PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

Note: Update on Section 66A of the IT Act, 2000

As per the decision of the Supreme Court dated 24th March, 2015; Section 66A of Information Technology Act, 2000 (Punishment for sending offensive messages through communication service, etc.) has been declared *Unconstitutional* as it is violative of Article 19(1)(a) related to freedom of speech and expressions. Now comments on social networking sites will not be offensive unless they come under the provisions of the Indian Penal Code, 1860.

Concepts of Governance and Management of Information Systems

1. Discuss different levels of managerial activity that are carried out in an enterprise.
2. Discuss key benefits of COBIT 5 framework.
3. As an internal auditor, what shall be your perspective while evaluating IT Governance of an enterprise?

Information System Concepts

4. Discuss major areas of Computer-based applications.
5. Discuss different components of ERP (Enterprise Resource Planning) and its benefits.
6. Discuss different attributes of Information.

Protection of Information Systems

7. Differentiate between Detective Controls and Corrective Controls.
8. Discuss the impact of Technology on Internal Controls.
9. Discuss major techniques to commit cyber frauds.

Business Continuity Planning and Disaster Recovery Planning

10. Discuss the different phases involved in the development of a Business Continuity Plan.
11. Why documentation is required in Business Continuity Management (BCM)? Which documents are classified as being part of the BCM system?
12. Discuss Business Impact Analysis (BIA).

Acquisition, Development and Implementation of Information Systems

13. What do you understand by "Incremental Model"? Discuss its strengths and weaknesses also.
14. Discuss majorly used System Development Tools.

15. How can 'System Maintenance' under System Development Life Cycle (SDLC) be categorized?

Auditing of Information Systems

16. Why is there a need for audit of Information Systems?
17. Discuss the System Control Audit Review File (SCARF) technique used in the audit of Information Systems.

Information Technology Regulatory Issues

18. Discuss the provision given in IT (Amendment) Act 2008 that gives "Power to make rules by Central Government in respect of Electronic Signature".
19. Discuss the guidelines recommended by Securities and Exchange Board of India (SEBI) to conduct audit of systems.

Emerging Technologies

20. What are the emerging threats under "Bring Your Own Device (BYOD)"?

Short Note Based Questions

21. Write short notes on following:
    (a) Benefits of Governance of Enterprise IT (GEIT)
    (b) Planning Languages in Decision Support Systems (DSS)
    (c) Objectives and Goals of Business Continuity Planning (BCP)
    (d) Strengths of Agile Model
    (e) Auditor's role in System Development Life Cycle (SDLC)
22. Differentiate between the following:
    (a) Full Backup and Incremental Backup
    (b) Open System and Closed System
    (c) Explicit Knowledge and Tacit Knowledge
    (d) Quality Assurance Management Control and Security Management Control
    (e) Program Debugging and Program Testing

Questions based on the Case Studies

23. PQR Company is a pharmaceutical retail chain having many branches located in different places for its operation. Its business processes are cumbersome and tedious as it has multiple sources of procurement and supply destinations. The Chief Executive Officer (CEO) of company feels that existing information system does not meet its present requirements. He seeks for high-end solution to streamline and integrate its operation

processes and information flow to synergize all its major resources. Further, he expects that the new system should provide a structured environment in which decisions concerning demand, supply, operational, personnel, finance, logistics etc. are fully supported by accurate and reliable information. The company follows the best practices of System Development Life Cycle (SDLC), which consists of various phases starting from preliminary investigation till post implementation review, controls and security aspects. The CEO of the company appoints a committee of three persons - IT expert, a Security expert and an Auditor of the company in order to suggest the following:

(a) List the activities to be performed during the phase of System Requirements Analysis.

(b) Discuss major Boundary Control techniques that should be used in user control?

24. ABC is a leading company in the manufacturing of food items. The company is in the process of automation of its various business processes. During this phase, technical consultant of the company has highlighted the importance of information security and has suggested introducing it right from the beginning. He has also suggested to perform the risk assessment activity and accordingly, to mitigate the assessed risk. For carrying out all these suggestions, various best practices have been followed by the company. In addition, after each activity, appropriate standards' compliances have been tested to check the quality of each process. Various policies related with business continuity planning and disaster recovery planning has been implemented to ensure three major expectations from the software, namely, resist, tolerate and recover.

Read the above carefully and answer the following:

(a) What are the major suggestions given by the technical consultant? How the company is implementing these suggestions?

(b) Discuss Recovery Plan under Business Continuity Planning.

(c) What should be the major components of a good information security policy, as per your opinion?

25. ABC Industries Ltd., a company engaged in a business of manufacture and supply of automobile components to various automobile companies in India, had been developing and adopting office automation systems, at random and in isolated pockets of its departments. The company has recently obtained three major supply contracts from International Automobile companies and the top management has felt that the time is appropriate for them to convert its existing information system into a new one and to integrate all its office activities. One of the main objectives of taking this exercise is to maintain continuity of business plans even while continuing the progress towards e-governance.

(a) When the existing information system is to be converted into a new system, what are the activities involved in the conversion process?

(b) What are the different office activities that can be performed under Office Automation Systems (OAS)?

(c) What is meant by Business Continuity Planning? Explain the areas covered by Business Continuity.

SUGGESTED ANSWERS/HINTS

1. There are three levels of managerial activity in an enterprise which are as follows:

   - Strategic Planning: Strategic Planning is defined as the process of deciding on objectives of the enterprise, on changes in these objectives, on the resources used to attain these objectives, and on the policies that are to govern the acquisition, use, and disposition of these resources. Strategic planning is the process by which top management determines overall organizational purposes and objectives and how they are to be achieved. Corporate-level strategic planning is the process of determining the overall character and purpose of the organization, the business it will enter and leave, and how resources will be distributed among those businesses.
   - Management Control: Management Control is defined as the process by which managers assure that resources are obtained and used effectively and efficiently in the accomplishment of the enterprise's objectives.
   - Operational Control: Operational Control is defined as the process of assuring that specific tasks are carried out effectively and efficiently.

