

PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

Question No. 1 is compulsory.

Candidates are also required to answer any five questions from the remaining six questions.

Question 1

ABC limited is a reputed Insurance company with their head office located in Chicago. With an aim to expand their business, they started a subsidiary company in India and obtained the license from IRDA. Now they want to set-up branches throughout India and to appoint agents to sell their Insurance Products. The company want to use latest technologies and to establish an IT Department with full IS security. The company was to implement COBIT 5 in their organization. Further they also want to sell their insurance products online and to develop a website to provide E-Commerce facility and implement Mobile Computing in their company.

You are appointed as IT Consultant for this company. Please answer the following queries raised by the Management?

- (a) *What are the enablers described by COBIT 5 Framework?* (5 Marks)
- (b) *What are the limitations of mobile computing?* (5 Marks)
- (c) *What is the information that an IS Auditor is expected to obtain at the audit location before proceeding with the IS Audit as per the provisions of IRDA?* (5 Marks)
- (d) *Explain the Impact of Cyber Frauds on Enterprises.* (5 Marks)

Answer 1

- (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.

- **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) Limitations of Mobile Computing are as follows:
- **Insufficient Bandwidth:** Mobile Internet access is generally slower than direct cable connections using technologies such as General Packet Radio Service (GPRS) and Enhanced Data for GSM (Global System for Mobile Communication) Evolution (EDGE), and more recently 3G 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. 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 is often distracted from driving are thus assumed to be more likely 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.
- (c) Before proceeding with the IS Audit as per the provisions of IRDA (Insurance Regulatory and Development Authority of India), the IS 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.
 - 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 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.
- (d) The impact of cyber frauds on enterprises can be viewed under the following dimensions:
- **Financial Loss:** Cyber frauds lead to actual cash loss to target company/organization. For example, wrongfully withdrawal of money from bank accounts.
 - **Legal Repercussions:** Entities hit by cyber frauds are caught in legal liabilities to their customers. Section 43A of the Information Technology (Amendment) Act 2008, fixes liability for companies/organizations having secured data of customers. These entities need to ensure that such data is well protected. In case a fraudster breaks into such database, it adds to the liability of entities.
 - **Loss of credibility or Competitive Edge:** News that an organizations database has been hit by fraudsters, leads to loss of competitive advantage. This also leads to lose credibility. There have been instances where share prices of such companies went down, as the news of such attack percolated to the market.
 - **Disclosure of Confidential, Sensitive or Embarrassing Information:** Cyber-attack may expose critical information in public domain. For example, the instances of individuals leaking information about governments secret programs.
 - **Sabotage:** The above situation may lead to misuse of such information by enemy country.

Question 2

- (a) *Discuss the pre-requisites of an effective MIS.* (6 Marks)
- (b) *Define and elaborate categories of risks that affect a system and taken into consideration at the time of assessment or audit of information systems.* (6 Marks)
- (c) *What is IT Governance? What are the key practices which determine the status of IT governance in the enterprise?* (4 Marks)

Answer 2

(a) The pre-requisites of an effective Management Information Systems (MIS) are as follows:

- o **Database** - It is collection of files, which is collection of records and records are nothing but collection of data. The data in database is organized in such a way that accessing to the data is improved and redundancy is reduced. The main characteristics of database are given as follows:
 - It is user-oriented.
 - It is capable of being used as a common data source to various users, helps in avoiding duplication of efforts in storage and retrieval of data and information.
 - It is available to authorized persons only.
 - It is controlled by a separate authority established for the purpose, known as Database Management System (DBMS).
- o **Qualified System and Management Staff** – The second pre-requisite of effective MIS is that it should be manned by qualified officers. These officers, who are experts in the field, should understand clearly the views of their fellow officers. For this, the organizational management base should comprise of two categories of officers - Systems and Computer Experts and Management experts.
 - Systems and Computer experts in addition to their expertise in their subject area/s should also be capable of understanding management concepts to facilitate the understanding of problems faced by the concern. They should also be clear about the process of decision making and information requirements for planning and control functions.
 - Management experts should also understand quite clearly the concepts and operations of a computer. This basic knowledge of computers will be useful to place them in a comfortable position, while working with systems technicians in designing or otherwise of the information system.
- o **Support of Top Management** – The support from top management is required for the effectiveness of MIS in an organization. The reasons for the same are as follows:
 - Any implementation, which does not receive the support of top management will not be effectively controlled and tends to get lesser priority and may be delayed or abandoned.
 - The resources involved in computer-based information systems are large and are growing larger in view of importance gained by management information system.
 - To gain the support of top management, the officers should place before top management all the supporting facts and state clearly the benefits, which will accrue from it to the concern. This step will certainly enlighten management, and will change their attitude towards MIS. Their wholehearted support and cooperation will help in making MIS an effective one.

