

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

Information Systems Concepts

1. (a) Explain some of the important implications of information systems in business.
(b) What are the major characteristics of computer based Information Systems? Explain in brief.
2. Describe the main pre-requisites of a Management Information System (MIS), which make it an effective tool.

Software Development Life Cycle Methodology

3. XYZ Ltd., primarily engaged in games development is in the process of automation of its various business processes. After considering all the relevant factors, the technical consultant of the company recommended to follow a combination of prototyping and waterfall model both for the project implementation. Identify the model and explain its basic principles.
4. (a) Discuss the major issues, which are typically addressed in the Feasibility Study of a project under SDLC.
(b) 'There are two primary methods, which are used to analyze the scope of a project under SDLC'. Explain those methods in brief.
5. (a) Management should establish acquisition standards that address the same security and reliability as development standards. What should be the focusing areas of acquisition standards?
(b) Discuss various categories of tests that a programmer should typically perform on a program unit.

Control Objectives

6. (a) Discuss the general questions, which are needed to be considered by an auditor for quality control.
(b) Describe major weaknesses associated with the packet filtering firewalls.
7. Describe the metrics used for the evaluation of effectiveness and efficiency of the system maintenance.
8. (a) Explain the possible ways for controlling the remote and distributed data processing applications.
(b) What is Data Privacy? Explain major techniques that are used to address Privacy Protection for IT Systems.

Testing – General and Automated Controls

9. (a) During the review of hardware, how will you review the hardware acquisition plan?
(b) While reviewing a network, what are the tasks, which should be accomplished by a reviewer to test the physical security?

Risk Assessment Methodologies and Applications

10. (a) What are the major categories of risk management strategies. Explain in brief.
(b) What do you understand by the term 'Risk Assessment'? Also discuss the areas needed to be focused for the risk assessment.

Business Continuity Planning and Disaster Recovery Planning

11. (a) What do you mean by 'Business Continuity Planning'? Also explain the areas covered by business continuity.
(b) A company has decided to outsource its alternate back-up and recovery process to a third party site. What are the issues which must be considered by the security administrator while drafting the contract?

An Overview of Enterprise Resource Planning (ERP)

12. (a) PQR Ltd. has recently migrated to real-time integrated ERP System. As an IS Auditor, advice the company as to what kinds of businesses risks it can face?
(b) Describe the general guidelines, which are to be followed before starting the implementation of an ERP package.

Information Systems Auditing Standards, Guidelines, Best Practices

13. What are the detailed controls and objectives of Systems Development and Maintenance with respect to Information Security Management System?
14. Define the following terms with reference to CMM:
(i) Software Process Capability,
(ii) Software Process Performance, and
(iii) Software Process Maturity

Drafting of IS Security Policy, Audit Policy, IS Audit Reporting- A Practical Perspective

15. (a) Explain Preventive and Restorative Information Protection with the help of examples.
(b) What are the major points that are needed to be taken into consideration for Access Control with reference to Information Security Policy?

Information Technology (Amendment) Act 2008

16. (a) Discuss the 'Authentication of Electronic Records' under Section 3 of Information Technology (Amendment) Act 2008.
(b) Describe the 'Retention of Electronic Records' in the light of Section 7 of Information Technology (Amendment) Act, 2008.
17. Discuss the major functions, which may be performed by the Controller of Certifying Authorities under Section 18 of Information Technology (Amendment) Act, 2008.

Questions based on Short Notes

18. Write short notes on the following:
 - (a) Strengths of Agile Methodologies
 - (b) Deterministic and Probabilistic Systems
 - (c) Systematic Risks
19. Write short notes on the following:
 - (a) Recovery Plan
 - (b) Trojan Horse
 - (c) White Box Testing
20. Write short notes on the following:
 - (a) Incremental Backup and Mirror Backup
 - (b) Important Backup Tips
 - (c) Power of State Government to make rules in the light of Section 90 of Information Technology (Amendment) Act, 2008

Questions based on the Case Studies

21. ABC Ltd. is a company that designs and sells electric cars through its various agencies. The company is focusing on European market where privacy laws are very strong. By recognizing the importance of internet, recently, the company decided to sell the cars online through its website for its worldwide customers. For the development of the company's web applications, the company follows the best practices of SDLC, which consists of various phases starting from 'Preliminary Investigation' till 'Post Implementation Review and Maintenance'. In the initial phases of the SDLC, the company determines the need for the customer information system. Major need for the system is to enable it for tracking customer buying habits and preferences in order to plan future car designs and marketing plans in a better way. The company also knows that the competitors may attack its website; hence, the company adapts the principle of '*integrating security into SDLC right from the beginning*'. The security activity, performed by the company's system development team in this phase is security categorization

based on a preliminary risk assessment for the information system. The security category indicates the importance of the Confidentiality, Integrity, and Availability (CIA) of the customer information system to the company. The design team looks at several risk areas, including sensitivity of information collected; criticality of the system; security risks common to customer information systems; and regulatory, legal, and privacy issues pertinent to customer information systems. The system design team assigns high, medium, and low risk values to each area of risk. Doing the preliminary risk assessment as part of establishing the need for the system helps to identify any security related issues before much time and efforts go into the next SDLC phases. It also gets the design team thinking about security issues early in the SDLC *from the inception itself*. Based on the preliminary risk assessment, the team puts the customer information system in a high risk category.