   IT strategic plans provide direction to deployment of information systems and it is important that key functionaries in the enterprise are aware and are involved in its development and implementation. Management should ensure that IT long and short-range plans are communicated to business process owners and other relevant parties across the enterprise. Management should establish processes to capture and report feedback from business process owners and users regarding the quality and usefulness of long and short-range plans. The feedback obtained should be evaluated and considered in future IT planning.

2. The key benefits of COBIT 5 framework are as follows:

   - A comprehensive framework such as COBIT 5 enables enterprises in achieving their objectives for the governance and management of enterprise IT.
   - The best practices of COBIT 5 help enterprises to create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use.
   - Further, COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT related interests of internal and external stakeholders.

- COBIT 5 helps enterprises to manage IT related risk and ensures compliance, continuity, security and privacy.
- COBIT 5 enables clear policy development and good practice for IT management including increased business user satisfaction.
- The key advantage in using a generic framework such as COBIT 5 is that it is useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.
- COBIT 5 supports compliance with relevant laws, regulations, contractual agreements and policies.

3. IT Governance can be evaluated by both external as well internal auditors. The Institute of Internal Auditors (IIA) issues the guidance that outlines specific areas and critical aspects relating to governance structure and practices, which can be reviewed as part of internal audit. These are briefly explained here.

- Leadership: The following aspects need to be verified by the auditor:
  - Evaluate the relationship between IT objectives and the current/strategic needs of the organization and the ability of IT leadership to effectively communicate this relationship to IT and organizational personnel.
  - Assess the involvement of IT leadership in the development and on-going execution of the organization's strategic goals.
  - Determine how IT will be measured in helping the organization achieve these goals.
  - Review how roles and responsibilities are assigned within the IT organization and how they are executed.
  - Review the role of senior management and the board in helping establish and maintain strong IT governance.
- Organizational Structure: The following aspects need to be assessed by the auditor:
  - Review how organization management and IT personnel are interacting and communicating current and future needs across the organization.
  - This should include the existence of necessary roles and reporting relationships to allow IT to meet the needs of the organization, while providing the opportunity to have requirements addressed via formal evaluation and prioritization. In addition, how IT mirrors the organization structure in its enterprise architecture should also be included.
- Processes: The following aspects need to be checked by the auditor:
  - Evaluate IT process activities and the controls in place to mitigate risks to the organization and whether they provide the necessary assurance regarding

processes and underlying systems.

- What processes are used by the IT organization to support the IT environment and consistent delivery of expected services?

- Risks: The following aspects need to be reviewed by the auditor:
  - Review the processes used by the IT organization to identify, assess, and monitor/mitigate risks within the IT environment.
  - Additionally, determine the accountability that personnel have within risk management and how well these expectations are being met.
- Controls: The following aspects need to be verified by the auditor:
  - Assess key controls that are defined by IT to manage its activities and the support of the overall organization.
  - Ownership, documentation, and reporting of self-validation aspects should be reviewed by the internal audit activity.
  - Additionally, the control set should be robust enough to address identified risks based on the organization's risk appetite and tolerance levels, as well as any compliance requirements.
- Performance Measurement/Monitoring: The following aspects need to be verified by the auditor:
  - Evaluate the framework and systems in place to measure and monitor organizational outcomes where support from IT plays an important part in the internal outputs in IT operations and developments.

4. Major areas of Computer based applications are Finance and Accounting, Marketing and Sales, Manufacturing, Inventory/Stock Management, Human Resource Management etc., which are given as follows:
   - Finance and Accounting – The main goal of this subsystem is to ensure the financial viability of the organization, enforce financial discipline and plan and monitor the financial budget. It also helps in forecasting revenues, determining the best resources and uses of funds and managing other financial resources. Typical sub-application areas in finance and accounting are - Financial accounting; General ledger; Accounts receivable/payable; Asset accounting; Investment management; Cash management; Treasury management; Fund management and Balance sheet.
   - Marketing and Sales – The objective of this subsystem is to maximize the sales and ensure customer satisfaction. The marketing system facilitates the chances of order procurement by marketing the products of the company, creating new customers and advertising the products. The sales department may use an order processing system to keep the status and track of orders, generate bills for the orders executed and delivered to the customer, strategies for rendering services

during warranty period and beyond, analyzing the sales data by category such as by region, product, sales manor sales value.

- Production or Manufacturing – The objective of this subsystem is to optimally deploy man, machine and material to maximize production or service. The system generates production schedules and schedules of material requirements, monitors the product quality, plans for replacement or overhauling the machinery and also helps in overhead cost control and waste control.
- Inventory /Stores Management - The inventory management system is designed with a view to keeping the track of materials in the stores. The system is used to regulate the maximum and minimum level of stocks, raise alarm at danger level stock of any material, give timely alert for re-ordering of materials with optimal re-order quantity and facilitate various queries about inventory like total inventory value at any time, identification of important items in terms stock value (ABC analysis), identification most frequently moving items (XYZ analysis) etc.
- Human Resource Management - Human resource is the most valuable asset for an organization. Effective and efficient utilization of manpower in a dispute-free environment in this key functional area ensures to facilitate disruption free and timely services in business. Human Resource Management System (HRMS) aims to achieve this goal. Skill database maintained in HRM system, with details of qualifications, training, experience, interests etc. helps management for allocating manpower to right activity at the time of need or starting a new project. This system also keeps track of employees' output or efficiency. Administrative functions like keeping track of leave records or handling other related functions are also included HRM system. An HRM system may have the following modules – Personnel administration; Recruitment management; Travel management; Benefit administration; Salary administration; Promotion management etc.

5. Enterprise Resource Planning (ERP) is process management software that allows an organization to use a system of integrated applications to manage the business and automate many back-office functions related to technology, services and human resources. ERP software integrates all facets of an operation, including product planning, development, manufacturing, sales and marketing. ERP model consists of four components which are implemented through a methodology and are as follows:

   (i) Software Component: The software component is the component that is most visible part and consists of several modules such as Finance, Human Resource, Supply Chain Management, Supplier Relationship Management, Customer Relationship, and Business Intelligence.

   (ii) Process Flow: It is the model that illustrates the way how information flows among the different modules within an ERP system. By creating this model makes it easier to understand how ERP work.

