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

E-quip Limited has worldwide operations and is engaged in the business of manufacturing and supply of electronic equipment through its various outlets in India and abroad. Recognizing the advantages of connectivity through internet, the Management decides to sell its products in on-line mode by using Cloud Computing technology to achieve this objective.

The Company appoints a technical team for the development of the Company's new web application. The team calls for various meetings of different stakeholders and decides to follow the best practices of SDLC for its different phases. Keeping the importance of information security in the current vulnerable world, it suggests that security issues must be considered from the beginning itself. Accordingly, Business Impact Analysis (BIA) was done as a part of Business Continuity Management (BCM). As the auditor member of the technical team, the Management of E-quip Limited wants you to advise them on the following issues:

(a) What are the advantages and important implications of the proposed Information System for the Company? (5 Marks)

(b) What are the tasks you will undertake to ensure that BCM program is in place, while assessing BIA? (5 Marks)

(c) Management wants to know the major challenges in using Cloud Computing technology for running the new web application. Write any five challenges. (5 Marks)

(d) Explain briefly major ways to control remote and distributed data processing in the new Web Application. (5 Marks)

Answer

(a) The major advantage of the proposed Information system will be that it will enable the E-quip Limited to sell its products in an online mode in India and abroad through Internet connectivity by using Cloud Computing Technology. The proposed Information system will support company's business processes and operations; better business decision making; and will provide strategic and competitive advantage to ensure better quality and supply of its electronic equipments.

Following are some of the important implications of proposed Information Systems in business for E-Quip Limited:

- Information system helps managers in efficient decision-making to achieve the organizational goals.

- An organization will be able to survive and thrive in a highly competitive environment on the strength of a well-designed Information system.
- Information systems helps in making right decision at the right time i.e. just on time.
- A good information system may help in generating innovative ideas for solving critical problems.
- Knowledge gathered though Information system may be utilized by managers in unusual situations.
- Information system is viewed as a process; it can be integrated to formulate a strategy of action or operation.

(b) Business Impact Analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. The tasks to be undertaken to ensure that BCM program is in place while assessing BIA are as follows:

- 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.

(c) Major challenges in Cloud Computing Technology for running new Web application are as follows:

- **Confidentiality:** Prevention of the unauthorized disclosure of the data is referred as Confidentiality. With the use of encryption and physical isolation, data can be kept secret.
- **Integrity:** Integrity refers to the prevention of unauthorized modification of data and it ensures that data is of high quality, correct, consistent and accessible.
- **Availability:** Availability refers to the prevention of unauthorized withholding of data and it ensures the data backup through Business Planning Continuity Planning (BCP) and Disaster Recovery Planning (DRP). Temporary breakdowns, sustained and Permanent Outages, Denial of Service (DoS) attacks, equipment failure and natural calamities are all threats to availability.

- **Governance:** Due to the lack of control over the employees and services, there is problem relating to design, implementation, testing and deployment. So, there is a need of governance model, which controls the standards, procedures and policies of the organization.
- **Trust:** Trust ensures that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the Cloud provider, and their performance over time.
- **Legal Issues and Compliance:** There are various types of laws and regulations that impose security and privacy duties on the organization and potentially impact Cloud computing initiatives such as demanding privacy, data location and security controls, records management, and E-discovery requirements.
- **Privacy:** The privacy issues are embedded in each phase of the Cloud design that includes both the legal compliance and trusting maturity.
- **Audit:** Auditing is type of checking that 'what is happening in the Cloud environment'. It is an additional layer before the virtualized application environment, which is being hosted on the virtual machine to watch 'what is happening in the system'.
- **Data Stealing:** In a Cloud, data stored anywhere is accessible in public form and private form by anyone at any time. Some of the Cloud providers use server/s from other service providers and thus there is a probability that the data is less secure and is more prone to the loss from external server.
- **Architecture:** In the architecture of Cloud computing models, there should be a control over the security and privacy of the system. The reliability and scalability of architecture is dependent on the design and implementation to support the overall framework.
- **Identity Management and Access control:** A robust federated identity management architecture and strategy internal in the organization provides a trust and shares the digital attributes between the Cloud provider and organization ensuring the protection against attackers.
- **Incident Response:** It ensures to meet the requirements of the organization during an incident. It ensures that the Cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident.
- **Software Isolation:** Software isolation is to understand virtualization and other logical isolation techniques that the Cloud provider employs in its multi-tenant software architecture and evaluate the risks required for the organization.
- **Application Security:** Security issues relating to application security still apply when applications move to a cloud platform. Service provider should have the

complete access to the server with all rights for the purpose of monitoring and maintenance of server.

