

PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

Concepts of Governance and Management of Information Systems

1. (a) What is Governance of Enterprise IT (GEIT)? Explain its key benefits in brief.
(b) Discuss key management practices for implementing risk management.
2. Discuss the areas, which should be reviewed by Internal Auditors as a part of the review of Governance, Risk and Compliance (GRC).
3. Discuss the key management practices for assessing and evaluating the system of Internal Controls in an enterprise in detail.

Information Systems Concepts

4. What do you understand by Transaction Processing System (TPS)? Briefly discuss the key activities involved in a TPS.
5. (a) Briefly discuss major misconceptions about Management Information System (MIS).
(b) 'There are various constraints, which come in the way of operating an MIS'. Explain any four such constraints in brief.
6. What is Executive Information Systems (EIS)? Explain major characteristics of an EIS.

Protection of Information Systems

7. (a) What are the key components of a good Security Policy? Explain in brief.
(b) Discuss five interrelated components of Internal Controls.
8. What do you understand by Boundary Controls? Explain major boundary control techniques in brief.
9. (a) Briefly explain major Data Integrity Policies.
(b) What do you understand by Asynchronous Attacks? Explain various forms of asynchronous attacks in brief.

Business Continuity Planning and Disaster Recovery Planning

10. (a) Discuss the objectives of Business Continuity Planning (BCP).
(b) While developing a Business Continuity Plan, what are the key tasks that should be covered in the second phase 'Vulnerability Assessment and General definition of Requirement'?
11. (a) Discuss the maintenance tasks undertaken in the development of a 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?

Acquisition, Development and Implementation of Information Systems

12. (a) Describe major strengths of Prototyping Model.
(b) What are the possible advantages of System Development Life Cycle (SDLC) from the perspective of IS Audit?
13. Explain two primary methods, which are used for the analysis of the scope of a project in System Development Life Cycle (SDLC).
14. Bring out the reasons as to why organizations fail to achieve their Systems Development Objectives?

Auditing of Information Systems

15. Discuss the issues relating to the performance of evidence collection and understanding the reliability of controls.
16. What do you understand by System Control Audit Review File (SCARF) technique? Explain various types of information collected by using SCARF technique in brief.

Information Technology Regulatory Issues

17. (a) Explain the objectives of the Information Technology Act, 2000.
(b) Discuss the 'Use of Electronic Records in Government and its agencies' in the light of Section 6 of Information Technology Act 2000.
18. Mr. A has received some information about Mr. B on his mobile phone. He knows that this information has been stolen by the sender. He not only retained this information but also sent it to Mr. B and his friends. Because of this act, Mr. B is annoyed and his life is in danger. Read the above carefully and answer the following:
 - (a) Under what sections of IT Act, 2000; Mr. B can file an FIR with police against Mr. A? Discuss the related provisions in detail.
 - (b) Mr. A is reasonably suspected of having committed an offence under the IT Act, 2000. Specify the rank of police officers, who can search and arrest him and the concerned section of the said Act. Also explain the related provisions in detail.

Emerging Technologies

19. (a) Discuss the major goals of Cloud Computing in brief.
(b) What do you understand by Public Cloud? Also discuss its major advantages in brief.
20. (a) 'The work habits of computer users and businesses can be modified to minimize adverse impact on the global environment'. Discuss some of such steps, which can be followed for Green IT.

- (b) Discuss any four challenges to Cloud Computing in brief.

Questions based on Short Notes/Differential between various concepts

21. Write short notes on the following:
- (a) Trojan Horse
 - (b) Snapshots
 - (c) Test Plan under BCP & DRP
 - (d) Audit Hooks
22. Differentiate between the following:
- (a) Black Box Testing and White Box Testing.
 - (b) Differential Backup and Full Backup.
 - (c) Structured English and Flowchart.

Questions based on the Case Studies

23. ABC Ltd. is a company dealing in electronic items through its various offices in India and abroad. Currently, the company is using various stand-alone systems, which are found to be on higher risk due to technology as well as supplier/s. By recognizing the importance of Information Technology, it intends to implement E-Governance system at all of its departments. Dependency on electronic information and IT systems is essential to support critical business processes. Accordingly, a system analyst is engaged to conduct requirements analysis and investigation of the present system. In addition, he also highlighted the importance of Risk Management and suggested that the management of IT related risks is now being understood as a key part of enterprise governance; hence, it must be managed properly. As a result of the same, efficient ways were explored to achieve the goals especially for risk management. Research Studies reveal that cost and efforts may be reduced up to a considerable level by reducing risk from the beginning in the SDLC.

Read the above carefully and answer the following:

- (a) What do you mean by System Requirements Analysis? What are the activities to be performed during System Requirement Analysis phase?
 - (b) Explain various Risk Management Strategies. In your opinion, which strategy you will recommend in this scenario and why?
 - (c) Agile methodology is one of the popular approaches of system development. What are the major strengths of this methodology in your opinion?
24. PQR Institute is a distance learning Institute offering various professional courses, which are popular across the world. One of the prominent reasons of the popularity of the courses is rigorous examination system of the Institute, which is currently a manual

process. It is observed that its students are facing problems regarding their routine work and queries due to this manual process. In addition, they are required to visit the Institute physically even for very small tasks. In view of these aforementioned facts, the Controller of Examinations decided to launch a web based Portal to facilitate the students of different courses. It is proposed to upload the examination forms, admit cards, results etc. of various courses on this Portal. It is expected that the portal will be very useful for the students as it aims to provide the access of various examination related resources on anytime anywhere basis. For the implementation of this project, a technical consultant was appointed by the Institute. Accordingly, an initial feasibility study under various dimensions was done and a detailed report was submitted. As a next step, as per the recommendations of the consultant, an expression of interest was published by the Institute in various national/regional newspapers inviting organizations to showcase their capabilities and suggest a good solution as per the requirements of the examination department of the Institute.