(iii) Customer mindset: By implementing ERP system, the old ways for working which user understand and comfortable with; have to be changed and may lead to users' resistance. For example, some users may say that they have spent many years doing an excellent job without help from ERP system. In order to lead ERP implementation to succeed, the company needs to eliminate negative value or belief that users may carry toward utilizing new system.

(iv) Change Management: In ERP implementation, change needs to be managed at several levels - User attitude; resistance to change; and Business process changes.

Benefits of ERP are as follows:

- Streamlining processes and workflows with a single integrated system.
- Reduce redundant data entry and processes and in other hand it shares information across the department.
- Establish uniform processes that are based on recognized best business practices.
- Improved workflow and efficiency.
- Improved customer satisfaction based on improved on-time delivery, increased quality, shortened delivery times.
- Reduced inventory costs resulting from better planning, tracking and forecasting of requirements.
- Turn collections faster based on better visibility into accounts and fewer billing and/or delivery errors.
- Decrease in vendor pricing by taking better advantage of quantity breaks and tracking vendor performance.
- Track actual costs of activities and perform activity based costing.
- Provide a consolidated picture of sales, inventory and receivables.

6. Attributes of Information: Some of the important attributes of useful and effective information are as follows:

- Availability - Information is useless if it is not available at the time of need. Database is a collection of files which is collection of records and data from where the required information is derived for useful purpose.
- Purpose/Objective - Information must have purposes/objective at the time it is transmitted to a person or machine, otherwise it is simple data. The basic objective of information is to inform, evaluate, persuade, and organize that further helps in decision making, generating new concepts and ideas, identify and solve problems, planning, and controlling which are needed to direct human activity in business enterprises.

- Mode and format - The mode of communicating information to humans should be in such a way that it can be easily understand by the people. The mode may be in the form of voice, text and combination of these two. Format also plays an important role in communicating the idea. It should be designed in such a way that it assists in decision making, solving problems, initiating planning, controlling and searching. According to the type of information the different formats can be used e.g. diagrams, graphs, curves are best suited for representing the statistical data. Format of information should be simple, relevant and should highlight important points but should not be too cluttered up.
- Current/Updated - The information should be refreshed from time to time as it usually rots with time and usage. For example, the running score sheet of a cricket match available in Internet sites should be refreshed at fixed interval of time so that the current score will be available. Similar is the case with broker who wants the latest information about the stock market.
- Rate - The rate of transmission/reception of information may be represented by the time required to understand a particular situation. Useful information is the one which is transmitted at a rate which matches with the rate at which the recipient wants to receive. For example- the information available from internet site should be available at a click of mouse, one should wait for it an hour.
- Frequency - The frequency with which information is transmitted or received affects its value. For example- the weekly reports of sales shows little change as compared to the quarterly and contribute less for accessing salesman capability.
- Completeness and Adequacy - The information provided should be complete and adequate in itself because only complete information can be used in policy making. For example-the position of student in a class can be find out only after having the information of the marks of all students and the total number of students in a class.
- Reliability - It is a measure of failure or success of using information for decision-making. If information leads to correct decision on many occasions, we say the information is reliable.
- Validity - It measures how close the information is to the purpose for which it asserts to serve. For example, the experience of employee supports in evaluating his performance.
- Quality - It means the correctness of information. For example, an over-optimistic manager may give too high estimates of the profit of product which may create problem in inventory and marketing.
- Transparency - It is essential in decision and policy making. For example, total amount of advance does not give true picture of utilization of fund for decision about future course of action; rather deposit-advance ratio is perhaps more transparent information in this matter.

- Value of Information - It is defined as difference between the value of the change in decision behavior caused by the information and the cost of the information. In other words, given a set of possible decisions, a decision-maker may select one on basis of the information at hand. If new information causes a different decision to be made, the value of the new information is the difference in value between the outcome of the old decision and that of the new decision, less the cost of obtaining the information.

7. Detective Controls: These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. An example of a detective control would be a use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend. The main characteristics of such controls are given as follows:

   - Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc;
   - An established mechanism to refer the reported unlawful activities to the appropriate person or group;
   - Interaction with the preventive control to prevent such acts from occurring; and
   - Surprise checks by supervisor.

   Examples of detective controls include Hash totals; Check points in production jobs; Echo control in telecommunications; Error message over tape labels; Duplicate checking of calculations; Periodic performance reporting with variances; Past-due accounts report; The internal audit functions; Intrusion detection system; Cash counts and bank reconciliation; and Monitoring expenditures against budgeted amount.

   Corrective Controls: Corrective controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. A Business Continuity Plan (BCP) is considered to be a corrective control. The main characteristics of the corrective controls are 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. Examples of Corrective Controls are Contingency planning; Backup procedure; Rerun procedures; Change input value to an application system, and Investigate budget variance and report violations.

8. The impact of Technology on Internal Controls is as follows:

   - Competent and Trustworthy Personnel: Personnel should have proper skill and knowledge to discharge their duties. Substantial power is often vested in the errors responsible for the computer-based information systems developed, implemented, operated, and maintained within organizations.

- Segregation of Duties: In a manual system, during the processing of a transaction, there are split between different people, such that one person does not process a transaction right from start to finish. However, in a computerised system, the auditor should also be concerned with the segregation of duties within the IT department. As a basic control, segregation of duties prevents or detects errors or irregularities. Within an IT environment, the staff in the IT department of an enterprise will have a detailed knowledge of the interrelationship between the source of data, how it is processed and distribution and use of output.
- Authorization Procedures: In manual systems, auditors evaluate the adequacy of procedures for authorization of examining the work of employees. In computer systems, authorization procedures often are embedded within a computer program. For example: In some on-line transaction systems, written evidence of individual data entry authorisation, e.g. a supervisor's signature, may be replaced by computerised authorisation controls such as automated controls written into the computer programs (e.g. programmed credit limit approvals).
- Adequate Documents and Records: In a manual system, adequate documents and records are needed to provide an audit trail of activities within the system. In computer systems, documents might not be used to support the initiation, execution, and recording of some transactions. Thus, no visible audit or management trail would be available to trance the transactions in a computerized system.
- Physical Control over Assets and Records: Physical control over access and records is critical in both manual systems and computer systems. In the manual systems, protection from unauthorised access was through the use of locked doors and filing cabinets. Computerised financial systems have not changed the need to protect the data. A client's financial data and computer programs can all be maintained at a single site – namely the site where the computer is located. This concentration of information systems assets and records also increases the losses that can arise from computer abuse or a disaster.
- Adequate Management Supervision: In a manual system, management supervision of employee activities is relatively straightforward as the managers and the employees are often at the same physical location. In computer system, however, data communication facilities can be used to enable employees to be closer to the customers they service. Thus supervision of employees might have to be carried our remotely. The Management's supervision and review helps to deter and detect both errors and fraud.
- Independent Checks on Performance: In manual systems, independent checks are carried out because employees are likely to forget procedures, make genuine mistakes, become careless, or intentionally fail to follow prescribed procedures. If the program code in a computer system is authorized, accurate, and complete; the system will always follow the designated procedures in the absence of some other type of failure like hardware or systems software failure.