- o **Control and maintenance of MIS-** Control of the MIS means the operation of the system as it was designed to operate. Some time, users develop their own procedures or short cut methods to use the system, which reduce its effectiveness. To check such habits of users, the management at each level in the organization should devise checks for the information system control. Maintenance is closely related to control. Formal methods for changing and documenting changes must be provided.
- (b) Risks that affect a system and are taken into consideration at the time of assessment or audit of information systems can be differentiated as Inherent risk, Control Risk and Detection Risk. They are as follows:
 - **Inherent Risk:** Inherent risk is the susceptibility of information resources or resources controlled by the information system to material theft, destruction, disclosure, unauthorized modification, or other impairment, assuming that there are no related internal controls. Inherent risk is the measure of auditor's assessment that there may or may not be material vulnerabilities or gaps in the audit subject exposing it to high risk before considering the effectiveness of internal controls. If the auditor concludes that there is a high likelihood of risk exposure, ignoring internal controls, the auditor would conclude that the inherent risk is high. For example, inherent risk would be high in case of auditing internet banking in comparison to branch banking or inherent risk would be high if the audit subject is an off-site. ATM in an example of the same. Internal controls are ignored in setting inherent risk because they are considered separately in the audit risk model as control risk. It is often an area of professional judgment on the part of an auditor.
 - **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.

- (c) **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. The objective of IT Governance is to determine and cause the desired behavior and results to achieve the strategic impact of IT. In other words, IT Governance is the system by which IT activities in a company or enterprise are directed and controlled to achieve business objectives with the ultimate objective of meeting stakeholder needs.

Key practices to determine status of IT Governance are as follows:

- Who makes directing, controlling and executing decisions?
- How the decisions are made?
- What information is required to make the decisions?
- What decision-making mechanisms are required?
- How exceptions are handled?
- How the governance results are monitored and improved?

Question 3

- (a) *Application programs are written, tested and documented to convert the design specifications into a functional system. Explain the characteristics that a good coded application program should have.* (6 Marks)
- (b) *Discuss the ways audit trails can be used to support security objectives.* (6 Marks)
- (c) *Explain the maintenance tasks undertaken in the Development of BCP.* (4 Marks)

Answer 3

- (a) Application programs are written, tested and documented to convert the design specifications into a functional system. A good coded application program should have the following characteristics:
- **Reliability:** It refers to the consistency with which a program operates over a period of time. However, poor setting of parameters and hard coding of some data subsequently could result in the failure of a program after some time.
 - **Robustness:** It refers to the applications' strength to uphold its operations in adverse situations by considering all possible inputs and outputs of a program in case of least likely situations.
 - **Accuracy:** It refers not only to 'what program is supposed to do', but should also take care of 'what it should not do'. The second part becomes more challenging for quality control personnel and auditors.
 - **Efficiency:** It refers to the performance per unit cost with respect to relevant parameters and it should not be unduly affected with the increase in input values.

- **Usability:** It refers to a user-friendly interface and easy-to-understand internal/external documentation.
 - **Readability:** It refers to the ease of maintenance of program even in the absence of the program developer.
- (b) Audit trails can be used to support security objectives in three ways:
- **Detecting Unauthorized Access to the system:** Detecting unauthorized access can occur in real time or after the fact. 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. After-the-fact, detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.
 - **Facilitating the Reconstruction of 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. For example, by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.
 - **Promoting 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.
- (c) The maintenance tasks undertaken in development of Business Continuity Planning (BCP) are to:
- Determine the ownership and responsibility for maintaining the various Business Continuity Planning (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.

Question 4

- (a) *"The intuitive character of executive decision making is reflected strongly in the types of information found most useful to executives". Discuss characteristics of the types of information used in executive decision making* (6 Marks)
- (b) *Describe the key benefits of IT Governance achieved at highest level in an organization.* (6 Marks)
- (c) *What are the main characteristics of detective controls which are designed to detect errors, omissions or malicious acts that occur?* (4 Marks)