Read the above carefully and answer the following:

- (a) What are three major attributes of information security? Out of these attributes, which attribute will be having the highest priority while developing web based examination portal?
 - (b) In your opinion, what may be the possible dimensions under which the feasibility study of the proposed Portal was done?
 - (c) What may be the major validation methods for validating the vendors' proposal for developing the Portal?
25. XYZ Group is in the process of launching a new business unit to provide various technical consultancy services to the organizations worldwide to assist them in the computerization of their business modules. It involves a number of activities starting from capturing of requirements to maintenance. Business continuity and disaster recovery planning are two key activities, which must be taken care of right from the beginning. Business continuity focuses on maintaining the operations of an organization, especially the IT infrastructure in face of a threat that has materialized. Disaster recovery, on the other hand, arises mostly when business continuity plan fails to maintain operations and there is a service disruption. This plan focuses on restarting the operations using a prioritized resumption list. But both the plans must be assessed regarding their performance on a periodic basis.

Read the above carefully and answer the following:

- (a) What are the issues, which are emphasized by the methodology for developing a Business Continuity Plan?
- (b) Explain the objectives of performing Business Continuity Planning tests.
- (c) Out of various backup options available, explain Incremental Backup in brief?

SUGGESTED ANSWERS / HINTS

1. (a) **Governance of Enterprise IT (GEIT):** Governance of Enterprise IT is a sub-set of corporate governance and facilitates implementation of a framework of IS controls within an enterprise as relevant and encompassing all key areas. The primary objectives of GEIT are to analyze and articulate the requirements for the governance of enterprise IT, and to put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.
- Major benefits of GEIT are given 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.
- (b) Key Management Practices for implementing Risk Management are given as follows:
- ◆ **Collect Data:** Identify and collect relevant data to enable effective IT related risk identification, analysis and reporting.
 - ◆ **Analyze Risk:** Develop useful information to support risk decisions that take into account the business relevance of risk factors.
 - ◆ **Maintain a Risk Profile:** Maintain an inventory of known risks and risk attributes, including expected frequency, potential impact, and responses, and of related resources, capabilities, and current control activities.
 - ◆ **Articulate Risk:** Provide information on the current state of IT- related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.
 - ◆ **Define a Risk Management Action Portfolio:** Manage opportunities and reduce risk to an acceptable level as a portfolio.
 - ◆ **Respond to Risk:** Respond in a timely manner with effective measures to limit the magnitude of loss from IT related events.
2. Major areas which should be reviewed by Internal Auditors as a part of the review of Governance, Risk and Compliance (GRC) are given as follows:

- **Scope:** The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.
- **Governance:** The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:
 - ◆ Promoting appropriate ethics and values within the organization;
 - ◆ Ensuring effective organizational performance management and accountability;
 - ◆ Communicating risk and control information to appropriate areas of the organization; and
 - ◆ Coordinating the activities of and communicating information among the board, external and internal auditors, and management.
- **Evaluate Enterprise Ethics:** The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics related objectives, programs, and activities. The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.
- **Risk Management:** The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.
- **Interpretation:** The internal audit activity must determine whether risk management processes are effective in a judgment resulting from the internal auditor's assessment that:
 - ◆ Organizational objectives support and align with the organization's mission;
 - ◆ Significant risks are identified and assessed;
 - ◆ Appropriate risk responses are selected that align risks with the organization's risk appetite; and
 - ◆ Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.
- **Risk Management Process:** The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness. Risk management processes are monitored through on-going management activities, separate evaluations, or both.

- **Evaluate Risk Exposures:** The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:
 - ◆ Achievement of the organization's strategic objectives;
 - ◆ Reliability and integrity of financial and operational information;
 - ◆ Effectiveness and efficiency of operations and programs;
 - ◆ Safeguarding of assets; and
 - ◆ Compliance with laws, regulations, policies, procedures, and contracts.
 - **Evaluate Fraud and Fraud Risk:** The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.
 - **Address Adequacy of Risk Management Process:** During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks. Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes. When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.
3. The key management practices for assessing and evaluating the system of internal controls in an enterprise are given 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 centres, and network operations centres. 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. **Transaction Processing System (TPS):** At the lowest level of management, TPS is an information system that manipulates data from business transactions. Any business activity such as sales, purchase, production, delivery, payments or receipts involves transaction and these transactions are to be organized and manipulated to generate various information products for internal and external use. For example, selling of a product to a customer will give rise to the need of further information like customer billing, inventory status and increase in account receivable balance. TPS will thus record and manipulate transaction data into usable information.
- Major activities involved in a TPS are given as follows:
- Capturing data and organizing in files or databases;
 - Processing files/databases using application software;
 - Generating information in the form of reports; and
 - Processing queries from various quarters of the organization.
5. (a) Following are the major misconceptions about Management Information System (MIS):
- ◆ Any computer based information system is a MIS.
 - ◆ Any reporting system is MIS.
 - ◆ MIS is a management technique.
 - ◆ MIS is a bunch of technologies.