- Comparing Recorded Accountability with Assets: Data and the assets that the data purports to represent should periodically be compared to determine whether incompleteness or inaccuracies in the data exist or whether shortages or excesses in the assets have occurred. In a manual system, independent staff prepares the basic data used for comparison purposes. In a computer system, however, software is used to prepare this data. Again, internal controls must be implemented to ensure the veracity of program code, because traditional separation of duties no longer applies to the data being prepared for comparison purposes.
- Delegation of Authority and Responsibility: A clear line of authority and responsibility is an essential control in both manual and computer systems. In a computer system, however, delegating authority and responsibility in an unambiguous way might be difficult because some resources are shared among multiple users. Further, more users are developing, modifying, operating, and maintaining their own application systems instead of having this work performed by IS professionals.

9. Following are the major techniques to commit cyber frauds:

- Hacking: It refers to unauthorized access and use of computer systems, usually by means of personal computer and a telecommunication network. Normally, hackers do not intend to cause any damage.
- Cracking: Crackers are hackers with malicious intentions, which means, un-authorized entry. Now across the world hacking is a general term, with two nomenclatures namely: Ethical and Un-ethical hacking. Un-ethical hacking is classified as Cracking.
- Data Diddling: Changing data before, during, or after it is entered into the system in order to delete, alter, or add key system data is referred as data diddling.
- Data Leakage: It refers to the unauthorized copying of company data such as computer files.
- Denial of Service (DoS) Attack: It refers to an action or series of actions that prevents access to a software system by its intended/authorized users; causes the delay of its time-critical operations; or prevents any part of the system from functioning.
- Internet Terrorism: It refers to the using Internet to disrupt electronic commerce and to destroy company and individual communications.
- Logic Time Bombs: These are the program that lies idle until some specified circumstances or a particular time triggers it. Once triggered, the bomb sabotages the system by destroying programs, data or both.
- Masquerading or Impersonation: In this case, perpetrator gains access to the system by pretending to be an authorized user.

- Password Cracking: Intruder penetrates a system's defence, steals the file containing valid passwords, decrypts them and then uses them to gain access to system resources such as programs, files and data.
- Piggybacking: It refers to the tapping into a telecommunication line and latching on to a legitimate user before s/he logs into the system.
- Round Down: Computer rounds down all interest calculations to 2 decimal places. Remaining fraction is placed in account controlled by perpetrator.
- Scavenging or Dumpster Diving: It refers to the gaining access to confidential information by searching corporate records.
- Social Engineering Techniques: In this case, perpetrator tricks an employee into giving out the information needed to get into the system.
- Super Zapping: It refers to the unauthorized use of special system programs to bypass regular system controls and performs illegal acts.
- Trap Door: In this technique, perpetrator enters in the system using a back door that bypasses normal system controls and perpetrates fraud.

10. The eight phases involved in the development of a Business Continuity Plan (BCP) are as follows:

- Phase 1 – Pre-Planning Activities (Project Initiation): This Phase is used to obtain an understanding of the existing and projected computing environment of the organization. This enables the project team to refine the scope of the project and the associated work program; develop project schedules; and identify and address any issues that could have an impact on the delivery and the success of the project.

  During this phase, a Steering Committee should be established that have the overall responsibility for providing direction and guidance to the Project Team. The Project Manager should work with the Steering Committee in finalizing the detailed work plan and developing interview schedules for conducting the Security Assessment and the Business Impact Analysis. Two other key deliverables of this phase are the development of a policy to support the recovery programs; and an awareness program to educate management and senior individuals who will be required to participate in the project.
- Phase 2 – Vulnerability Assessment and General Definition of Requirements: This phase addresses measures to reduce the possibility of disaster occurrence, rather than concentrating primarily on minimizing impact of an actual disaster. This phase includes the following key tasks:
  - 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.
- Assemble Project Team and conduct awareness sessions.

- Phase 3 – Business Impact Assessment (BIA): A Business Impact Assessment (BIA) of all business units that are part of the business environment enables the project team to identify critical systems, processes and functions; assess the economic impact of incidents and disasters that result in a denial of access to systems services and other services and facilities; and assess the "pain threshold," that is, the length of time business units can survive without access to systems, services and facilities. The BIA Report should be presented to the Steering Committee that identifies critical service functions and the timeframes in which they must be recovered after interruption. The BIA Report should then be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities.
- Phase 4 – Detailed Definition of Requirements: During this phase, a profile of recovery requirements is developed and is used as a basis for analyzing alternative recovery strategies and identifying resources required to support critical functions identified in Phase 3. This profile should include hardware (mainframe, data and voice communications and personal computers), software (vendor supplied, in-house developed, etc.), documentation (DP, user, procedures), outside support (public networks, DP services, etc.), facilities (office space, office equipment, etc.) and personnel for each business unit. Recovery Strategies will be based on short term, intermediate term and long term outages. Another key deliverable of this phase is the definition of the plan scope, objectives and assumptions.
- Phase 5 – Plan Development: During this phase, recovery plans components are defined and plans are documented. This phase also includes the implementation of changes to user procedures, upgrading of existing data processing operating procedures required to support selected recovery strategies and alternatives,

vendor contract negotiations (with suppliers of recovery services) and the definition of Recovery Teams, their roles and responsibilities. Recovery standards are also be developed during this phase.