Read the above carefully and answer the following:

- (a) What is SDLC? Explain the major activities performed in the Requirements Analysis phase.
 - (b) Define Confidentiality, Integrity, and Availability. What should be the level of Confidentiality in terms of high/medium/low for ABC Ltd. in your opinion?
 - (c) Information Security is a key area for web applications in today's vulnerable world. How ABC Ltd. is addressing the same for its website?
 - (d) Discuss some points, which may be considered for establishing better information protection.
22. PQR University is a globally reputed university; specially known for its Department of Information Technology and Management. Recently, the Heads of both the departments decided to launch a web based Course Information System (CIS) to facilitate the students of different courses, which is intended to provide an easy and wide interface for the students and the course instructors to access course/s information. Such a system is expected to provide major benefits and facilitate a better and healthy communication between the course instructors and the students. For the implementation of this project, a technical consultant was appointed by the university. Accordingly, an initial feasibility study under various dimensions was done and a detailed report was submitted, which recommended the departments to go for a complete transformation and listed all the related areas that may be covered under CIS. As a next step, as per the recommendations of the consultant, an expression of interest was released by the University inviting various organizations to showcase their capabilities and suggest a good solution as per the requirements of both the departments of the university.

Read the above carefully and answer the following:

- (a) How the technical consultant is moving forward to address the need of both the departments?

- (b) Feasibility study of the proposed CIS is accomplished under various dimensions such as technical, financial, economical, operational, legal, schedule/time etc. Out of these, explain schedule/time feasibility in brief.
 - (c) Being a web based system; the proposed CIS will be open to various threats to its computerized environment. Discuss any five common threats out of these.
23. XYZ Consultants is a leading consultancy company dealing with the consultation of various domains of information systems and their audit. Recently, the company has been assigned a project of ABC Ltd. relating to Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP). As a first step, the consultant prepared a document for setting the objectives of the proposed project. The primary objective of the BCP set up by them was to minimize the losses by minimizing the cost associated with disruptions and enable the organization to survive a disaster and to re-establish the normal business operations. They further recommended that in order to survive, ABC Ltd. must assure that critical operations can resume the normal processing within a reasonable time frame. After implementation of all the required procedures and controls, an independent audit was also carried out for different activities of BCP and DRP for smooth functioning of the company.

Read the above carefully and answer the following:

- (a) What are the different phases of the methodology for developing a Business Continuity Plan?
 - (b) Discuss the audit tools and techniques used for the auditing of BCP/DRP.
 - (c) Security administrators consider various backup options for alternate processing facility arrangements. Explain any two out of them.
24. ABC Ltd. is a company engaged in the business of manufacturing and supplying of automobile parts. The company has its head office at Delhi, with its five regional offices and several branches across India. Recently, the company faced several problems in the data consolidation and accordingly decided to implement a real time Enterprise Resource Planning (ERP) system. ERP has played an important role in the last decade as a tool to manage and control the operation processes holistically. The implementation of an ERP system not only reduces costs in many areas within the corporation, but also provides immediate and precise information for the managers. The success of any ERP system depends on many key factors; one of the most important key success factors is people. Unless the key man who has the real power on decision making has the basic knowledge of ERP system, and being objectively, even perfect ERP software and experienced consultants cannot ensure the perfection of ERP implementation.

Read the above carefully and answer the following:

- (a) Describe major steps involved in the implementation of a typical ERP package.

- (b) ERP implementation also engenders various fears. Explain any five fears out of those.
- (c) Explain some of the popular expectations from ERP implementation.
25. PQR Technologies Ltd. is in the development of web applications for various domains. For the development purposes, the company is committed to follow the best practices suggested by SDLC. A system development methodology is a formalized, standardized, documented set of activities used to manage a system development project. It refers to the framework that is used to structure, plan and control the process of developing an information system. Each of the available methodologies is best suited to specific kinds of projects, based on various technical, organizational, project and team considerations.
- Read the above carefully and answer the following:
- (a) Describe accountants' involvement in development work in brief.
- (b) 'Waterfall approach is one of the popular approaches for system development'. Explain the basic principles of this approach.
- (c) Briefly describe any five weaknesses of Agile Methodology.

SUGGESTED ANSWERS / HINTS

1. (a) Some of the important implications of Information Systems in business are given as follows:
- Information systems help managers in effective decision-making to achieve the organizational goals.
 - Based on well-designed Information systems, an organization achieve an edge over others in the competitive environment.
 - Information systems help to take right decision at the right time.
 - Innovative ideas for solving critical problems may come out from good Information systems.
 - Knowledge gathered through Information systems may be utilized by managers in unusual situations.
 - An information system is viewed as a process; it can be integrated to formulate a strategy of action or operation.
- (b) Major characteristics of computer based Information Systems are given as follows:
- All systems work for predetermined objectives and the system is designed and developed accordingly.