(d) Remote and distributed data processing applications can be controlled in many ways. Some of these are given as follows:

- Remote access to computer and data files through the network should be implemented.
- Having a terminal lock can assure physical security to some extent.
- Applications that can be remotely accessed via modems and other devices should be controlled appropriately.
- Terminal and computer operations at remote locations should be monitored carefully and frequently for violations.
- In order to prevent the unauthorized users' access to the system, there should be proper control mechanisms over system documentation and manuals.
- Data transmission over remote locations should be controlled. The location which sends data should attach needed control information that helps the receiving location to verify the genuineness and integrity.
- When replicated copies of files exist at multiple locations, it must be ensured that all are identical copies that contain the same information and checks are also done to ensure that duplicate data does not exist.

Question 2

(a) You are appointed to audit the Information Systems of ABC Limited. As a part of preliminary evaluation, list the major aspects which you would study to gain a good understanding of the technology environment and the related control issues. (6 Marks)

(b) Software Applications require interface between user and the business functions. Discuss User Controls describing various types of controls to be exercised to achieve system effectiveness and efficiency. (6 Marks)

(c) As an IS auditor, what are the key areas you would verify during review of BCM arrangements of an enterprise. (6 Marks)

Answer

(a) As a part of preliminary evaluation, the major aspects which should be studied to gain a good understanding of the technology environment and related control issues are as follows:

- 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.

(b) **User Controls:** Application system represents the interface between the user and the business functions. From the users' perspective, it is the applications that drive the business logic and thus User Controls are required.

The user controls that are to be exercised for system effectiveness and efficiency are as follows:

- **Boundary Controls:** These establish interface between the user of the system and the system itself. The system must ensure that it has an authentic user. Further users are allowed using resources in restricted ways.
- **Input Controls:** Responsible for ensuring the accuracy and completeness of data and instruction input into an application system. Input Controls are validation and error detection of data input into the system.
- **Processing Controls:** These controls are responsible for computing, sorting, classifying and summarizing data. These maintain the chronology of events from the time data is received from input or communication systems to the time data is stored into the database or output as results.
- **Output Controls:** These controls provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared and routed to users.
- **Database Controls:** These are responsible to provide functions to define, create, modify, delete and read data in an information system. These maintain procedural data-set of rules to perform operations on the data to help a manager to take decisions.

(c) During review of BCM arrangements of an enterprise, an IS auditor should verify that:

- 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' 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 that have been 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.

Question 3

(a) Many-a-time organizations fail to achieve their system development objectives. Justify the statement giving reasons. (6 Marks)

(b) Office Automation Systems (OAS) is the most rapidly expanding system. Describe the broad groups of OAS based on the types of its operations. (6 Marks)

(c) The manner of selecting auditors builds confidence among various stakeholders. Describe SEBI norms for selecting an auditor. (6 Marks)

Answer

(a) Many-a-time organizations fail to achieve their systems development objectives. Some of the most notable reasons for this are as follows:

(i) **User Related Issues:** It refers to those issues where user/customer is reckoned as the primary agent.

- **Shifting User Needs:** User requirements for IT are constantly changing and 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.
- **Lack of User Participation:** Users must participate in the development efforts to define their requirements, feel ownership for project success, and work to resolve development problems.
- **Inadequate Testing and User Training:** New systems must be tested before

installation to determine that they operate correctly and users must be trained to effectively utilize the new system.

(ii) **Developer Related Issues:** It refers to the issues and challenges with regard to the developers.

- **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.

(iii) **Management Related Issues:** It refers to the bottlenecks with regard to organizational set up, administrative and overall management to accomplish the system development goals.

- **Lack of Senior Management Support and Involvement:** Senior management must provide guidance to developers and users of information systems in terms of which development projects are important so that they act accordingly.
- **Development of Strategic Systems:** Because strategic decision making is unstructured; the requirements, specifications, and objectives for such development projects are difficult to define.

(iv) **New Technologies:** When an organization tries to create a competitive advantage by applying advance technologies, it generally finds that attaining system development objectives is more difficult because personnel are not as familiar with the new technologies in practice. To obtain a required skill set in order to adapt new technologies becomes a major challenge for the organizations.

(b) Office Automation Systems (OAS) is most rapidly expanding computer based information systems. The broad groups that can be formed on the basis of its operations are as follows:

(i) **Text processing system:** The text processing system automates the process of document capture and/ or creation of new documents such as letters, reports, memo etc. This permits use of standard stored information to produce personalized documents. It reduces effort and minimizes the chances of errors.