Answer 4

- (a) "The intuitive character of executive decision-making is reflected strongly in the types of information found most useful to executives". The characteristics of the types of information used in executive decision making are as follows:
- o **Lack of structure** – Many of the decisions made by executives are relatively unstructured. These types of decisions are not as clear-cut as deciding how to debug a computer program or how to deal with an overdue account balance. Also, it is not always obvious, 'which data are required' or 'how to weigh available data when reaching a decision.'
 - o **High degree of uncertainty** – Executives work in a decision space that is often characterized by a lack of precedent. For example, when the Arab oil embargo hit in mid 1970s, no such previous event could be referenced for advice. Executives also work in a decision space where results are not scientifically predictable from actions. If prices are lowered, for instance, product demand will not automatically increase.
 - o **Future orientation** – Strategic-planning decisions are made to shape future events. As conditions change, enterprises must change also. It is the executive's responsibility to make sure that the organization keeps pointed toward the future. Some key questions about the future include: "How will future technologies affect what the company is currently doing? What will the competition (or the government) do next? What products will consumers demand five years from now?" As one can see, the answers to these questions about the future external environment are vital.
 - o **Informal Source** – Executives, more than other types of managers, rely heavily on informal source for key information. For example, lunch with a colleague in another firm might reveal some important competitor strategies. Informal sources such as television might also feature news of momentous concern to the executive – news that he or she would probably never encounter in the company's database or in scheduled computer reports.
 - o **Low level of detail** – Most important executive decisions are made by observing broad trends. This requires the executive to be more aware of the large overview than the tiny items. Even so, many executives insist that the answers to some questions can only be found by mucking through details.

- (b) The key benefits of IT Governance which are achieved by implementing/improving governance or management of enterprise, at the highest level in an organization 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.
- (c) The main characteristics of Detective controls which are designed to detect errors, omissions or malicious acts that occur are as follows:
- Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc.;
 - An established mechanism to refer the reported unlawful activities to the appropriate person or group;
 - Interaction with the preventive control to prevent such acts from occurring; and
 - Surprise checks by supervisor.

Question 5

- (a) *Discuss File Interrogation as one of the three levels of input validation controls. (6 Marks)*
- (b) *What is ITIL? Elaborate "service designs" under ITIL. (6 Marks)*
- (c) *Explain the key steps that can be followed for a risk-based approach to make an audit plan. (4 Marks)*

Answer 5

- (a) Input validation controls are intended to detect errors in the transaction data before the data are processed. File Interrogation is one of the three levels of input validation controls.
- o **Version Usage:** Proper version of a file should be used for processing the data correctly. In this regard it should be ensured that only the most current file be processed.
 - o **Internal and External Labeling:** Labeling of storage media is important to ensure that the proper files are loaded for process. Where there is a manual process for

loading files, external labeling is important to ensure that the correct file is being processed. Where there is an automated tape loader system, internal labeling is more important.

- o **Data File Security:** Unauthorized access to data file should be prevented, to ensure its confidentiality, integrity and availability. These controls ensure that the correct file is used for processing.
 - o **Before and after Image and Logging:** The application may provide for reporting of before and after images of transactions. These images combined with the logging of events enable re-constructing the data file back to its last state of integrity, after which the application can ensure that the incremental transactions/events are rolled back or forward.
 - o **File Updating and Maintenance Authorization:** Sufficient controls should exist for file updating and maintenance to ensure that stored data are protected. The access restrictions may either be part of the application program or of the overall system access restrictions.
 - o **Parity Check:** When programs or data are transmitted, additional controls are needed. Transmission errors are controlled primarily by detecting errors or correcting codes.
- (b) **IT Infrastructure Library (ITIL):** The ITIL is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. In its current form known as ITILv3, 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.

Service Design: Service Design is one of the five volumes in ITIL framework that translates strategic plans and objectives and creates the designs and specifications for execution through service transition and operations. It provides guidance on combining infrastructure, applications, systems, and processes, along with suppliers and partners, to present feasible service offerings. It further includes design principles and methods for converting strategic objectives into portfolios of services and service assets.

- **Service Catalogue Management:** Service Catalogue management maintains and produces the Service Catalogue and ensures that it contains accurate details, dependencies and interfaces of all services made available to customers. Service Catalogue information includes ordering and requesting processes, prices, deliverables and contract points.
- **Service Level Management:** Service-level management provides for continual identification, monitoring and review of the levels of IT services specified in the Service-Level Agreements (SLAs). Service-Level Management is the primary interface with the customer and is responsible for ensuring that the agreed IT services

are delivered when and where they are supposed to be; liaising with availability management, capacity management, incident management and problem management.