- ◆ MIS is an implementation of organizational systems and procedures. It is a file structure.
 - ◆ The study of MIS is about use of computers.
 - ◆ More data in generated reports refers more information to managers.
 - ◆ Accuracy plays vital role in reporting.
- (b) Four major constraints, which come in the way of operating a Management Information System (MIS), are given as follows:
- Non-availability of experts, who can diagnose the objectives of the organization and provide a desired direction for installing a system, which operates properly. 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 which sub-system of MIS should be installed and operated first. The criteria, which should guide the experts, depends on its need and importance.
 - Due to varied objectives of business concerns, the approach adopted by experts for designing and implementing MIS is non-standardized.
 - Non-cooperation from staff is a crucial problem, which should be handled tactfully. This can be carried out by organizing lectures, showing films and also explaining to them the utility of the system. Besides this, some staff should also be involved in the development and implementation of the system to buy-in their participation.
6. **Executive Information Systems (EIS):** It is sometimes referred to as an Executive Support System (ESS) too. It 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.

Characteristics of EIS: Major characteristics of an EIS are given 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 tools like trend analysis, market conditions etc.
- EIS can easily be given as a DSS support for decision making.

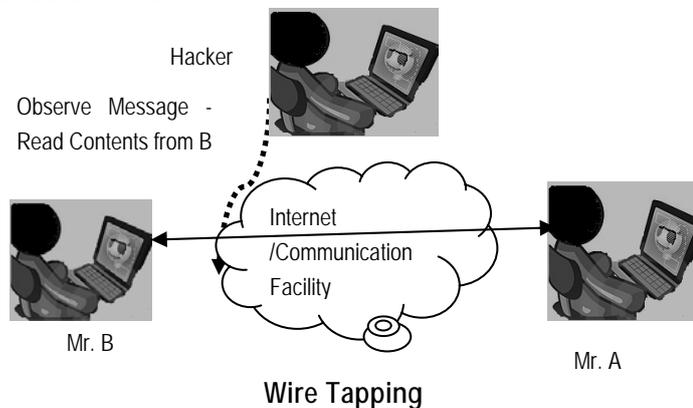
7. (a) A good security policy should clearly state the following:
- ◆ Purpose and Scope of the Document and the intended audience;
 - ◆ The Security Infrastructure;
 - ◆ Security policy document maintenance and compliance requirements;
 - ◆ Incident response mechanism and incident reporting;
 - ◆ Security organization Structure;
 - ◆ Inventory and Classification of assets;
 - ◆ Description of technologies and computing structure;
 - ◆ Physical and Environmental Security;
 - ◆ Identity Management and access control;
 - ◆ IT Operations management;
 - ◆ IT Communications;
 - ◆ System Development and Maintenance Controls;
 - ◆ Business Continuity Planning;
 - ◆ Legal Compliance; and
 - ◆ Monitoring and Auditing Requirements.
- (b) Internal Controls comprise of the following five interrelated components:
- ◆ **Control Environment:** These are the elements that establish the control context in which specific accounting systems and control procedures must operate. The control environment is manifested in management's operating style, the ways authority and responsibility are assigned, the functional method of the audit committee, the methods used to plan and monitor performance and so on.
 - ◆ **Risk Assessment:** These are the elements that identify and analyze the risks faced by an organisation and the way the risk can be managed. Both external and internal auditors are concerned with errors or irregularities that cause material losses to an organisation.
 - ◆ **Control Activities:** These are the elements that operate to ensure transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded, and independent checks on performance and valuation of records. These are called accounting controls. Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency objectives.

- ◆ **Information and Communication:** These are the elements, in which information is identified, captured and exchanged in a timely and appropriate form to allow personnel to discharge their responsibilities.
 - ◆ **Monitoring:** These are the elements that ensure internal controls operate reliably over time.
8. **Boundary Controls:** The major controls of the boundary system are the access control mechanisms that link authentic users to resource who are permitted to access. The access control mechanism has three steps - Identification, Authentication and Authorization with respect to the Access Control Policy.

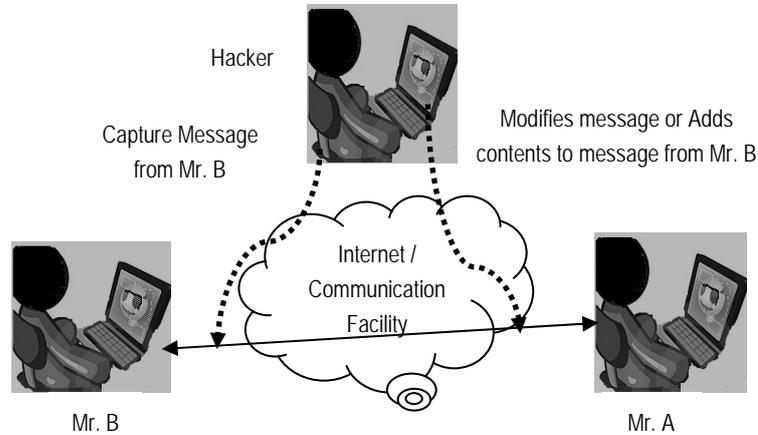
Major Boundary Control techniques are given as follows:

- **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. A cryptographic technique encrypts data (clear text) into cryptograms (cipher text) and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst. Three techniques of cryptography are transposition (permute the order of characters within a set of data), substitution (replace text with a key-text) and product cipher (combination of transposition and substitution).
 - **Passwords:** User identification by an authentication mechanism normally with strong password may be a good boundary access control. A few best practices followed to avoid failures in this control system are; minimum password length, avoid usage of common dictionary words, periodic change of passwords, hashing of passwords and number of unsuccessful entry attempts.
 - **Personal Identification Numbers (PIN):** PIN is similar to a password. It is assigned to a user by an institution using a random number stored in its database and sent independently to a user after identification. It can also be a customer selected number. Hence, a PIN may be exposed to vulnerabilities while issuance or delivery, validation, transmission and storage.
 - **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. thumb and/or finger impression, eye retina etc. are also used as boundary control techniques.
9. (a) Major Data Integrity Policies are given as under:
- ◆ **Virus-Signature Updating:** Virus signatures must be updated automatically when they are made available from the vendor through enabling of automatic updates.

- ◆ **Software Testing:** All software must be tested in a suitable test environment before installation on production systems.
 - ◆ **Division of Environments:** The division of environments into Development, Test, and Production is required for critical systems.
 - ◆ **Offsite Backup Storage:** Backups must be sent offsite for permanent storage.
 - ◆ **Quarter-End and Year-End Backups:** Quarter-end and year-end backups must be done separately from the normal schedule for accounting purposes
 - ◆ **Disaster Recovery:** A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.
- (b) **Asynchronous Attacks:** Data that is waiting to be transmitted are liable to unauthorized access called Asynchronous Attack. They occur in many environments where data can be moved asynchronously across telecommunication lines. Numerous transmissions must wait for the clearance of the line before data being transmitted. These attacks are hard to detect because they are usually very small pin like insertions. There are many forms of asynchronous attacks; some of them are given as follows:
- (i) **Data Leakage:** Data is a critical resource for an organization to function effectively. Data leakage involves leaking information out of the computer by means of dumping files to paper or stealing computer reports and tape.
 - (ii) **Wire-tapping:** This involves spying on information being transmitted over telecommunication network.

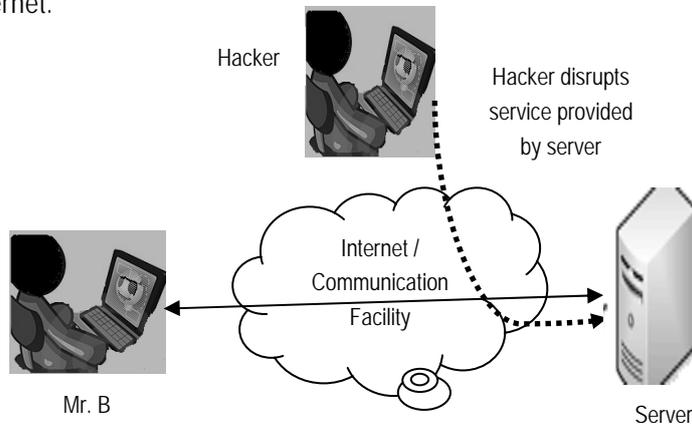


- (iii) **Piggybacking:** This is the act of following an authorized person through a secured door or electronically attaching to an authorized telecommunication link that intercepts and alters transmissions. This involves intercepting communication between the operating system and the user and modifying them or substituting new messages. A special terminal is tapped into the communication for this purpose.



Piggybacking

- (iv) **Shutting Down of the Computer/Denial of Service:** This is initiated through terminals or microcomputers that are directly or indirectly connected to the computer. Individuals, who know the high-level systems log on-ID initiate shutting down process. The security measure will function effectively if there are appropriate access controls on the logging on through a telecommunication network. When overloading happens some systems have been proved to be vulnerable to shutting themselves. Hackers use this technique to shut down computer systems over the Internet.



Denial of Service

10. (a) **Objectives of Business Continuity Planning (BCP):** The primary objective of a Business Continuity Planning is to enable an organization to survive a disaster and to re-establish normal business operations. In order 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 for the safety and well-being of people on the premises at the time of disaster;
 - ◆ Continue critical business operations;
 - ◆ Minimise the duration of a serious disruption to operations and resources (both information processing and other resources);
 - ◆ Minimise immediate damage and losses;
 - ◆ Establish management succession and emergency powers;
 - ◆ Facilitate effective co-ordination of recovery tasks;
 - ◆ Reduce the complexity of the recovery effort;
- (b) While developing a Business Continuity Plan, the key tasks that should be covered in the second phase 'Vulnerability Assessment and General definition of Requirement' are given as follows:
- ◆ A thorough Security Assessment of the computing and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security; insurance; security planning and administration; application controls; and personal computers.
 - ◆ The Security Assessment will enable the project team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.
 - ◆ Present findings and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.
 - ◆ Define the scope of the planning effort.
 - ◆ Analyze, recommend and purchase recovery planning and maintenance software required to support the development of the plans and to maintain the plans current following implementation.
 - ◆ Develop a Plan Framework.
11. (a) Major maintenance tasks undertaken in development of a BCP are to:
- ◆ 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 recovery purposes, security administrators must ensure that a contract is written to cover the following issues:
- ◆ 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;
 - ◆ Procedures to ensure security of company's data from being accessed/damaged by other users of the facility; and
 - ◆ What controls will be in place for working at the off-site facility.
12. (a) Major strengths of Prototyping Model are given as follows:
- ◆ It improves both user participation in system development and communication among project stakeholders.
 - ◆ It is especially useful for resolving unclear objectives; developing and validating user requirements; experimenting with or comparing various design solutions, or investigating both performance and the human computer interface.
 - ◆ Potential exists for exploiting knowledge gained in an early iteration as later iterations are developed.
 - ◆ It helps to easily identify, confusing or difficult functions and missing functionality.
 - ◆ It enables to generate specifications for a production application.
 - ◆ It encourages innovation and flexible designs.
 - ◆ It provides for quick implementation of an incomplete, but functional application.
 - ◆ It typically results in a better definition of users' needs and requirements than traditional systems development approach.