- In general, a system has a number of interrelated and interdependent subsystems or components. No subsystem can function in isolation; it depends on other subsystems for its inputs.
 - If one subsystem or component of a system fails, in most of the cases, the whole system does not work. However, it depends on how the subsystems are interrelated.
 - The way a subsystem works with another subsystem is called interaction. The different subsystems interact with each other to achieve the goal of the system.
 - The work done by individual subsystems is integrated to achieve the central goal of the system. The goal of individual subsystem is of lower priority than the goal of the entire system.
2. The following are the main pre-requisites of an effective MIS, which make it an effective tool:
- ♦ **Database:** It is a super-file, which consolidates data records formerly stored in many data files. In database, the data is organized in such a way that access mechanism to the data is improved and redundancy is reduced. Normally, the database is subdivided into major information sub-sets needed to run. The database should be user-oriented, capable of being used as a common data source, available to authorized persons only and should be controlled by a separate authority such as DBMS. Such a database is capable of meeting information requirements of its executives, which is necessary for planning, organizing and controlling the operations of the business.
 - ♦ **Qualified System and Management Staff:** MIS should be handled by qualified officers. These officers who are experts in the field should understand clearly the views of their fellow officers. The organizational management base should comprise of two categories of officers (i) System and Computer experts and (ii) Management experts. Management experts should clearly understand the concepts and operations of a computer. Their whole hearted support and cooperation helps in making MIS an effective tool.
 - ♦ **Support of Top Management:** An MIS becomes effective only if it receives the full support of top management. To gain the support of top management, the officer should place all the supporting facts before them and state clearly the benefits, which will accrue from it to the concern. This step certainly enlightens the management and changes their attitude towards MIS.
 - ♦ **Control and Maintenance of MIS:** Control of the MIS means the operation of the system as it was designed to operate. Sometimes, users develop their own procedures or shortcut methods to use the system, which reduces its effectiveness.

To check such habits of users, the management at each level in the organization should device checks for the information system control.

Maintenance is closely related to control. There are times when the need for improvement to the system will be discovered. Formal methods for changing and documenting changes must be provided.

- ◆ **Evaluation of MIS:** An effective MIS should be capable of meeting the information requirements of its executives in future as well. The capability can be maintained by evaluating the MIS and taking appropriate timely action. The evaluation of MIS should take into account the following points:
 - Examining the flexibility to cope with future requirements;
 - Ascertaining the view of the users and designers about the capabilities and deficiencies of the system ; and
 - Guiding the appropriate authority about the steps to be taken to maintain effectiveness of MIS.

3. As given in the scenario, XYZ Ltd. is primarily engaged in games development and after considering all the relevant factors, the technical consultant of the company recommended to follow a combination of prototyping and waterfall model both for the project implementation the model to be used would be *Spiral*.

The spiral model is a software development process, combining elements of both design and prototyping-in-stages, in an effort to combine the advantages of top-down and bottom-up concepts. It is a system development method, which combines the features of the prototyping model and the waterfall model both. The spiral model is intended for large, expensive and complicated projects. Game development is a main area where the spiral model is used and needed, that is because of the size and the constantly shifting goals of those large projects.

Its basic principles are given as follows:

- ◆ The new system requirements are defined in as much detail as possible. This usually involves interviewing a number of users representing all the external or internal users and other aspects of the existing system.
- ◆ A preliminary design is created for the new system. This phase is the most important part of 'Spiral Model' in which all the possible alternatives that can help in developing a cost effective project are analyzed and strategies are decided to use them. This phase has been added specially in order to identify and resolve all the possible risks in the project development. If risks indicate any kind of uncertainty in requirements, prototyping may be used to proceed with the available data and find out possible solution in order to deal with the potential changes in the requirements.

- ◆ A first prototype of the new system is constructed from the preliminary design. This is usually a scaled-down system, and represents an approximation of the characteristics of the final product.
 - ◆ A second prototype is evolved through a fourfold procedure by:
 - evaluating the first prototype in terms of its strengths, weaknesses, and risks;
 - defining the requirements of the second prototype;
 - planning and designing the second prototype; and
 - constructing and testing the second prototype.
4. (a) The following issues are typically addressed in the Feasibility Study of a project under SDLC:
- Determining whether the solution is as per the business strategy;
 - Determining whether the existing system can rectify the situation without a major modification;
 - Defining the time frame for which the solution is required;
 - Determining the approximate cost to develop the system; and
 - Determining whether the vendor product offers a solution to the problem.
- (b) Two primary methods, which are used to analyze the scope of a project under 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, the analyst will 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.
5. (a) Acquisition standards should basically focus on:
- Ensuring security, reliability, and functionality already built into a product.
 - Ensuring managers for complete and appropriate vendor, contract, and licensing reviews and acquiring products compatible with existing systems.

- Including invitations-to-tender and request-for-proposals; Invitations-to-tender involve soliciting bids from vendors when acquiring hardware or integrated systems of hardware and software. Request-for-proposals involve soliciting bids when acquiring off-the-shelf or third-party developed software.
 - Establishing acquisition standards to ensure functional, security, and operational requirements to be accurately identified and clearly detailed in request-for-proposals.
- (b) There are five categories of tests that a programmer should typically perform on a program unit. These are given as follows:
- **Functional Tests:** Functional Tests check 'whether programs do what they are supposed to do or not'. The test plan specifies operating conditions, input values, and expected results, and as per this plan, programmer checks by inputting the values to see whether the actual result and expected result match.
 - **Performance Tests:** Performance Tests should be designed to verify the response time, the execution time, the throughput, primary and secondary memory utilization and the traffic rates on data channels and communication links.
 - **Stress Tests:** Stress testing is a form of testing that is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results. These tests are designed to overload a program in various ways. The purpose of a stress test is to determine the limitations of the program. For example, during a sort operation, the available memory can be reduced to find out whether the program is able to handle the situation.
 - **Structural Tests:** Structural Tests are concerned with examining the internal processing logic of a software system. For example, if a function is responsible for tax calculation, the verification of the logic is a structural test.
 - **Parallel Tests:** In Parallel Tests, the same test data is used in the new and old system and the output results are then compared.
6. (a) The following are the general questions, which are required to be considered by an auditor for quality control:
- Does the system design follow a defined and acceptable standard?
 - Are completed designs discussed and agreed with the users?
 - Does the project's quality assurance procedures ensure that project documentation (e.g. design documents, specifications, test and installation plans) is reviewed against the organization's technical standards and policies, and the User Requirements Specification;