- **Availability Management:** Availability management targets allow organizations to sustain the IT service-availability to support the business at a justifiable cost. The high-level activities comprise of realizing availability requirements, compiling availability plan, monitoring availability and maintenance obligations. Availability management addresses many IT component abilities like reliability, maintainability, serviceability, resilience and security to perform at an agreed level over a period of time.
 - **Capacity Management:** Capacity management supports the optimum and cost-effective provision of IT services by helping organizations match their IT resources to business demands. The high-level activities include application sizing; workload management; demand management; modeling; capacity planning; resource management and performance management.
 - **IT Service Continuity Management:** IT Service Continuity Management (ITSCM) covers the processes by which plans are put in place and managed to ensure that IT services can recover and continue even after a serious incident occurs.
 - **Information Security Management:** A basic goal of security management is to ensure adequate information security, which in turn, is to protect information assets against risks, and thus to maintain their value to the organization. This is commonly expressed in terms of ensuring their confidentiality, integrity and availability, along with related properties or goals such as authenticity, accountability, non-repudiation and reliability.
 - **Supplier Management:** The purpose of Supplier Management is to obtain value for money from suppliers and contracts. It ensures that underpinning contracts and agreements align with business needs, Service Level Agreements and Service Level Requirements. Supplier Management oversees process of identification of business needs, evaluation of suppliers, establishing contracts, their categorization, management and termination.
- (c) The key steps that can be followed for a risk-based approach to make an audit plan are as follows:
- Inventory the information systems in use in the organization and categorize them.
 - Determine which of the systems impact critical functions or assets, such as money, materials, customers, decision making, and how close to real time they operate.
 - Assess what risks affect these systems and the severity of the impact on the business.
 - Based on the above assessment, decide the audit priority, resources, schedule and frequency.

Question 6

- (a) *Proper assessment of the degree of risk is critical to the effectiveness of the audit. Discuss some of the critical factors to be considered by an IS Auditor as part of his/her preliminary review.* (6 Marks)
- (b) *“A variety of tasks during the SDLC are performed by special teams/individuals.” Define in brief the role(s) of – (i) Systems Analyst (ii) Programmer (iii) Database Administrators (iv) Domain Specialist (v) IS Auditor (vi) Quality Assurance.* (6 Marks)
- (c) *What competencies are necessary for personnel assigned specific management responsibilities within the system while developing BCM?* (4 Marks)

Answer 6

- (a) Proper assessment of the degree of risk is critical to the effectiveness of the audit. The following are some of the critical factors to be considered by an IS auditor as part of his/her preliminary review.
- (i) **Knowledge of the Business:** Related aspects are General economic factors and industry conditions affecting the entity's business; Nature of Business, its products & services; General exposure to business; Its clientele, vendors and most importantly, strategic business partners/associates to whom critical processes have been outsourced; Level of competence of the Top management and IT Management, and finally, Set up and organization of IT department.
 - (ii) **Understanding the Technology:** This includes the process to gain a good understanding of the technology environment and related control issues. This could include consideration of analysis of business processes and level of automation; 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 and finally, Studying IT policies, standards, guidelines and procedures.
 - (iii) **Understanding Internal Control Systems:** For gaining understanding of Internal Controls emphasis is to be placed on compliance and substantive testing.
 - (iv) **Legal Considerations and Audit Standards:** The auditor should carefully evaluate the legal as well as statutory implications on his/her audit work. The Information Systems audit work could be required as part of a statutory requirement in which case he should take into consideration the related stipulations, regulations and guidelines for conduct of his audit. The statutes or regulatory framework may impose stipulations about minimum set of control objectives to be achieved by the subject organization.

Sometimes, this may also include restrictions on the use of certain types of technologies e.g. freeware, shareware etc. The IS Auditor should also consider the Audit Standards applicable to his conduct and performance of audit work. Non-compliance with the mandatory audit standards would not only impact on the violation of the code of professional ethics but also have an adverse impact on the auditor's work.

- (v) **Risk Assessment and Materiality:** Risk Assessment is a critical and inherent part of the Information Systems Auditor's planning and audit implementation. It implies the process of identifying the risk, assessing the risk, and recommending controls to reduce the risk to an acceptable level, considering both the probability and the impact of occurrence. Risk assessment allows the auditor to determine the scope of the audit and assess the level of audit risk and error risk (the risk of errors occurring in the area being audited).
- (b) A variety of tasks during the System Development Life Cycle (SDLC) are performed by special teams/individuals. The roles are as follows:
 - (i) **Systems Analyst:** The systems analyst's main responsibility is to conduct interviews with users and understand their requirements. S/he is a link between the users and the designers/programmers, who convert the users' requirements in the system requirements and plays a pivotal role in the Requirements analysis and Design phase.
 - (ii) **Programmer:** Programmer is a mason of the software industry, who converts design into programs by coding using programming language. Apart from developing the application in a programming language, they also test the program for debugging activity to assure correctness and reliability.
 - (iii) **Database Administrators:** The data in a database environment must be maintained by a specialist in database administration to support the application program. The DBAs handle multiple projects; ensures the integrity and security of information stored in the database and helps the application development team in database performance issues. Inclusion of new data elements must be done only with the approval of the database administrator.
 - (iv) **Domain Specialist:** Whenever a project team must develop an application in a field that's new to them, they take the help of a domain specialist. For example, if a team undertakes application development in Insurance, about which they have little knowledge, they may seek the assistance of an Insurance expert at different stages. This makes it easier to anticipate or interpret user needs. A domain specialist need not have knowledge of software systems.
 - (v) **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.