- Phase 6 – Testing/Exercising Program: The plan Testing/Exercising Program is developed during this phase. Testing/exercising goals are established and alternative testing strategies are evaluated. Testing strategies tailored to the environment should be selected and an on-going testing program should be established.
- Phase 7 – Maintenance Program: Maintenance of the plans is critical to the success of an actual recovery. The plans must reflect changes to the environments that are supported by the plans. It is critical that existing change management processes are revised to take recovery plan maintenance into account. In areas, where change management does not exist, change management procedures will be recommended and implemented. Many recovery software products take this requirement into account.
- Phase 8 – Initial Plan Testing and Implementation: Once plans are developed, initial tests of the plans are conducted and any necessary modifications to the plans are made based on an analysis of the test results. Specific activities of this phase include defining the test purpose/approach; identifying test teams; structuring the test; conducting the test; analyzing test results; and modifying the plans as appropriate. As the recovery strategies are defined, specific testing procedures should be developed to ensure that the written plans are comprehensive and accurate.

11. It is important to keep preparations including documentation, up-to-date for the following reasons:

- Contracts and agreements are needed to reflect the changes.
- If additional equipment is needed, it must be maintained and periodically replaced when it is no longer dependable or no longer fits the organization's architecture.
- The BCM maintenance process demonstrate the documented evidence of the proactive management and governance of the enterprise's business continuity program; the key people who are to implement the BCM strategy and plans are trained and competent; the monitoring and control of the BCM risks faced by the enterprise; and the evidence that material changes to the enterprise's structure, products and services, activities, purpose, staff and objectives have been incorporated into the enterprise's business continuity and incident management plans.

The following documents (representative only) are classified as being part of the Business Continuity Management system:

- The business continuity policy;
- The business continuity management system;

- The business impact analysis report;
- The risk assessment report;
- The aims and objectives of each function;
- The activities undertaken by each function;
- The business continuity strategies;
- The overall and specific incident management plans;
- The business continuity plans;
- Change control, preventative action, corrective action, document control and record control processes;
- Local Authority Risk Register;
- Exercise schedule and results;
- Incident log; and
- Training program.

12. Business Impact Analysis (BIA): Business Impact Analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. The process of BIA determines and documents the impact of a disruption of the activities that support its key products and services. It enables the business continuity team to identify critical systems, processes and functions, assess the economic impact of incidents and disasters that result in a denial of access to the system, services and facilities, and assess the "pain threshold, "that is, the length of time business units can survive without access to the system, services and facilities. For each activity supporting the delivery of key products and services within the scope of its Business Continuity Management (BCM) program, the enterprise should:

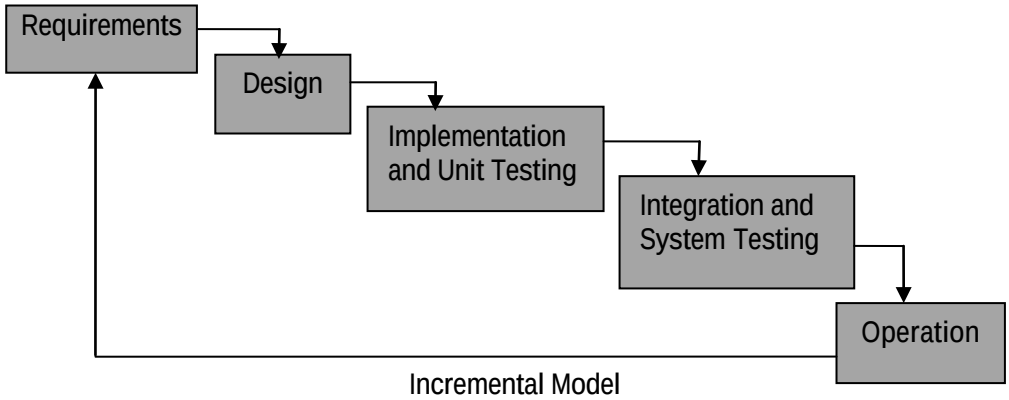
    - assess the impacts that would occur if the activity was disrupted over a period of time;
    - identify the maximum time period after the start of a disruption within which the activity needs to be resumed;
    - identify critical business processes;
    - assess the minimum level at which the activity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

    The enterprise should have a documented approach to conduct BIA. The enterprise should document its approach to assessing the impact of disruption and its findings and conclusions. The BIA Report should be presented to the Top Management. This report

identifies critical service functions and the time frame in which they must be recovered after interruption. The BIA Report should then be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities. Developing the Business Continuity Plan (BCP) also takes into account the BIA process.

13. Incremental Model: The Incremental Model is a method of software development where the model is designed, implemented and tested incrementally (a little more is added each time) until the product is finished. The product is defined as finished when it satisfies all of its requirements. This model combines the elements of the waterfall model with the iterative philosophy of prototyping. The product is decomposed into a number of components, each of which are designed and built separately. Each component is delivered to the client when it is complete. This allows partial utilization of product and avoids a long development time. It also creates a large initial capital outlay with the subsequent long wait avoided. This model of development also helps to ease the traumatic effect of introducing completely new system all at once. A few pertinent features are listed as follows:

- A series of mini-waterfalls are performed, where all phases of the waterfall development model are completed for a small part of the system, before proceeding to the next increment.
- Overall requirements are defined before proceeding to evolutionary, mini – Waterfall development of individual increments of the system.
- The initial software concept, requirement analysis, and design of architecture and system core are defined using the Waterfall approach, followed by iterative Prototyping, which culminates in installation of the final prototype (i.e. Working system).



Incremental Model

Strengths: Some of the strengths of Incremental Model identified by the experts and practitioners include the following:

- Potential exists for exploiting knowledge gained in an early increment as later increments are developed.
- Moderate control is maintained over the life of the project through the use of written documentation and the formal review and approval/signoff by the user and information technology management at designated major milestones.
- Stakeholders can be given concrete evidence of project status throughout the life cycle.
- It is more flexible and less costly to change scope and requirements.
- It helps to mitigate integration and architectural risks earlier in the project.
- It allows the delivery of a series of implementations that are gradually more complete and can go into production more quickly as incremental releases.
- Gradual implementation provides the ability to monitor the effect of incremental changes, isolated issues and make adjustments before the organization is negatively impacted.

