauthorised copies of sensitive data can lead to destruction of assets (hardware, software, data, information etc.)
- **Value of Computer Hardware, Software and Personnel***:* These are critical resources of an organisation, which has a credible impact on its infrastructure and business competitiveness.
- **High Costs of Computer Error:** In a computerised enterprise environment where many critical business processes are performed, a data error during entry or process would cause great damage.

- **Maintenance of Privacy:** Today, data collected in a business process contains private information about an individual too. These data were also collected before computers but now, there is a fear that privacy has eroded beyond acceptable levels.
- **Controlled evolution of computer Use:** Use of Technology and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.

**18. Audit Trails:** Audit trails are the logs that can be designed to record activity at the system, application, and user level. When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives. Many operating systems allow management to select the level of auditing to be provided by the system. This determines 'which events will be recorded in the log'. An effective audit policy will capture all significant events without cluttering the log with trivial activity.

Audit trail controls attempt to ensure that a chronological record of all events that have occurred in a system is maintained. This record is needed to answer queries, fulfill statutory requirements, detect the consequences of error and allow system monitoring and tuning. The accounting audit trail shows the source and nature of data and processes that update the database. The operations audit trail maintains a record of attempted or actual resource consumption within a system.

**Audit trails can be used to support security objectives in three ways:**

- **Detecting Unauthorized Access*:*** The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls. A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by a virus or worm. Depending upon how much activity is being logged and reviewed; real-time detection can impose a significant overhead on the operating system, which can degrade operational performance.
- **Reconstructing Events*:*** Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors. Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future. Audit trail analysis also plays an important role in accounting control.
- **Personal Accountability*:*** Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behavior. Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log.

**19.** SEBI (Securities and Exchange Board of India) mandated that exchanges shall conduct an annual system audit by a reputed independent auditor.

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

**20.** Section 65 of Information Technology Act, 2000 is about "Tampering with Computer Source Documents". The section is -

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

**Explanation -** For the purposes of this section, "Computer Source Code" means the listing of programme, computer commands, design and layout and program analysis of computer resource in any form.

**21.** Every business decision is accompanied with a set of threats and so is Bring Your Own Device (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.
- **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 a majority of 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.

**22.** Characteristics of Community Clouds in Cloud Computing 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.

Advantages of Community Clouds in Cloud Computing are as follows:

- It allows establishing a low-cost private cloud.
- It allows collaborative work on the cloud.
- It allows sharing of responsibilities among the organizations.
- It has better security than the public cloud.

**23. (a)** The PDCA cyclic process is explained below:

- **The Plan Phase (Establishing the Information Security Management System (ISMS)) –** This phase serves to plan the basic organization of information security, set objectives for information security and choose the appropriate security controls (the standard contains a catalogue of 133 possible controls).
- **The Do Phase (Implementing and Working of ISMS) –** This phase includes carrying out everything that was planned during the previous phase.
- **The Check Phase (Monitoring and Review of the ISMS) –** The purpose of this phase is to monitor the functioning of the ISMS through various "channels", and check whether the results meet the set objectives.
- **The Act Phase (Update and Improvement of the ISMS) –** The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase.

**(b)** Role of IS Auditor in reviewing Physical Access Controls involves the following:

- **Risk Assessment:** The auditor must satisfy him/herself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures there from.
- **Controls Assessment:** The auditor based on the risk profile evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks.

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

**(c)** Benefits of Governance of Enterprise IT (GEIT) are as follows:

- It provides a consistent approach integrated and aligned with the enterprise governance approach.
- It ensures that IT-related decisions are made in line with the enterprise's strategies and objectives.
- It ensures that IT-related processes are overseen effectively and transparently.
- It confirms compliance with legal and regulatory requirements.
- It ensures that the governance requirements for board members are met.

**(d)** **Information Technology General Controls (ITGC):** These are the basic policies and procedures that ensure that an organization's information systems are properly safeguarded, that application programs and data are secure, and that computerized operations can be recovered in case of unexpected interruptions. IT General Controls are the foundation for the overall IT control environment as they provide the assurance that systems operate as intended and that output is reliable.

ITGCs may also be referred to as General Computer Controls (GCC) which are defined as: Controls, other than application controls, which relate to the environment within which computer-based application systems are developed, maintained and operated, and which are therefore applicable to all applications. The objectives of general controls are to ensure the proper development and implementation of applications, the integrity of program and data files and of computer operations. Like application controls, general controls may be either manual or programmed. Examples of general controls include the development and implementation of an IS strategy and an IS security policy, the organization of IS staff to separate conflicting duties and planning for disaster prevention and recovery.

**(e)** **Business Continuity Plan (BCP) Manual:** A BCP manual is a documented description of actions to be taken, resources to be used and procedures to be followed before, during and after an event that severely disrupts all or part of the business operations. The BCP Manual is expected to specify the responsibilities of the BCM team, whose mission is to establish appropriate BCP procedures to

ensure the continuity of enterprise's critical business functions. In the event of an incident or disaster affecting any of the functional areas, the BCM Team serves as liasioning teams between the functional area(s) affected and other departments providing support services.

**24. (a)** **Explicit knowledge:** Explicit knowledge is that which can be formalized easily and as a consequence is easily available across the organization. Explicit knowledge is articulated, and represented as spoken words, written material and compiled data. This type of knowledge is codified, easy to document, transfer and reproduce. For example – Online tutorials, Policy and procedural manuals.