- Do quality reviews follow a defined and acceptable standard?
 - Are quality reviews carried out under the direction of a technically competent person, who is managerially independent from the design team;
 - Are auditors/security staff invited to comment on the internal control aspects of system designs and development specifications?
 - Are statistics of defects uncovered during quality reviews and other forms of quality control maintained and analyzed for trends? Is the outcome of trend analysis feedback into the project to improve the quality of other deliverables?
 - Are defects uncovered during quality reviews always corrected?
 - Are all system resources (hardware, software, documentation) that have passed quality review been placed under change control management and version control?
 - Has a System Installation Plan been developed and quality reviewed?
 - Has a Training Plan been developed and quality reviewed? Has sufficient time and resources been allocated to its delivery? (to avoid "skills stagnation", the delivery of training will need to be carefully scheduled);
- (b) Major weaknesses associated with the packet filtering firewalls are given as follows:
- The system is unable to prevent attacks that exploit application-specific vulnerabilities and functions because the packet filter does not examine packet contents.
 - Logging functionality is limited to the same information used to make access control decisions.
 - Most of such fire walls do not support advanced user authentication schemes.
 - Firewalls are generally vulnerable to attacks and exploitation that take advantage of vulnerabilities in network protocols.
 - The firewalls are easy to misconfigure, which allow traffic to pass that should be blocked.
7. The effectiveness and efficiency of the system maintenance process is evaluated with the following metrics:
- ◆ The ratio of actual maintenance cost per application/operation versus the average of all applications/process;
 - ◆ Average time to deliver change requests;
 - ◆ The number of change requests for the system application that were related to bugs, critical errors, and new functional specifications;

- ◆ The number of production problems per application and per respective maintenance changes;
 - ◆ The instances of divergence from standard procedures such as undocumented applications, unapproved design, and testing reductions;
 - ◆ The quantity of modules returned to development due to errors discovered in acceptance testing; and
 - ◆ Time elapsed to analyze and fix problems.
8. (a) Possible ways for controlling of remote and distributed data processing applications are given as follows:
- Remote access to computer and data files through the network should be implemented.
 - A terminal lock can assure physical security up to some extent.
 - Applications that can be remotely accessed via modems and other devices should be controlled appropriately.
 - Terminal and computer operations at remote locations should be monitored carefully and frequently for violations.
 - In order to prevent the unauthorized users entry into the system, there should be proper control mechanisms over system documentation and manuals.
 - Data transmission over remote locations should be controlled. The location which sends data should attach needed control information that helps the receiving location to verify the genuineness and integrity.
 - When replicated copies of files exist at multiple locations it must be ensured that all are identical copies contain the same information and checks are also done to ensure that duplicate data does not exist.
- (b) **Data Privacy:** This refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data. Privacy problems exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. The most common sources of data that are affected by data privacy issues are:
- Health information,
 - Criminal justice,
 - Financial information,
 - Genetic information, and
 - Location information.

Privacy protection for IT systems: Increasingly, as heterogeneous information systems with different privacy rules are interconnected, technical controls and logging mechanisms (policy appliances) will be required to reconcile, enforce and monitor privacy policy rules (and laws) as information is shared across systems and to ensure accountability for information use. There are several technologies to address privacy protection in enterprise IT systems. These falls into two categories: communication and enforcement, which are given as follows:

(i) Policy Communication

- P3P - The Platform for Privacy Preferences. P3P is a standard for communicating privacy practices and comparing them to the preferences of individuals.

(ii) Policy Enforcement

- XACML - The extensible Access Control Markup Language together with its Privacy Profile is a standard for expressing privacy policies in a machine readable language which a software system can use to enforce the policy in enterprise IT systems.
- EPAL - The Enterprise Privacy Authorization Language is very similar to XACML, but is not yet a standard.
- WS-Privacy - "Web Service Privacy" will be a specification for communicating privacy policy in web services. For example, it may specify how privacy policy information can be embedded in the SOAP envelope of a web service message.

9. (a) During the review of hardware, review of the hardware acquisition plan is accomplished by the following:

- Whether the IS management has issued written policy statements regarding the acquisition of hardware;
- Whether the criteria for the acquisition of hardware are laid out and procedures and forms established to facilitate the acquisition approval process;
- Whether the hardware acquisition plan is in concurrence with the strategic business plan of management;
- Whether there is awareness of the budget constraints;
- Whether the requests for the acquisition of hardware are supported by cost benefit analysis;
- Whether all hardware are purchased through the IS purchasing department to take advantage of volume discounts or other quality benefits;
- Whether the environment is conducive and space is adequate to accommodate the current and new hardware;