- ◆ A very short time period is normally required to develop and start experimenting with a prototype. This short time period allows system users to immediately evaluate proposed system changes.
 - ◆ Since system users experiment with each version of the prototype through an interactive process, errors are hopefully detected and eliminated early in the developmental process. As a result, the information system ultimately implemented should be more reliable and less costly to develop than when traditional systems development approach is employed.
- (b) From the perspective of the IS Audit, following are the possible advantages of System Development Life Cycle (SDLC):
- ◆ The IS auditor can have clear understanding of various phases of the SDLC on the basis of the detailed documentation created during each phase of the SDLC.
 - ◆ The IS Auditor on the basis of his/her examination, can state in his/her report about the compliance by the IS management with the procedures, if any, set by management.
 - ◆ If the IS Auditor has technical knowledge and ability to handle different areas of SDLC, s/he can be a guide during the various phases of SDLC.
 - ◆ The IS auditor can provide an evaluation of the methods and techniques used through the various development phases of the SDLC.
13. Two primary methods which are used for the analysis of the scope of a project in SDLC are given as follows:
- **Reviewing Internal Documents:** The analysts conducting the investigation first try to learn about the organization involved in, or affected by, the project. For example, to review an inventory system proposal, an analyst may try to know how the inventory department operates and who are the managers and supervisors. Analysts can usually learn these details by examining organization charts and studying written operating procedures.
 - **Conducting Interviews:** Written documents tell the analyst how the systems should operate, but they may not include enough details to allow a decision to be made about the merits of a systems proposal, nor do they present users' views about current operations. To learn these details, analysts use interviews. Interviews allow analysts to know more about the nature of the project request and the reasons for submitting it. Usually, preliminary investigation interviews involve only management and supervisory personnel.
14. Following are the major reasons due to which organizations fail to achieve their System Development objectives:

- (i) **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 after 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 User Participation:** Often users do not participate in the development stage because they are preoccupied with their existing work, or do not understand the benefits of the new system. User apathy 'I have nothing to gain if I participate' is also a reason.
 - ◆ **Inadequate Testing and User Training:** Often systems are not tested due to lack of time and rush to introduce the new system or because problems were not envisaged at the development stage. Inadequate user training may be a result of poor project planning, or lack of training techniques, or because user management does not release personnel for training due to operational pressure.
- (ii) **Developer Related Issues:** It refers to the issues and challenges with regard to developers. Some of the critical bottlenecks are mentioned below:
- ◆ **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 lack sufficient educational background and requisite state of the art skills. Furthermore, many companies do little to help their development personnel stay technically sound, and often a training plan and training budget do not exist.
- (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. Some of such bottlenecks are mentioned as follows:

- ◆ **Lack of Senior Management Support and Involvement:** Developers and users of information systems watch senior management to determine 'which systems development projects are important' and act accordingly by shifting their efforts away from any project, which is not receiving management attention. In addition, management may not allocate adequate resources, as well as budgetary control over use of resources, assigned to the project.
 - ◆ **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 technology.

In order to overcome these aforementioned issues, organizations must execute a well-planned systems development process efficiently and effectively. Accordingly, a sound system development team is inevitable for project success.

15. The performance of evidence collection and understanding the reliability of controls involve the following major issues:
- **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 summarizing 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 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 of time. 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 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 the 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-only" 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 (journalized) 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 organizations 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 who are the parties to the contract.
16. **System Control Audit Review File (SCARF):** The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written on a special audit file - the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities. Auditors might use SCARF technique to collect the following types of information:
- **Application System Errors** - SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.
 - **Policy and Procedural Variances** - Organizations have to adhere to the policies, procedures and standards of the organization and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.
 - **System Exception** - SCARF can be used to monitor different types of application system exceptions. For example, salespersons might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.
 - **Statistical Sample** - Some embedded audit routines might be statistical sampling routines, SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.
 - **Snapshots and Extended Records** - Snapshots and extended records can be written into the SCARF file and printed when required.
 - **Profiling Data** - Auditors can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.

- **Performance Measurement** - Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.