(ii) **Electronic Document Management system:** It captures the information contained in documents, stored for future reference and makes them available to the users as and when required. These systems are very helpful in remote access of documents and internal communication through network. It also helps to keep record of resources utilization.

(iii) **Electronic message communication system:** The electronic message communication system helps in receipts and distribution of electronic records. It offers a lot of economy in terms of reduced time in sending or receiving the message; online development and editing; broadcasting and rerouting; and integration with other information system. E-mail, Fax, and voice mail are important OAS.

(iv) **Teleconferencing and Video Conferencing systems:** This OAS helps in receipt and distribution of information involving more than two persons located at two or more different places through audio or video with or without computer system

(c) The SEBI norms for Auditor Selection are as follows:

- Auditor must have minimum 3 years of experience in IT audit of Securities Industry participants e.g. stock exchanges, clearing houses, depositories etc. The audit experience should have covered all the major Areas mentioned under SEBI's Audit Terms of Reference (TOR).
- The Auditor must have experience in/direct access to experienced resources in the areas covered under TOR. It is recommended that resources employed shall have relevant industry recognized certifications e.g. CISA (Certified Information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium (ISC)².
- The Auditor should have IT audit/governance frameworks and processes conforming to industry leading practices like CoBIT.
- The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the Exchange/Depository. He should not have been engaged over the last three years in any consulting engagement with any departments/units of the entity being audited.
- The Auditor may not have any cases pending against its previous auditees, which fall under SEBI's jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.

Question 4

(a) Do you consider Corrective Controls are a part of Internal Controls? Describe the characteristics of Corrective Controls. (6 Marks)

(b) Different auditors go about IS auditing in different ways. Despite this, IS audit process can be categorized into broad categories. Discuss the statement explaining broad steps involved in the process. (6 Marks)

(c) Testing a program unit is essential before implementing it. Name any four categories of test; a programmer typically performs on a programmable unit. (4 Marks)

Answer

(a) Yes, we consider Corrective Controls to be a part of Internal Controls. Corrective controls are designed to reduce the impact or correct an error once it has been detected. Contingency planning, Backup procedure, Rerun procedures, and Investigate budget variance and report violations are some of the examples of corrective controls.

The main characteristics of the corrective controls are as follows:

- Minimizing the impact of the threat;
- Identifying the cause of the problem;
- Providing remedy to the problems discovered by detective controls;
- Getting feedback from preventive and detective controls;
- Correcting error arising from a problem; and
- Modifying the processing systems to minimize future occurrences of the incidents.

(b) Information Systems (IS) audit process can broadly be categorized on the basis of audit of Systems and applications; Information processing facilities; Systems Development; IT management and enterprise architecture; and Telecommunications, Intranets and Extranets.

Different auditors go about IS auditing in different ways. However, broadly the steps involved in an IS audit process are as follows:

(i) **Scoping and pre-audit survey:** Auditors determine the main area/s of focus and any areas that are explicitly out-of-scope, based on the scope-definitions agreed with management.

(ii) **Planning and preparation:** During which the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan or risk-control-matrix.

(iii) **Fieldwork:** Gathering evidences by interviewing staff and managers; reviewing documents, and observing processes etc.

(iv) **Analysis:** This step involves desperately sorting out, reviewing and trying to make sense of all that evidence gathered earlier. SWOT (Strengths, Weaknesses, Opportunities, Threats) or PEST (Political, Economic, Social, Technological) techniques can be used for analysis.

(v) **Reporting:** Reporting to the management is done after analysis of evidence gathered and analyzed.

(vi) **Closure:** Closure involves preparing notes for future audits and follow up with management to complete the actions they promised after previous audits.

(c) There are five categories of tests that a programmer typically performs on a program unit. These are described as follows:

- **Functional Tests:** To check 'whether programs do, what they are supposed to do or not'.
- **Performance Tests:** To verify the response time, the execution time, the throughput etc.
- **Stress Tests:** To determine the limitations of the program.
- **Structural Tests:** To examine the internal processing logic of a software system.
- **Parallel Tests:** To compare the output of the same data processed in new and old system.

Question 5

(a) Mr. A has hacked into Defence Information Systems with an intention to steal classified information that threatens the security and sovereignty of India. He has used the services of a local cafe, 'CyberNet' for this purpose. The owner of 'CyberNet' tries to stop Mr. A but is threatened by Mr. A. Hence the owner of 'CyberNet' does not disclose A's activities to anyone. Mr. A is caught by the Vigilance Officers of the department.

(i) Is Mr. A punishable for his activities?

(ii) Is the intermediary, 'CyberNet' liable?