Weaknesses: Some of the weaknesses of Incremental Model identified by the experts and practitioners include the following:

- When utilizing a series of mini-waterfalls for a small part of the system before moving onto the next increment, there is usually a lack of overall consideration of the business problem and technical requirements for the overall system.
- Each phase of an iteration is rigid and do not overlap each other.
- Problems may arise pertaining to system architecture because not all requirements are gathered up front for the entire software life cycle.
- Since some modules will be completed much earlier than others, well-defined interfaces are required.
- It is difficult to demonstrate early success to management.

14. Some of the prominent System Development Tools are as follows:

(a) Structured English: Structured English 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.

(b) Flowcharts: 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.

(c) Data Flow Diagrams: A Data Flow Diagram (DFD) uses few simple symbols to illustrate the flow of data among external entities (such as people or organizations, etc.), processing activities and data storage elements. A DFD is composed of four basic elements - Data Sources and Destinations, Data Flows, Transformation processes, and Data stores and have specified symbols.

(d) Decision Tree: A Decision Tree is a support tool that uses a tree-like graph or model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility. Decision tree is commonly used in operations research, specifically in decision analysis, to help identify a strategy most likely to reach a goal and to calculate conditional probabilities.

(e) Decision Table: A Decision Table is a table, which may accompany a flowchart, defining the possible contingencies that may be considered within the program and the appropriate course of action for each contingency. Decision tables are necessitated by the fact that branches of the flowchart multiply at each diamond (comparison symbol) and may easily run into scores and even hundreds. If, therefore, the programmer attempts to draw a flowchart directly, s/he is liable to miss some of the branches.

(f) CASE Tools: CASE (Computer-Aided-Software Engineering) refers to the automation of anything that humans do to develop systems and support virtually all phases of traditional system development process. For example, these packages can be used to create complete and internally consistent requirements specifications with graphic generators and specifications languages. An ideal CASE system would have an integrated set of tools and features to perform all aspects in the life cycle. Some of the features that various CASE products possess are - Repository / Data Dictionary; Computer aided Diagramming Tools; Word Processing; Screen and Report generator; Prototyping; Project Management; Code Generation; and Reverse Engineering.

(g) System Components Matrix: A System Component Matrix provides a matrix framework to document the resources used, the activities performed and the information produced by an information system. It can be used as an information system framework for both systems analysis and system design and views the information system as a matrix of components that highlights how the basic activities of input, processing, output, storage and controls are accomplished in an information system; and how the use of hardware, software and people resources can convert data resources into information products.

(h) Data Dictionary: A Data Dictionary contains descriptive information about the data items in the files of a business information system. Thus, a data dictionary is a computer file about data. Each computer record of a data dictionary contains

information about a single data item used in a business information system. This information may include - the identity of the source document(s) used to create the data item; the names of the computer files that store the data item; the names of the computer programs that modify the data item; the identity of the computer programs or individuals permitted to access the data item for the purpose of file maintenance, upkeep, or inquiry; the identity of the computer programs or individuals not permitted to access the data item etc.

(i) User Interface Layout and Forms: Several type layout forms for both soft and hard copy are used to model input/output components of an automated information system. Some of the prominent and inevitable ones are Layout form and Screen Generator; Menu Generator; Report Generator and Code Generator.

15. System Maintenance is an important aspect of SDLC. As key personnel change positions in the organization, new changes will be implemented, which will require system updates at regular intervals. Most of the information systems require at least some modification after development. The need for modification arises from a failure to anticipate/capture all the requirements during system analysis/design and/or from changing organizational requirements. Maintenance can be categorized in the following ways:

- Scheduled Maintenance: Scheduled maintenance is anticipated and can be planned for operational continuity and avoidance of anticipated risks. For example, the implementation of a new inventory coding scheme can be planned in advance, security checks may be promulgated etc.
- Rescue Maintenance: Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate troubleshooting solution. A system that is properly developed and tested should have few occasions of rescue maintenance.
- Corrective Maintenance: Corrective maintenance deals with fixing bugs in the code or defects found during the executions. A defect can result from design errors, logic errors coding errors, data processing and system performance errors. The need for corrective maintenance is usually initiated by bug reports drawn up by the end users. Examples of corrective maintenance include correcting a failure to test for all possible conditions or a failure to process the last record in a file.
- Adaptive Maintenance: Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system. The term environment in this context refers to the totality of all conditions and influences, which act from outside upon the system, for example, business rule, government policies, work patterns, software and hardware operating platforms. The need for adaptive maintenance can only be recognized by monitoring the environment.

- Perfective Maintenance: Perfective maintenance mainly deals with accommodating to the new or changed user requirements and concerns functional enhancements to the system and activities to increase the system's performance or to enhance its user interface.
- Preventive Maintenance: Preventive maintenance concerns with the activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system. The long-term effect of corrective, adaptive and perfective changes increases the system's complexity. As a large program is continuously changed, its complexity, which reflects deteriorating structure, increases unless work is done to maintain or reduce it. This work is known as preventive change.

16. Audit of Information Systems is required due to following reasons:
    - Organisational Costs of Data Loss: Data is a critical resource of an organisation for its present and future process and its ability to adapt and survive in a changing environment.
    - Cost of Incorrect Decision Making: Management and operational controls taken by managers involve detection, investigations and correction of the processes. These high level decisions require accurate data to make quality decision rules.
    - Costs of Computer Abuse: Unauthorised access to computer systems, malwares, unauthorised physical access to computer facilities and unauthorised copies of sensitive data can lead to destruction of assets (hardware, software, data, information etc.)
    - Value of Computer Hardware, Software and Personnel*:* These are critical resources of an organisation, which has a credible impact on its infrastructure and business competitiveness.
    - High Costs of Computer Error: In a computerised enterprise environment where many critical business processes are performed, a data error during entry or process would cause great damage.
    - Maintenance of Privacy: Today, data collected in a business process contains private information about an individual too. These data were also collected before computers but now, there is a fear that privacy has eroded beyond acceptable levels.
    - Controlled evolution of computer Use: Use of Technology and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.
17. 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

onto 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 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.