**Tacit knowledge:** Tacit knowledge, on the other hand, resides in a few often-in just one person and hasn't been captured by the organization or made available to others. Tacit knowledge is unarticulated and represented as intuition, perspective, beliefs, and values that individuals form based on their experiences. It is personal, experimental and context-specific. It is difficult to document and communicate the tacit knowledge. For example – hand-on skills, special know-how, employee experiences.

**(b)** **Program Debugging:** Debugging is the most primitive form of testing activity, which refers to correcting programming language syntax and diagnostic errors so that the program compiles cleanly. A clean compile means that the program can be successfully converted from the source code written by the programmer into machine language instructions. Debugging can be a tedious task consisting of following four steps:

- Giving input the source program to the compiler,
- Letting the compiler to find errors in the program,
- Correcting lines of code that are erroneous, and
- Resubmitting the corrected source program as input to the compiler.

**Program Documentation:** The writing of narrative procedures and instructions for people, who will use software is done throughout the program life cycle. Managers and users should carefully review both internal and external documentation to ensure that the software and system behave as the documentation indicates. If they do not, documentation should be revised. User documentation should also be reviewed for understandability i.e. the documentation should be prepared in such a way that the user can clearly understand the instructions.

(c) **Manual Logging:** All visitors should be prompted to sign a visitor's log indicating their name, company represented, their purpose of visit, and person to see. Logging may happen at both fronts - reception and entrance to the computer room. A valid and acceptable identification such as a driver's license, business card or vendor identification tag may also be asked for before allowing entry inside the company.

**Electronic Logging:** This feature is a combination of electronic and biometric security systems. The users logging can be monitored and the unsuccessful attempts being highlighted.

(d) **Identity as a Service (IDaaS):** It is an ability given to the end users; typically, an organization or enterprise; to access the authentication infrastructure that is built, hosted, managed and provided by the third-party service provider. Generally, IDaaS includes directory services, authentication services, risk and event monitoring, single sign-on services, and identity and profile management.

**Security as a Service(SECaaS):** It is an ability given to the end user to access the security service provided by the service provider on a pay-per-use basis. It is a new approach to security in which cloud security is moved into the cloud itself whereby cloud service users will be protected from within the cloud using a unified approach to threats. Four mechanisms of Cloud security that are currently provided are Email filtering, Web content filtering, Vulnerability management and Identity management.

(e) **Control Risk:** Control risk is the risk that could occur in an audit area, and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system. Control risk is a measure of the auditor's assessment of the likelihood that risk exceeding a tolerable level and will not be prevented or detected by the client's internal control system. This assessment includes an assessment of whether a client's internal controls are effective for preventing or detecting gaps and the auditor's intention to make that assessment at a level below the maximum (100 percent) as a part of the audit plan.

**Detection Risk:** Detection risk is the risk that the IT auditor's substantive procedures will not detect an error which could be material, individually or in combination with other errors. For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high because logs for the whole period of the audit are not available at the time of the audit. The detection risk associated with lack of identification of disaster recovery plans is ordinarily low since existence is easily verified.

25. (a) **Methods of Validating the proposal:** Large organizations would naturally tend to adopt a sophisticated and objective approach to validate the vendor's proposal. Some of the validation methods for approving the vendor's proposal are as follows:

- **Checklists:** It is the most simple and a subjective method for validation and evaluation. The various criteria are put in check list in the form of suitable questions against which the responses of the various vendors are validated. For example, Support Service Checklists may have parameters like Performance; System development, Maintenance, Conversion, Training, Back-up, Proximity, Hardware and Software.
- **Point-Scoring Analysis:** Point-scoring analysis provides an objective means of selecting a final system. There are no absolute rules in the selection process, only guidelines for matching user needs with software capabilities. Thus, even for a small business, the evaluators must consider such issues as the company's data processing needs, its in-house computer skills, vendor reputations, software costs, and so forth.
- **Public Evaluation Reports:** Several consultancy as well as independent agencies compare and contrast the hardware and software performance for various manufacturers and publish their reports in this regard. This method has been frequently and usefully employed by several buyers in the past and is particularly useful where the buying staffs have inadequate knowledge of facts.
- **Benchmarking Problems related Vendor's Solutions:** Benchmarking problems related to vendors' proposals are accomplished by sample programs that represent at least a part of the buyer's primary work load and include considerations and can be current applications that have been designed to represent planned processing needs. That is, benchmarking problems are oriented towards testing whether a solution offered by the vendor meets the requirements of the job on hand of the buyer.
- **Testing Problems:** Test problems disregard the actual job mix and are devised to test the true capabilities of the hardware, software or system. For example, test problems may be developed to evaluate the time required to translate the source code (program in an assembly or a high level language) into the object code (machine language), response time for two or more jobs in multi-programming environment, overhead requirements of the operating system in executing a user program, length of time required to execute an instruction, etc.

**(b)** Various features of Electronic 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 -** Email permits sending a message to a large number of target recipients. Thus, it is easy to send a circular to all branches of a bank using Email resulting in a lot of saving of paper. 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 if accurate and the information required for the message is accesses quickly.
- **Portability -** Email 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 advancements in communication technologies and competition among the communication service providers have made Email the most economical mode for sending and receiving messages. The email is very helpful for formal communication as well as informal communication within the enterprise.