- Whether IS management's hardware acquisition plan has taken into consideration technological obsolescence of the installed equipment, as well the new equipment in the acquisition plan;
 - Whether there has been a consideration of lease expirations on current equipment; and
 - Whether documentation for hardware and software specifications, installation requirements, warranties, guarantees and likely lead-time associated with planned acquisitions is properly maintained.
- (b) While reviewing a network, the tasks, which should be accomplished by a reviewer to test the physical security, are given as follows:
- Inspect the LAN wiring closet and transmission wiring and verify they are physically secured.
 - Observe the LAN file server computer and verify it is secured in a manner to reduce the risk of removal of components and the computer itself.
 - Obtain a copy of the key logs for the file server room and the wiring closet, match the key logs to actual keys that have been issued and determine that all keys held are assigned to the appropriate people, for example, the LAN Administrator and support staff.
 - Select a sample of keys held by people without authorized access to the LAN file server facility and wiring closet and determine that these keys do not permit access to these facilities.
 - Look for LAN operating manuals and documentation not properly secured.
 - Environmental controls for LANs are similar to those considered in the mainframe environment. However, the equipment may not require as extensive atmospheric controls as a mainframe. The following should be considered:
 - LAN file server equipment should be protected from the effects of static electricity (anti-static rug) and electrical surges (surge protector)
 - Air conditioning and humidity control systems should be adequate to maintain temperatures within manufacturers' specifications.
 - The LAN should be equipped with an uninterrupted power supply (UPS) that will allow the LAN to operate in case of minor power fluctuations or in case of a prolonged power outage.
 - The LAN file server facility should be kept free of dust, smoke and other matter particularly food.
 - Backup diskettes and tapes should be protected from environmental damage and the effects of magnetic fields.

10. (a) Major categories of risk management strategies are given as follows :

- **Risk Avoidance:** It means 'not doing an activity that involves risk'. It involves losing out on the potential gain that accepting the risk might have provided. For example, not using Internet/public network on a system connected to organization's internal network, instead using a stand-alone PC for Internet usage.
- **Risk Mitigation/Reduction:** It involves implementing controls to protect IT infrastructure and to reduce the severity of the loss or the likelihood of the loss from occurring. For example, using an effective anti-virus solution to protect against the risk of viruses and updating it on timely basis.
- **Risk Transfer:** It involves causing another party to accept the risk i.e. sharing risk with partners or insurance coverage.
- **Risk Retention/Acceptance:** It means formally acknowledging that the risk exists and monitoring it. In some cases, it may not be possible to take immediate action to avoid/mitigate the risk. All risks that are not identified or avoided or transferred are retained by default. These risks are called residual risks. Risk management aims to identify, select and implement the controls that are necessary to reduce residual exposures to acceptable levels.

The goals and mission of an organization should be considered in selecting any of these risk management strategies. It may not be practical to address all identified risks, so priority should be given to the risks that have the potential to cause significant harm to the assets.

(b) **Risk Assessment:** Risk assessment is a step in the risk management procedure. Risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat. A risk assessment can provide an effective approach that will serve as the foundation for avoiding of disasters. Through risk analysis, it is possible to identify, assess and then mitigate the risk.

Risk Assessment is a critical step in disaster and business continuity planning. Risk Assessment is the analysis of threats to resources (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status in the minimum time in case of a disaster. Disasters may lead to vulnerable data and crucial information suddenly becoming unavailable. The unavailability of data may be due to the non-existence or inadequate testing of the existing plan.

The areas to be focused upon are given as follows:

- (i) **Prioritization:** All applications are inventoried and critical ones identified. Each of the critical application is reviewed to assess its impact on the organization, in case a disaster occurs. Subsequently, appropriate recovery

plans are developed.

- (ii) **Identifying critical applications:** Amongst the applications, currently being processed the critical applications are identified. Further analysis is done to determine specific jobs in the applications, which may be more critical. Even though the critical value would be determined based on its present value, future changes should not be ignored.
- (iii) **Assessing their impact on the organization:** Business Continuity Planning (BCP) should not concentrate only on business disruption but should also take into account other organizational functions, which may be affected. The areas to be considered include:
 - Legal liabilities,
 - Interruptions of customer services,
 - Possible losses, and
 - Likelihood of fraud and recovery procedures.
- (iv) **Determining recovery time-frame:** Critical recovery time period is the period of time in which business processing must be resumed before the organization incurs severe losses. This critical time depends upon the nature of operations. It is essential to involve the end users in the identification of critical functions and critical recovery time period.
- (v) **Assess Insurance Coverage:** The information system insurance policy should be a multiperil policy, designed to provide various types of coverage. Depending on the individual organization and the extent of coverage required, suitable modifications may be made to the comprehensive list provided below:
 - **Hardware and facilities:** The equipment should be covered adequately. Provision should be made for the replacement of all equipment with a new one by the same vendor.
 - **Software reconstruction:** In addition to the cost of media, programming costs for recreating the software should also be covered.
 - **Extra expenses:** The cost incurred for continuing the operations till the original facility is restored should also be covered.
 - **Business interruption:** This applies mainly to centres performing outsourced jobs of clients. The loss of profit caused by the damaged computer media should be covered.
 - **Valuable paper and records:** The actual cost of valuable papers and records stored in the insured premises should be covered.