17. (a) Major objectives of the Information Technology Act, 2000 are as follows:

- ◆ To grant legal recognition for transactions carried out by means of Electronic Data Interchange (EDI) and other means of electronic communication commonly referred to as "electronic commerce" in place of paper based methods of communication;
- ◆ To give legal recognition to Digital Signatures for authentication of any information or matter, which requires authentication under any law;
- ◆ To facilitate electronic filing of documents with Government departments;
- ◆ To facilitate electronic storage of data;
- ◆ To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions;
- ◆ To give legal recognition for keeping of books of accounts by banker's in electronic form; and
- ◆ To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934.

(b) Section 6 provides for use of electronic records in government and its agencies even though the original law requiring these documents did not provide for electronic forms. It allows use of electronic form for:

- ◆ filing any form, application or other documents;
- ◆ creation, retention or preservation of records, issue or grant of any license or permit;
- ◆ receipt or payment in Government offices.

The appropriate Government has the power to prescribe the manner and format of the electronic records.

18. (a) Mr. B can file an FIR in police against Mr. A under the following Sections of Information Technology Act, 2000:

- ◆ **Section 66A:** Punishment for sending offensive messages through communication service, etc.;
- ◆ **Section 66B:** Punishment for dishonestly receiving stolen computer resource or communication device; and
- ◆ **Section 66E:** Punishment for violation of privacy.

All these applicable sections in this case are given as follows:

[Section 66A] Punishment for sending offensive messages through communication service, etc.

Any person who sends, by means of a computer resource or a communication device,-

- (a) any information that is grossly offensive or has menacing character; or
- (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently by making use of such computer resource or a communication device,
- (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

[Section 66B] Punishment for dishonestly receiving stolen computer resource or communication device.

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

[Section 66E] Punishment for violation of privacy

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

- (b) Not below the rank of an Inspector or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf can search and arrest Mr. A, suspected of having committed an offence under the IT Act, 2000.

Related provisions have been covered in Section 80 of IT Act, 2000. The details are given as follows:

[Section 80] Power of Police Officer and Other Officers to Enter, Search, etc.

- (1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Inspector or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest

without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.

Explanation: For the purposes of this sub-section, the expression "Public Place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

- (2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.
- (3) The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

19. (a) Major goals of Cloud Computing are given as follows:

- ◆ To create a highly efficient IT ecosystem, where resources are pooled together and costs are aligned with what resources are actually used;
- ◆ To access services and data from anywhere at any time;
- ◆ To scale the IT ecosystem quickly, easily and cost-effectively based on the evolving business needs;
- ◆ To consolidate IT infrastructure into a more integrated and manageable environment;
- ◆ To reduce costs related to IT energy/power consumption;
- ◆ To enable or improve "Anywhere Access" (AA) for ever increasing users; and
- ◆ To enable rapid provision of resources as needed.

(b) **Public Cloud:** This environment can be used by the general public. This includes individuals, corporations and other types of organizations. Typically, public clouds are administrated by third parties or vendors over the Internet, and the services are offered on pay-per-use basis. These are also called Provider Clouds. Business models like SaaS (Software-as-a-Service) and public clouds complement each other and enable companies to leverage shared IT resources and services.

The advantages of public cloud include the following:

- ◆ It is widely used in the development, deployment and management of enterprise applications, at affordable costs.
- ◆ It allows the organizations to deliver highly scalable and reliable applications rapidly and at more affordable costs.

Moreover, one of the limitations is security assurance and thereby building trust among the clients is far from desired but slowly liable to happen.

20. (a) Major steps, which can be followed for Green IT, are given as follows.
- ◆ Power-down the CPU and all peripherals during extended periods of inactivity.
 - ◆ Try to do computer-related tasks during contiguous, intensive blocks of time, switching off hardware at other times.
 - ◆ Power-up and power-down energy-intensive peripherals such as laser printers according to need.
 - ◆ Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors.
 - ◆ 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.
 - ◆ Minimize the use of paper and properly recycle waste paper.
 - ◆ Dispose of e-waste according to central, state and local regulations.
 - ◆ Employ alternative energy sources for computing workstations, servers, networks and data centers.
- (b) Four challenges to Cloud Computing are given as follows:
- ◆ **Confidentiality:** Prevention of unauthorized disclosure of data is referred to as Confidentiality. Normally, Cloud works on public networks; therefore, there is a requirement to keep the data confidential the unauthorized entities. With the use of encryption and physical isolation, data can be kept secret. The basic approaches to attain confidentiality are the encrypting the data before placing it in a Cloud with the use of TC3 (Total Claim Capture & Control).
 - ◆ **Integrity:** Integrity refers to the prevention of unauthorized modification of data and it ensures that data is of high quality, correct, consistent and accessible. After moving the data to the cloud, owner hopes that their data and applications are secure. It should be ensured that the data is not changed after being moved to the cloud. It is important to verify if one's data has been tampered with or deleted. Strong data integrity is the basis of all the service models such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Methods like Digital Signature, Redundant Array of Independent Disks (RAID) strategies etc. are some ways to preserve integrity in Cloud computing. The most direct way to enforce the integrity control is to employ cryptographic hash function. For example, a solution is developed as underlying data structure using hash tree for authenticated network storage.
 - ◆ **Availability:** Availability refers to the prevention of unauthorized withholding of data and it ensures the data backup through Business Continuity Planning

(BCP) and Disaster Recovery Planning (DRP). In addition, Availability also ensures that they meet the organization's continuity and contingency planning requirements. Availability can be affected temporarily or permanently, and a loss can be partial or complete. Temporary breakdowns, sustained and Permanent Outages, Denial of Service (DoS) attacks, equipment failure, and natural calamities are all threats to availability. One of the major Cloud service provider, AWS had a breakdown for several hours, which led to data loss and access issues with multiple Web 2.0 services.