Please discuss the liabilities enunciated under the relevant sections of the Information Technology Act, 2000 in the above two cases. (6 Marks)

(b) The Management of IT related risks is a key part of Enterprise Governance. Name the key management practices to achieve this objective. (6 Marks)

(c) State four major tasks performed by an Operating System while allowing users and their applications to share and access common resources. (4 Marks)

Answer

(a) (i) Yes, Mr. A is punishable for his activities under the Section 66F.

[Section 66F(1)(B)] Punishment for cyber terrorism

Whoever knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the

advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

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

Considering the facts provided in the case where Mr. A hacked into Defense Information System with an intention to steal classified information threatening the security and sovereignty of India, Mr. A is punishable for his activities.

(ii) Yes, Intermediary 'CyberNet' is liable under the Section 79.

[Section 79] Exemption from liability of intermediary in certain cases

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him.

(2) The provisions of sub-section (1) shall apply if -

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or

(b) the intermediary does not-

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

Thus, according to Section 79(2)(c); the Intermediary 'CyberNet' failed to observe due diligence in discharging his duties and also the other guidelines as prescribed by the Central Government. So, Intermediary 'CyberNet' is liable.

(b) The key Management Practices for implementing IT Risk Management are given as follows:

- **Collect Data:** To enable effective IT related risk identification, analysis and reporting.
- **Analyze Risk:** To develop useful information to support risk decisions.
- **Maintain a Risk Profile:** To maintain an inventory of known risks and risk attributes.

- **Articulate Risk:** To inform IT- related exposures and opportunities to all required stakeholders for appropriate response.
- **Define a Risk Management Action Portfolio**: To manage opportunities and reduce risk to an acceptable level as a portfolio.
- **Respond to Risk:** To respond limit the magnitude of loss from IT related events in a timely manner.

(c) 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. Some of the major tasks performed by an Operating system are as follows:

- **Scheduling Jobs:** They can determine the sequence in which jobs are executed, using priorities established.
- **Managing Hardware and Software Resources:** They can first cause the user's application program to be executed by loading it into primary storage and then cause the various hardware units to perform as specified by the application.
- **Maintaining System Security:** They may require users to enter a password - a group of characters that identifies users as being authorized to have access to the system.
- **Enabling Multiple User Resource Sharing:** They can handle the scheduling and execution of the application programs for many users at the same time, a feature called multiprogramming.
- **Handling Interrupts:** An interrupt is a technique used by the operating system to temporarily suspend the processing of one program in order to allow another program to be executed. Interrupts are issued when a program requests an operation.
- **Maintaining Usage Records:** They can keep track of the amount of time used by each user for each system unit - the CPU, secondary storage, and input and output devices.

Question 6

(a) Discuss key management practices required for aligning IT Strategy with Enterprise Strategy.

(6 Marks)

(b) You are selected by UVW Limited to review and strengthen Software Access Control mechanism for their Company. Prepare a report on the need of boundary controls enlisting major boundary control techniques to be implemented by them. (6 Marks)

(c) A business manager should have adequate knowledge to operate Information Systems effectively. Elaborate. *(4 Marks)*

Answer

(a) The key management practices, which are required for aligning IT strategy with enterprise Strategy is as follows:

- **Understand enterprise direction:** This considers the current enterprise environment and business processes; enterprise strategy and future objectives and also the external environment of the enterprise.
- **Assess the current environment, capabilities and performance:** This assesses the performance of current internal business and IT capabilities and external IT services, and develops an understanding of the enterprise architecture in relation to IT.
- **Define the target IT capabilities:** This defines the target business and IT capabilities and required IT services on the basis of enterprise environment and requirements; assessment of the current business process and IT environment and issues; and consideration of reference standards, best practices.
- **Conduct a gap analysis:** This identifies the gaps between the current and target environments and considers the alignment of assets with business outcomes to optimize investment.
- **Define the strategic plan and road map:** This creates a strategic plan that defines, in cooperation with relevant stakeholders, how IT- related goals will contribute to the enterprise's strategic goals.
- **Communicate the IT strategy and direction:** This creates awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy.

(b) The company UVW Limited intends to review and strengthen its Software Access Control mechanism. To achieve this objective, the Boundary controls can be put in place that will establish interface between the user of the system and the system itself. The major controls of the boundary system are the access control mechanisms that links the authentic users to the authorized resources, they are permitted to access and thus are the line of control for intruders to gain access to UVW Company's asset. The access control mechanism has three steps of Identification, Authentication and Authorization with respect to the access control policy implemented. The user can provide three factors of input information for the authentication process and gain access to his required resources.

Major Boundary Control techniques are as follows:

- **Cryptography:** It deals with programs for transforming data into cipher text that are meaningless to anyone, who does not possess the authentication to access the

respective system resource or file. Techniques of cryptography are Transposition, Substitution and Product Cipher.