- **Errors and omissions:** This cover is against the legal liability arising out of errors and omissions committed by system analysts, programmes and other information system personnel.
 - **Fidelity coverage:** This coverage is for acts of employees in the case of financial institutions, which use their own computers for providing services to clients.
 - **Media transportation:** The potential loss or damage to media while being transported to off-site storage / premises should be covered.
- (vi) **Identification of exposures and implications:** It is not possible to accurately predict as to when and how a disaster would occur. So, it is necessary to estimate the probability and frequency of disaster.
- (vii) **Development of recovery plan:** The plan should be designed to provide for recovery from total destruction of a site.
11. (a) 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:
- **Business resumption planning** – The Operation's piece of business continuity planning;
 - **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.
 - **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.
- (b) If a third party site is to be used for backup and recovery purposes, security administrators must ensure that a contract is written to cover the following major issues such as:
- How soon the site will be made available subsequent to a disaster;
 - The number of organizations that will be allowed to use the site concurrently in the event of a disaster;

- The priority to be given to concurrent users of the site in the event of a common disaster;
 - The period during which the site can be used;
 - The conditions under which the site can be used;
 - The facilities and services the site provider agrees to make available; and
 - What controls will be in place and working at the off-site facility.
12. (a) The company, PQR Ltd. may face several new business risks when migrating to real-time, integrated ERP systems. These risks include the following:
- *Single point of failure* – All input data of an organization and transaction processing are within one application system, then this may happen.
 - *Structural Changes* - Significant personnel and organizational structural changes associate with reengineering or redesigning business processes.
 - *Job Role Changes* - Traditional roles of users are changed to empowered-based role. They have more chances to access enterprise information in real-time. This point of control shifts from the back-end financial processes to the front-end point of creation.
 - *Online Real-Time* – This environment requires a continuous business interaction. This warrants the capabilities of utilizing the ERP application and responds quickly to any problem that requires a re-entry of information (e.g., if field personnel are unable to transmit orders from handheld terminals, customer service staff may need the skills to enter orders into the ERP system correctly so the production and distribution operations will not be adversely impacted).
 - *Change Management* - It is challenging to bring together a highly integrated environment when different business processes have existed among business units for long. The level of user acceptance of the system has a significant influence on its success. Training and awareness of users is mandatory to understand that their actions or inaction have a direct impact upon other users and in the performance of their day-to-day duties.
 - *Distributed Computing Experience* - Inexperience with implementing and managing this kind of environment may pose significant challenges.
 - *Broad System Accessibility* – Increased remote access by users and outsiders and high integration among application functions allow increased access to the application and data.
 - *Dependency on External Assistance* – Organization accustomed to in-house legacy systems may find that they have to rely on external help. Unless such external assistance is properly managed, it could introduce an element of

security and resource management risk that may expose the organizations to a greater risk.

- *Program Interfaces and Data Conversions*—Extensive interfaces and data conversions from legacy systems and other commercial software are necessary. The exposures of data integrity, security and capacity requirements for ERP are much higher.
 - *Audit Expertise* – Specialist expertise is required to effectively audit and control an ERP environment. The relative complexity of ERP systems has created specialization such that each specialist may know only a relatively small fraction of the entire ERP's functionality in a particular core module, e.g. FI auditors, who are required to audit the entire organization's business processes, have to maintain a good grasp of all the core modules to function effectively.
 - *Single sign on* - It reduces the security administration efforts associated with administering web-based access to multiple systems, but simultaneously introduces additional risks in that an incorrect assignment of access may result in inappropriate access to multiple systems.
 - *Data content quality* - As enterprise applications are opened to external suppliers and customers, the need for integrity in enterprise data becomes paramount.
 - *Privacy and confidentiality* - Regularity and governance issues surrounding the increased capture and visibility of personal information, i.e. spending habits.
- (b) General guidelines, which are to be followed before starting the implementation of an ERP package, are given as follows:
- Understanding the corporate needs and culture of the organization and then adopt the implementation technique to match these factors;
 - Doing a business process redesign exercise prior to starting the implementation;
 - Establishing a good communication network across the organization;
 - Providing a strong and effective leadership so that people down the line are well motivated;
 - Finding an efficient and capable project manager;
 - Creating a balanced team of implementation consultants, who can work together as a team;
 - Selecting a good implementation methodology with minimum customization;
 - Training end-users; and

- Adapting the new system and making the required changes in the working environment to make effective use of the system in future.
13. The detailed controls and objectives of Systems Development and Maintenance with respect to Information Security Management System are given as follows:
- ◆ *Security requirements of system* : To ensure that security is built into information systems;
 - ◆ *Security in application systems* : To prevent loss, modification or misuse of user data in application system;
 - ◆ *Cryptographic Controls* : To protect the confidentiality, authenticity or integrity of information;
 - ◆ *Security of system files* : To ensure that IT projects and support activities are conducted in a secure manner; and
 - ◆ *Security in development and support process*: To maintain the security of application system software and information.
14. (i) **Software Process Capability:** It describes the range of expected results that can be achieved by following a software process. The software process capability of an organization provides one means of predicting the most likely outcomes to be expected from the next software project the organization undertakes.
- (ii) **Software Process Performance:** It represents the actual results achieved by following a software process. Thus, software process performance focuses on the results achieved, while software process capability focuses on results expected.
- (iii) **Software Process Maturity:** This is the extent to which a specific process is explicitly defined, managed, measured, controlled, and effective. Maturity implies a potential for growth in capability and indicates both the richness of an organization's software process and the consistency with which it is applied in projects throughout the organization. As a software organization gains in software process maturity, it institutionalizes its software process via policies, standards, and organizational structures. Institutionalization entails building an infrastructure and a corporate culture that supports the methods, practices, and procedures of the business so that they endure after those who originally defined them have gone.
15. (a) **Preventative Information Protection:** It is based on the use of security controls, which itself is a group of three types of controls such as Physical, Logical, and Administrative. These are briefly given as follows:
- Physical controls deal with Doors, Locks, Guards, Floppy Disk Access Locks, Cables locking systems to desks/walls, CCTV, Paper Shredders, Fire Suppression Systems,

- Logical controls deal with Passwords, File Permissions, Access Control Lists, Account Privileges, Power Protection Systems, and
- Administrative controls deal with Security Awareness, User Account Revocation, and Policy.