- ◆ **Architecture:** In the architecture of Cloud computing models, there should be control over the security and privacy of the system. The architecture of the Cloud is based on a specific service model. Its reliable and scalable infrastructure is dependent on the design and implementation to support the overall framework.

21. (a) **Trojan Horse:** These are malicious programs that are hidden under any authorized program. Typically, a Trojan horse is an illicit coding contained in a legitimate program, and causes an illegitimate action. The concept of Trojan is similar to bombs but a computer clock or particular circumstances do not necessarily activate it. A Trojan may:

- ◆ Change or steal the password or
- ◆ May modify records in protected files or
- ◆ May allow illicit users to use the systems.

Trojan Horse hides in a host and generally do not damage the host program. Trojans cannot copy themselves to other software in the same or other systems. The trojans may get activated only if the illicit program is called explicitly. It can be transferred to other system only if an unsuspecting user copies the Trojan program.

Christmas Card is a well-known example of Trojan. It was detected on internal E-mail of IBM system. On typing the word 'Christmas', it will draw the Christmas tree as expected, but in addition, it will send copies of similar output to all other users connected to the network. Because of this message on other terminals, other users cannot save their half finished work.

(b) **Snapshots:** Tracing a transaction in a computerized system can be performed with the help of snapshots or extended records. The snapshot software is built into the system at those points where material processing occurs which takes images of the flow of any transaction as it moves through the application. These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction. The main areas to dwell upon while involving such a system are to locate the snapshot points based on materiality of transactions when the snapshot will be captured and the reporting system design and implementation to present data in a meaningful way.

- (c) **Test Plan under BCP & DRP:** The final component of a Disaster Recovery Plan (DRP) is a test plan. The purpose of the test plan is to identify deficiencies in the emergency, backup, or recovery plans or in the preparedness of an organization and its personnel for facing a disaster. It must enable a range of disasters to be simulated and specify the criteria by which the emergency, backup, and recovery plans can be deemed satisfactory. Periodically, test plans must be invoked. Unfortunately, top managers are often unwilling to carry out a test because daily operations are disrupted. They also fear a real disaster could arise as a result of the test procedures.
- (d) **Audit Hooks:** There are audit routines that flag suspicious transactions. For example, internal auditors at Insurance Company determined that their policyholder system was vulnerable to fraud every time a policyholder changed his or her name or address and then subsequently withdrew funds from the policy. They devised a system of audit hooks to tag records with a name or address change. The internal audit department will investigate these tagged records for detecting fraud. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach of real-time notification may display a message on the auditor's terminal.
22. (a) **Black Box Testing:** Black Box Testing takes an external perspective of the test object, to derive test cases. These tests can be functional or non-functional, though usually functional. The test engineer has no prior knowledge of the test object's internal structure. The test designer selects typical inputs including simple, extreme, valid and invalid input-cases and executes to obtain assurance or uncover errors.

This method of test design is applicable to all levels of software testing i.e. unit, integration, functional testing, system and acceptance. The higher the level, the box is bigger and more complex, and the more one is forced to use black box testing to simplify. While this method can uncover unimplemented parts of the specification, one cannot be sure that all existent paths are tested. If a module performs a function, which it is not supposed to, the black box test may not identify it.

White Box Testing: It uses an internal perspective of the system to design test cases based on internal structure. It requires programming skills to identify all paths through the software. The tester chooses test case inputs to exercise paths through the code and determines the appropriate outputs. Since the tests are based on the actual implementation, if the implementation changes, the tests probably will need to change, too. It is applicable at the unit, integration and system levels of the testing process, it is typically applied to the unit. While it normally tests paths within a unit, it can also test paths between units during integration, and between subsystems during a system level test. After obtaining a clear picture of the internal workings of a product, tests can be conducted to ensure that the internal operation of the product conforms to specifications and all the internal components are adequately exercised.

- (b) **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.

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.

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. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data.

- (c) **Structured English:** Structured English, also known as Program Design Language (PDL), is the use of the English language with the syntax of structured programming. Thus, Structured English aims at getting the benefits of both the programming logic and natural language. Program logic that helps to attain precision and natural language that helps in getting the convenience of spoken languages. A better structured, universal and precise tool is referred to as pseudo code.

Flowchart: Flowcharting is a pictorial representation technique that can be used by analysts to represent the inputs, outputs and processes of a business process. It is a common type of chart that represents an algorithm or process showing the steps as boxes of various kinds, and their order by connecting these with arrows. Flowcharts are used in analyzing, designing, documenting or managing a process or program in various fields.

23. (a) System Requirements Analysis is a phase, which includes a thorough and detailed understanding of the current system, identification of the areas that need modification/s to solve the problem, the determination of user/managerial requirements and to have fair ideas about various system development tools.