- (vi) **Quality Assurance:** This team sets the standards for development, and checks compliance with these standards by project teams on a periodic basis. Any quality assurance person, who has participated in the development process, shall not be viewed as 'independent' to carry out quality audits.
- (c) While developing the BCM, the competencies necessary for personnel assigned specific management responsibilities within the system are as follows:
- Actively listens to others, their ideas, views and opinions;
 - Provides support in difficult or challenging circumstances;
 - Responds constructively to difficult circumstances;
 - Adapts leadership style appropriately to match the circumstances;
 - Promotes a positive culture of health, safety and the environment;
 - Recognizes and acknowledges the contribution of colleagues;
 - Encourages the taking of calculated risks;
 - Encourages and actively responds to new ideas;
 - Consults and involves team members to resolve problems;
 - Demonstrates personal integrity; and
 - Challenges established ways of doing things to identify improvement opportunities.

Question 7

Write short notes on any *four* of the following:

- (a) *Types of back –ups*
- (b) *Indian Computer Emergency Response Team*
- (c) *Major Components of WEB 3.0*
- (d) *Final Acceptance Testing*
- (e) *Advantages of BYOD*

(4 x 4 =16 Marks)

Answer 7

- (a) Various types of back-ups are as follows:
- **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.
 - **Incremental Backup:** An incremental backup captures files that were created or changed since the last backup, regardless of backup type. This is the most economical method, as only the files that changed since the last backup are backed

up. This saves a lot of backup time and space. Normally, incremental backup is very difficult to restore. One will have to start with recovering the last full backup, and then recovering from every incremental backup taken since.

- **Differential Backup:** A differential backup stores files that have changed 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 backup. 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.
 - **Mirror back-up:** 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) **Indian Computer Emergency Response Team (CERT – In):** The Section 70B of IT (Amendment) Act, 2008 provides guidelines on how Indian Computer Emergency Response Team serves as national agency for incident response. The team shall serve as the national agency for performing the following functions in Cyber Security, which are as follows:
- Collection, analysis and dissemination of information on cyber incidents;
 - Forecast and alerts of cyber security incidents;
 - Emergency measures for handling cyber security incidents;
 - Coordination of cyber incidents response activities;
 - Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
 - Such other functions relating to cyber security as may be prescribed.
- (c) The two major components of Web 3.0 are as follows:
- (i) **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.
 - (ii) **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.

To conclude, Web 3.0 helps to achieve a more connected open and intelligent web applications using the concepts of natural language processing machine learning, machine reasoning and autonomous agents.

- (d) **Final Acceptance Testing:** It is a type of System Testing under Systems Development Life Cycle (SDLC) which is conducted when the system is just ready for implementation. During this testing, it is ensured that the new system satisfies the quality standards adopted by the business and the system satisfies the users.

The final acceptance testing has two major parts:

- **Quality Assurance Testing:** It ensures that the new system satisfies the prescribed quality standards and the development process is as per the organization's quality assurance policy, methodology and prescriptions.
- **User Acceptance Testing:** It ensures that the functional aspects expected by the users have been well addressed in the new system. Alpha Testing and beta Testing are two types of the user acceptance testing. Alpha Testing is the first stage often performed by the users within the organization by the developers to improve and ensure the quality / functionalities as per user satisfaction. Beta testing is the second stage generally performed by the external users after deployment of the system.

- (e) **Advantages of Bring Your Own Device (BYOD)** are as follows:

- **Happy Employees:** Employees love to use their own devices when at work. This also reduces the number of devices an employee has to carry; otherwise he would be carrying his personal as well as organization provided devices.
- **Lower IT budgets:** The employees could involve financial savings to the organization since employees would be using the devices they already possess, thus reducing the outlay of the organization in providing devices to them.
- **IT reduces support requirement:** IT department does not have to provide end user support and maintenance for all these devices resulting in cost savings.
- **Early adoption of new Technologies:** Employees are generally proactive in adoption of new technologies that result in enhanced productivity of employees leading to overall growth of business.
- **Increased employee efficiency:** The efficiency of employees is more when the employee works on his/her own device. In an organization provided devices, employees have to learn and there is a learning curve involved in it.