18. Section 10 of IT Amendment Act 2008 discusses the provision of "Power to make rules by Central Government in respect of Electronic Signature" which states that -

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

(a) the type of Electronic Signature;

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

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

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

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

19. Mandatory audits of systems and processes bring transparency in the complex workings of Securities and Exchange Board of India (SEBI), prove integrity of the transactions and build confidence among the stakeholders. SEBI has mandated that exchanges shall conduct an annual system audit by a reputed independent auditor. The guidelines recommended by Securities and Exchange Board of India (SEBI) to conduct audit of systems are as follows:

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

20. Emerging threats under "Bring Your Own Device (BYOD)" can be classified into four areas as outlined below:

- Network Risks: It is normally exemplified and hidden in 'Lack of Device Visibility'. When company-owned devices are used by all employees within an organization, the organization's Information Technology practice has complete visibility of the devices connected to the network. This helps to analyze traffic and data exchanged over the Internet. As BYOD permits employees to carry their own devices (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the network. As network visibility is of high importance, this lack of visibility can be hazardous. For example - if a virus hits the network and all the devices connected to the network need be scanned, it is probable that some of the devices would miss out on this routine scan operation. In

addition to this, the network security lines become blurred when BYOD is implemented.

- Device Risks: It is normally exemplified and hidden in 'Loss of Devices'. A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information. Data lost from stolen or lost devices ranks as the top security threats as per the rankings released by Cloud Security Alliance. With easy access to company emails as well as corporate intranet, company trade secrets can be easily retrieved from a misplaced device.
- Application Risks: It is normally exemplified and hidden in 'Application Viruses and Malware'. With an increase in mobile usage, mobile vulnerabilities have increased concurrently. Organizations are not clear in deciding that 'who is responsible for device security – the organization or the user'.
- Implementation Risks: It is normally exemplified and hidden in 'Weak BYOD Policy'. The effective implementation of the BYOD program should not only cover the technical issues mentioned above but also mandate the development of a robust implementation policy. Because corporate knowledge and data are key assets of an organization, the absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse. In addition to this, a weak policy fails to educate the user, thereby increasing vulnerability to the above mentioned threats.

21. (a) Governance of Enterprise IT (GEIT) 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. Some of the key benefits of GEIT are as follows:

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

    (b) Two types of planning languages that are commonly used in DSS are General-purpose planning languages and Special-purpose planning languages. These are discussed below:

- General-purpose planning languages that allow users to perform many routine tasks, for example; retrieving various data from a database or performing statistical analyses. The languages in most electronic spreadsheets are good examples of general-purpose planning languages. These languages enable user to tackle abroad range of budgeting, forecasting, and other worksheet-oriented problems.
- Special-purpose planning languages are more limited in what they can do, but they usually do certain jobs better than the general-purpose planning languages. Some statistical languages, such as SAS (Statistical Analysis System) and SPSS (Statistical Package for the Social Sciences) are examples of special purpose planning languages.

(c) Objectives and Goals of Business Continuity Planning (BCP): The primary objective of a Business Continuity Plan is to minimize loss by minimizing the cost associated with disruptions and enable an organization to survive a disaster and to re-establish normal business operations. In order to survive, the organization must assure that critical operations can resume normal processing within a reasonable time frame. The key objective of the contingency plan should be to:

- Provide the safety and well-being of people on the premises at the time of disaster;
- Continue critical business operations;
- Minimize the duration of a serious disruption to operations and resources (both information processing and other resources);
- Minimize immediate damage and losses;
- Establish management succession and emergency powers;
- Facilitate effective co-ordination of recovery tasks;
- Reduce the complexity of the recovery effort; and
- Identify critical lines of business and supporting functions.

The goals of the Business Continuity Plan should be to:

- Identify weaknesses and implement a disaster prevention program;
- minimize the duration of a serious disruption to business operations;
- facilitate effective co-ordination of recovery tasks; and
- reduce the complexity of the recovery effort.

(d) Strengths of Agile Model: Some of the strengths identified by the experts and practitioners include the following:

- 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.

(e) In System Development Life Cycle (SDLC), some of the roles that an auditor has to perform are following:

- To attend project and steering committee meetings and examine project control documentation and conducting interviews in order to ensure 'what project control standards are to be complied with, (such as a formal systems development process) and determining the extent to which compliance is being achieved;
- To examine system documentation such as functional specifications to arrive at an opinion on controls based on the degree to which the system satisfies the general control objectives that any information system should meet;
- To provide a list of the standard controls, over such operational concerns as response time, CPU usage, and random access space availability that the auditor has used as assessment criteria;
- To rate various phases of SDLC on a rating system scale of 1 to 10 ;
- To give control objectives, directives and in general, validate the opinion expressed by technical experts.
- To provide control considerations that include documented policy and procedures; Established Project team with all infrastructure and facilities; Developers/ IT managers are trained on the procedures; Appropriate approvals are being taken at identified mile-stones; Development is carried over as per standards, functional specifications; Separate test environment for development/ test/ production / test plans; Design norms and naming conventions are as per standards and are adhered to; Business owners testing and approval before system going live; Version control on programs; Source Code is properly secured; Adequate audit trails are provided in system; and Appropriateness of methodologies selected etc.;

- To determine if the expected benefits of the new system are realized and whether users are satisfied with the new system during post implementation review etc.

22. (a) 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.

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.

(b) Open System: An Open System interacts with other systems in its environment. For example - Information system is an open system because it takes input from the environment and produces output to the environment, which changes as per the changes in the environment.

Closed System: Closed System does not interact with the environment and does not change with the changes in environment. Consider a 'throw-away' type sealed digital watch, which is a system, composed of a number of components that work in a cooperative fashion designed to perform some specific task. This watch is a closed system as it is completely isolated from its environment for its operation.