The following activities are performed in this phase:

- ◆ To identify and consult the stake owners to determine their expectations and resolve their conflicts;
- ◆ To analyze requirements to detect and correct conflicts and determine priorities;
- ◆ To verify requirements in terms of various parameters like completeness, consistency, unambiguous, verifiable, modifiable, testable and traceable;

- ◆ To gather data or find facts using tools like- interviewing, research/document collection, questionnaires, observation;
- ◆ To develop models to document Data Flow Diagrams, E-R diagrams; and
- ◆ To document activities such as interviews, questionnaires, reports etc. and development of a system dictionary to document the modelling activities.

The document/deliverable of this phase is a detailed system requirements report, which is generally termed as SRS.

(b) Following are the key risk management strategies:

- ◆ **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.

In the given scenario, we would recommend to follow the strategy of 'Terminate/Eliminate the risk'. Because the company is currently using various stand-alone systems, which are found to be on higher risk due to technology as well as supplier/s. By using this strategy, the risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.

(c) Major strengths of Agile Methodology are given as follows:

- ◆ Agile methodology has the concept of an adaptive team, which enables to respond to the changing requirements.

- ◆ The team does not have to invest time and efforts and finally find that by the time they delivered the product, the requirement of the customer has changed.
- ◆ Face to face communication and continuous inputs from customer representative leaves a little space for guesswork.
- ◆ The documentation is crisp and to the point to save time.
- ◆ The end result is generally the high quality software in least possible time duration and satisfied customer.

24. (a) Three major attributes of information security are given (CIA) that are as follows:

- ◆ **Confidentiality:** Prevention of the unauthorized disclosure of information;
- ◆ **Integrity:** Prevention of the unauthorized modification of information; and
- ◆ **Availability:** Prevention of the unauthorized withholding of information.

In the given scenario, Integrity will be having the highest priority while developing web based examination portal because in any examination system, the prime goal should be to make available the correct information only. It should not be altered or modified by any unauthorized person/s.

(b) The possible dimensions under which the feasibility study of the proposed Portal was done are given as follows:

- ◆ **Technical:** Is the technology needed available?
- ◆ **Financial:** Is the solution viable financially?
- ◆ **Economic:** Return on Investment?
- ◆ **Schedule/Time:** Can the system be delivered on time?
- ◆ **Resources:** Are human resources reluctant for the solution?
- ◆ **Operational:** How will the solution work?
- ◆ **Behavioural:** Is the solution going to bring any adverse effect on quality of work life?
- ◆ **Legal:** Is the solution valid in legal terms?

(c) Major validation methods of validating the vendors' proposal for developing the Knowledge Portal are as follows:

- (i) **Checklists:** It is the most simple and rather subjective method for validation and evaluation. The various criteria are put into check lists 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, Software.
- (ii) **Point-Scoring Analysis:** Point-scoring analysis provides an objective means of selecting the final system. There are no absolute rules in the selection

process, only guidelines for matching user needs with software capabilities. Evaluators must consider such issues as the University's needs to operate and maintain the portal, vendor reputations, software costs, user-friendliness for students (who are the customers in this case), and so forth.

- (iii) **Public Evaluation Reports:** Several consultancy 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. For those criteria where published reports are not available, however, resort would have to be made to other methods of validation. This method is particularly useful where the buying staff has inadequate knowledge of facts. E.g. Public reports by agencies like Gartner's magic quadrant on systems used by other universities offering online courses may be considered.
 - (iv) **Benchmarking Problem for Vendor's Proposals:** Benchmarking problems for vendors' proposals are sample programs that represent at least a part of the buyer's primary computer work load and include software considerations and can be current applications programs or new programs that have been designed to represent planned processing needs. E.g. develop a set of sample requirements of a student and see whether the proposed system is able to effectively and efficiently deliver them. That is, benchmarking problems are oriented towards testing whether a computer system offered by the vendor meets the requirements of the buyer.
 - (v) **Test 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 download e-lectures (which are large sized files) by students, response time when large number of students login in at the same time, overhead requirements of the operating system in executing multiple user requests, length of time required to execute an instruction, etc. The results, achieved by the machine can be compared and price performance judgment can be made. It must be borne in mind, however that various capabilities to be tested would have to be assigned relative weightage as all requirements may not be equally important.
25. (a) The methodology for developing a Business Continuity Plan emphasizes the following:
- (i) Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
 - (ii) Obtaining commitment from appropriate management to support and participate in the effort;
 - (iii) Defining recovery requirements from the perspective of business functions;

- (iv) Documenting the impact of an extended loss to operations and key business functions;
 - (v) Focusing appropriately on disaster prevention and impact minimization, as well as orderly recovery;
 - (vi) Selecting business continuity teams that ensure the proper balance required for plan development;
 - (vii) Developing a business continuity plan that is understandable, easy to use and maintain;
 - (viii) Planning the testing of plans in a systematic manner and measuring results of such tests; and
 - (ix) 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.
- (b) The objectives of performing BCP tests are to ensure that:
- ◆ the recovery procedures are complete and workable;
 - ◆ the competence of personnel in their performance of recovery procedures can be evaluated;
 - ◆ the resources such as business processes, IS systems, personnel, facilities and data are obtainable and operational to perform recovery processes;
 - ◆ manual recovery procedures and IT backup system/s are current and can either be operational or restored; and
 - ◆ the success or failure of business continuity training program is monitored.
- (c) **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 are very difficult to restore. One will have to start with recovering the last full backup, and then recovering from every incremental backup taken since.