- **Passwords:** User identification by an authentication mechanism with personal characteristics like name, birth date, employee code, function, designation or a combination of two or more of these can be used as a password boundary access control.
- **Personal Identification Numbers (PIN):** PIN, similar to a password assigned to a user by an institution, is a random number stored in its database independent to a user identification details, or a customer selected number.
- **Identification Cards:** Identification cards are used to store information required in an authentication process. These cards are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.
- **Biometric Devices:** Biometric identification e.g. thumbs and/or finger impression, eye retina etc. are also used as boundary control techniques.

(c) 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.

Question 7

Write short notes on any four of the following:

(a) Principles of COBIT 5. *(4 Marks)*

(b) Effect of Computers on Evidence Collection for audit. *(4 Marks)*

(c) Back-up option sites for Alternate processing facility arrangements. *(4 Marks)*

d) Best practices of Green IT. *(4 Marks)*

(e) Vulnerability. *(4 Marks)*

Answer

(a) Principles of COBIT 5

- **Principle 1: Meeting Stakeholder Needs -** COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT. An enterprise can customize COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific; IT related goals and mapping these to specific processes and practices.
- **Principle 2: Covering the Enterprise End-to-End -** COBIT 5 integrates governance of enterprise IT into enterprise governance. COBIT 5 covers all functions and processes within the enterprise and considers all IT related governance and management enablers to be enterprise-wide and end-to-end.
- **Principle 3: Applying a Single Integrated Framework -** COBIT 5 is a single and integrated framework as it aligns with other latest relevant standards and frameworks, thus allowing the enterprise to use COBIT 5 as the overarching governance and management framework integrator.
- **Principle 4: Enabling a Holistic Approach -** COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT that require a holistic approach, taking into account several interacting components.
- **Principle 5: Separating Governance from Management -** The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organizational structures and serve different purposes.

(b) Effects of Computers on Evidence Collection for Audit: 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 due to which the auditor may not be able to review a whole reporting period transactions on the computer system.
- **Absence of input documents:** Transaction data may be entered into the computer directly without the presence of supporting documentation resulting 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 of time; thus making the auditor's job very difficult.
- **Lack of availability of printed output:** In the absence of physical output, it may be necessary for the auditor to directly access the electronic data retained on the client's computer.

- **Audit evidence:** Certain transactions may be generated automatically by the computer system.
- **Legal issues:** Making use of Electronic Data Interchange (EDI) and electronic trading over the Internet 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.

(c) Security administrators should consider the following Backup option sites for alternate processing facility arrangements:

- **Cold site:** A cold site has all the facilities needed to install a mainframe system-raised floors, air conditioning, power, communication lines, and so on. An organisation can establish its own cold-site facility or enter into an agreement with another organisation to provide a cold-site facility.
- **Hot site:** All hardware and operations facilities will be available at the hot site. In some cases, software, data and supplies might also be stored there. A hot site is expensive to maintain and are usually shared with other organisations that have hot-site needs.
- **Warm site:** A warm site provides an intermediate level of backup. It has all cold-site facilities in addition to the hardware that might be difficult to obtain or install.
- **Reciprocal agreement:** Two or more organisations might agree to provide backup facilities to each other in the event of one suffering a disaster. This backup option is relatively cheap, but each participant must maintain sufficient capacity to operate another's critical system.

(d) Best practices of Green IT are as follows:

- Involving stakeholders on campus yields policies and green IT initiatives more likely to be embraced by the campus community.
- Partnering takes advantage of existing efforts and ensures wider reach and more effective use of limited resources.
- Guidelines for using the best practices simplify adaption of green IT by campus users and encourage them to consider green computing practices the norm.
- On-going communication about and campus commitment to green IT best practices to produce notable results.

(e) **Vulnerability:** Vulnerability is the weakness in the system safeguards that exposes the system to threats and can be exploited by the attackers. The weakness may be in information system/s, cryptographic systems or other components e.g. system security procedures, hardware design, internal controls that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system.

Some examples of vulnerabilities are as follows:

- Leaving the front door unlocked makes the house vulnerable to unwanted visitors.
- Short passwords (less than 6 characters) make the automated information system vulnerable to password cracking or guessing routines.

In other words, Vulnerability is a state in a computing system (or set of systems), which must have at least one condition, out of the following:

- 'Allows an attacker to execute commands as another user' or
- 'Allows an attacker to access data that is contrary to the specified access restrictions for that data' or
- 'Allows an attacker to pose as another entity' or
- 'Allows an attacker to conduct a denial of service'.