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

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

(d) Quality Assurance Management Control: It is responsible for ensuring information systems development; implementation, operation, and maintenance conform to established quality standards. Organizations are increasingly producing safety-critical systems and users are becoming more demanding in terms of the

quality of the software they employ to undertake their work. Organizations are undertaking more ambitious information systems projects that require more stringent quality requirements and are becoming more concerned about their liabilities if they produce and sell defective software.

Security Management Control: It is responsible for access controls and physical security over the information systems function. Information security administrators are responsible for ensuring that information systems assets are secure. Assets are secure when the expected losses that will occur over some time are at an acceptable level. Some of the major threats and to the security of information systems and their controls are Fire, Water, Energy Variations, Structural Damage, Pollution, Unauthorized Intrusion, Viruses and Worms, Misuse of software, data and services, Hackers etc.

(e) Program Debugging: Debugging is the most primitive form of testing activity which refers to correcting programming language syntax and diagnostic errors so that the program compiles cleanly. A clean compile means that the program can be successfully converted from the source code written by the programmer into machine language instructions. Debugging can be a tedious task consisting of following four steps - Give input the source program to the compiler; Let the compiler to find errors in the program; Correct lines of code that are erroneous, and Resubmit the corrected source program as input to the compiler.

Program Testing: A careful and thorough testing of each program is imperative to the successful installation of any system. The programmer should plan the testing to be performed, including testing of all the possible exceptions. The test plan should require the execution of all standard processing logic based on chosen testing strategy/techniques. The program test plan should be discussed with the project manager and/or system users. A log of test results and all conditions successfully tested should be kept. The log will prove invaluable in finding the faults and debugging.

23. (a) The final deliverable during the System Requirements Analysis (SRA) phase is Systems Requirements Specification (SRS). The activities to be performed during this phase are as follows:

- To identify and consult the stakeholders to determine their expectations and resolve their conflicts;
- To analyze requirements to detect and correct conflicts and determine their priorities;
- To verify that the requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable;
- To gather data or find facts using tools like interviewing, research/document collection, questionnaires, observation;

- To model the activities such as developing models to document Data Flow Diagrams, E-R Diagrams; and
- To document activities such as interview, questionnaires, reports etc. and development of a system (data) dictionary to document the modelling activities.

(b) The major Boundary controls of the system are the access control mechanisms. Access controls are implemented with an access control mechanism and links the authentic users to the authorized resources for which they 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 as follows:

- Cryptography: It deals with programs for transforming data into codes that are meaningless to anyone, who does not possess the authentication to access the respective system resource or file. A cryptographic technique encrypts data into cryptograms and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst. The 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 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. 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, encryption of passwords and number of entry attempts.
- Personal Identification Numbers (PIN): PIN is similar to a password assigned to a user by an institution based on the user characteristics and encrypted using a cryptographic algorithm or the institute generates a random number stored in its database independent to a user identification details, or a customer selected number. Hence, a PIN or a digital signature are 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 used to identify a user; 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.

24. (a) During the automation of various processes of ABC Company, the technical consultant of the company has given the following major suggestions:

- By realizing the importance of information security, he suggested to introduce it right from the beginning.
- In addition, he also suggested performing the risk assessment activity.
- Finally, he advised to mitigate the assessed risk.

For the implementation of all the above mentioned suggestions, the company takes the following steps:

- The company followed various best practices for each process for the proper implementation of the suggestions.
- In addition, the company also tested the compliance of appropriate standards' after each activity, to check the quality of each process.
- Further, the company also implemented the policies related to business continuity planning and disaster recovery to ensure three broad expectations from the software: resist, tolerate and recover.

(b) Recovery Plan: The Recovery plans set out procedures to restore full information system capabilities. Recovery plans should identify a recovery committee that will be responsible for working out the specification of the recovery to be undertaken.

The plan should specify the responsibilities of the committee and provide guidelines on priorities to be followed. The plan might also indicate '*which applications are to be recovered first*'. Members of a recovery committee must understand their responsibilities and must periodically review and practice for executing their responsibilities so that they are prepared for a disaster. If committee members leave the organization, new members must be appointed immediately and briefed about their responsibilities.

(c) A good Information 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 (BCP),
- Legal compliances,
- Monitoring and auditing requirements, and
- Underlying technical policy.

25. (a) Conversion from existing information system to a new system involves the following activities:

(i) Defining the procedures for correcting and converting the data into the new application, determining 'what data can be converted through software and what data manually';

(ii) Performing data cleansing before data conversion;

(iii) Identifying the methods to assess the accuracy of conversion like record counts and control totals;

(iv) Designing exception reports showing the data which could not be converted through software; and

(v) Establishing responsibility for verifying and signing off and accepting overall conversion by the system owner.

(b) The different office activities under Office Automation Systems (OAS) are discussed as under:

(i) Document capture: Documents originating from outside sources like incoming mails, notes, handouts, charts, graphs etc. need to be preserved.

(ii) Document Creation: This consists of preparation of documents, dictation, editing of texts etc. and takes up major part of the secretary's time.

(iii) Receipts and Distribution: This basically includes distribution of correspondence to designated recipients.

(iv) Filling, Search, Retrieval and Follow-up: This is related to filling, indexing, searching of documents, which takes up significant time.

(v) Calculations: These include the usual calculator functions like routine arithmetic, operations for bill passing, interest calculations, working out the percentages and the like.

(vi) Recording Utilization of Resources: This includes, where necessary, record keeping in respect of specific resources utilized by office personnel.

All the activities mentioned have been made very simple and effective by the use of computers. The application of computers to handle the office activities is also termed as office automation.

(c) Business Continuity Planning (BCP) is the creation and validation of a practical logistical plan for how an organization will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a Business Continuity Plan. Planning is an activity to be performed before the disaster occurs otherwise it would be too late to plan an effective response. The resulting outage from such a disaster can have serious effects on the viability of a firm's operations, profitability, quality of service, and convenience.

Business Continuity covers the following areas:

(i) Business Resumption Planning: The Operation's piece of business continuity planning;

(ii) Disaster Recovery Planning: The technological aspect of BCP, the advance planning and preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of a disaster.

(iii) Crisis Management: The overall co-ordination of an organization's response to a crisis in an effective timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation or ability to operate.