Restorative Information Protection: If an organization cannot recover or recreate critical information systems in an acceptable time period, the organization will suffer and possibly have to go out of business. Hence, the key requirement of any restorative information system protection plan is that the information systems can be recovered. The claim of back program to backup data automatically cannot be reliable. It has so many problems. The restorative information protection program must address the following:

- Whether the recovery process has been evaluated and tested recently,
 - The time taken for restoration,
 - The quantum of productivity loss,
 - The strict adherence of plan, and
 - The time needed to input the data changes since the last backup.
- (b) Major points that are needed to be taken into consideration for Access Control with reference to Information Security Policy are given as follows:
- Access controls must be in place to prevent unauthorized access to information systems and computer applications
 - Access must only be granted in response to a business requirement. Formal processes must be in place to provide individuals with access. The requirement for access must be reviewed regularly.
 - System Owners are responsible for approving access to systems and they must maintain records of who has access to a particular system and at what level. The actual access controls in place must be audited against this record on a regular basis.
 - Users should be granted access to systems only up to the level required to perform their normal business functions.
 - The registration and de-registration of users must be formally managed.
 - Access rights must be deleted for individuals who leave or change jobs.
 - Each individual user of an information system or computer application will be provided with a unique user identifier (User ID)
 - It should not be permitted for an individual to use another person's user id or to log-on, to allow another individual to gain access to an information system or computer application.

- PCs and terminals should never be left unattended whilst they are connected to applications or the network. Someone may use the equipment to access confidential information or make unauthorized changes.
- Password Policy should be defined and the structure of passwords and the duration of the passwords should be specified. Passwords must be kept confidential and never disclosed to others.
- Mobile computing - When using mobile computing facilities, such as laptops, notebooks, etc., special care should be taken to ensure that business information is not compromised, particularly when the equipment is used in public places.

16. (a) [Section 3] Authentication of Electronic Records:

- (1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.
- (2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation -

For the purposes of this sub-section, "Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

- (a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
 - (b) that two electronic records can produce the same hash result using the algorithm.
- (3) Any person by the use of a public key of the subscriber can verify the electronic record.
 - (4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

(b) [Section 7] Retention of Electronic Records :

- (1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, -
 - (a) the information contained therein remains accessible so as to be usable for a subsequent reference;

- (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;
- (c) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

However,

this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

- (2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records. Publication of rules, regulation, etc.. in Electronic Gazette.

17. Section 18 of Information Technology (Amendment) Act, 2008 lays down the functions, which the Controller of Certifying Authorities may perform in respect of activities of Certifying Authorities. As per ITAA 2008, Section 18 is given as under:

[Section 18] The Controller may perform all or any of the following functions, namely:

- (a) exercising supervision over the activities of the Certifying Authorities;
- (b) certifying public keys of the Certifying Authorities
- (c) laying down the standards to be maintained by the Certifying Authorities;
- (d) specifying the qualifications and experience which employees of the Certifying Authorities should possess;
- (e) specifying the conditions subject to which the Certifying Authorities shall conduct their business;
- (f) specifying the content of written, printed or visual material and advertisements that may be distributed or used in respect of a Electronic Signature Certificate and the Public Key;
- (g) specifying the form and content of a Electronic Signature Certificate and the key;
- (h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;
- (i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
- (j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;

- (k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
- (l) resolving any conflict of interests between the Certifying Authorities and the subscribers;
- (m) laying down the duties of the Certifying Authorities;
- (n) maintaining a data-base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

18. (a) Strengths of Agile Methodologies: Major strengths of Agile Methodologies are given as follows:

- Agile methodology has the concept of an adaptive team, which is able to respond to the changing requirements. This is the main strength of this methodology.
- 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 no space for guesswork.
- The documentation is crisp and to the point to save time.
- The end result is the high quality software in least possible time duration and satisfied customer.

(b) Deterministic System: A deterministic system operates in a predictable manner wherein the interaction among the parts is known with certainty. If one has a description of the state of the system at a given point in time plus a description of its operation, the next state of the system may be given exactly, without error. An example is a correct computer program, which performs exactly according to a set of instructions.

Probabilistic System: The probabilistic system can be described in terms of probable behavior, but a certain degree of error is always attached to the prediction of what the system will do. An inventory system is an example of a probabilistic system. The average demand, average time for replenishment, etc, may be defined, but the exact value at any given time is not known. Another example is a set of instructions given to a human who, for a variety of reasons, may not follow the instructions exactly as given.

(c) Systematic Risks: These are unavoidable risks, which are constant across majority of the technologies and applications. For example, the probability of power outage is not dependant on the industry but is dependant on external factors. Systematic risks would remain, no matter what technology is used. Thus effort to seek

technological solution to reduce systematic risks would essentially be unfruitful activity and needs to be avoided. Systematic risks can be reduced by designing management control process and does not involve technological solutions. For example, the solution to non availability of consumable is maintaining a high stock of the same. Thus a systematic risk can be mitigated not by technology but by management process. Hence one would not make any additional payment for technological solution to the problem. To put in other words, there would not be any technology linked premium that one should pay trying to reduce the exposure to systematic risk.

19. (a) Recovery Plan: The backup plan is intended to restore operations quickly so the information system function can continue to service an organisation, whereas, 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 specifics 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. Again, the problem is that they will be required to undertake unfamiliar tasks. Periodically, they must review and practice executing their responsibilities so they are prepared should a disaster occur. If committee members leave the organisation, new members must be appointed immediately and briefed about their responsibilities.

(b) 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 Horses hide 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.

(c) **White Box Testing:** This testing technique 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.

20. (a) **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. User will have to start with recovering the last full backup, and then recovering from every incremental backup taken since.

Mirror Backup: A mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they can not be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

(b) **Important Backup Tips:** Major backup tips are given as follows:

- Draw a simple (easy to understand) plan of 'who will do what in the case of an emergency'.
- Be organized! Keep a record of what was backed up, when it was backed up and which backup media contains what data. We can also make a calendar of which type of backup is due on a certain date.
- Utilize the Volume Shadow Copy (VSS) service as provided by Windows Server 2003. This feature allows you to create point-in-time copies of data so that they can be restored and reverted to at any given time. For instance, if a user created a Word document yesterday and decides that s/he wants to revert to it today, s/he can do so using VSS.
- Select the option to verify backup, the process will take a little longer but it's definitely worth the wait.
- Create a reference point where we know everything is working properly. It will be quicker to restore the changes from tape.

- Select the option to restrict restoring data to owner or administrator and also set the Domain Group Policy to restrict the Restore privilege to Administrators only. This will help to reduce the risk of someone being able to restore data should the media be stolen.
- Create a step-by-step guideline (a flowchart for example) clearly outlining the sequence for the retrieval and restoration of data depending on the state of the system.

(c) [Section 90] Power of State Government to make rules:

- (1) The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.
- (2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely ☐
 - (a) the electronic form in which filing, issue, grant receipt or payment shall be effected under sub-section (1) of section 6;
 - (b) for matters specified in sub-section (2) of section 6;
- (3) Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the State Legislature where it consists of two Houses, or where such Legislature consists of one House, before that House.

- 21. (a)** System Development Life Cycle (SDLC) framework provides system designers and developers to follow a sequence of activities. It consists of a set of steps or phases in which each phase of the SDLC uses the results of the previous one. The SDLC is document driven, which means that at crucial stages during the process, documentation is produced. A phase of the SDLC is not complete until the appropriate documentation or artifact is produced. These are sometimes referred to as deliverables.

Major activities, which are performed in the 'Requirements Analysis Phase' is given 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 priorities;
- To verify the requirements to be 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 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 modeling activities.
- (b) **Confidentiality:** It refers to the prevention of the unauthorized disclosure of information.
- Integrity:** It refers to the prevention of the unauthorized modification of information.
- Availability:** It refers to the prevention of the unauthorized withholding of information.
- As given in the scenario, ABC Ltd. is focusing on European market where *privacy laws are very strong*. In addition, the company also determines for the customer information system, which would *collect the personal data from its customers*, viz. their buying habits and preferences etc. Therefore, in our opinion, the level of confidentiality for ABC Ltd. would be high.
- (c) ABC Ltd. has taken the following steps to address Information Security for its website:
- As a first and fundamental step, the company adapted the principle of 'integrating security into SDLC right from the beginning'.
 - The next step was doing security categorization based on a preliminary risk assessment for the information system. The security category indicates the importance of the Confidentiality, Integrity, and Availability (CIA) of the customer information system to the company.
 - Afterwards, the system design team assigned high, medium, and low risk values to each area of risk. Doing the preliminary risk assessment as part of establishing the need for the system helps to identify any security related issues before much time and effort goes into the next SDLC phases.
 - In addition, based on the preliminary risk assessment, the team put the customer information system in a high risk category.
- (d) Major points that may be considered for establishing better information protection are given as follows:
- **Not all data has the same value:** Each data has a different value and accordingly the information may be handled and protected differently. Organizations must determine the value of the different types of information in their environment before they plan for the appropriate levels of protection.
 - **Know where the critical data resides:** Identification of the location where each data is located enables an organization to establish an integrated security solution.

- **Develop an access control methodology:** Information does not have to be removed to cause damage or to have financial impact. Information that is inadvertently damaged, disclosed or copied without the knowledge of the owner may render the data useless. To guard against this, organizations must establish some type of access control methodology.
 - **Protect information stored on media:** Employees can cause considerable damage by walking out the door with information on USB Drives or CD-ROMS. In addition, companies should control magnetic media to reduce the loss of software (both application and operating system) and finally, when migrating from one platform to another, the status of all hard drives and the associated data should be controlled.
 - **Review hardcopy output:** The hardcopy output of employees' daily work should also be reviewed. In addition, 'what measures are used to safeguard all drafts and working papers' should also be reviewed.
22. (a) The technical consultant is moving forward to address the need of both the departments by the following ways:
- First of all, the consultant conducted an initial feasibility study.
 - In addition, they submitted a detailed report, which recommended the departments to go for a complete transformation.
 - They also listed all the related areas that may be covered under CIS.
 - As a next step, as per the recommendations of the consultant, an expression of interest was released by the University inviting various organizations to showcase their capabilities and suggest a good solution as per the requirements of both the departments of the university.
- (b) **Schedule/Time Feasibility:** Schedule feasibility involves the design team's estimation on 'how long it will take a new or revised system to become operational' and communicating this information to the steering committee. For example, if a design team projects that it will take next 16 months for a particular system design to become fully functional, the steering committee may reject the proposal in favor of a simpler alternative that the organization can implement in a shorter time frame.
- (c) Five common threats to its computerized environment of the proposed CIS are given as follows:
- (i) **Power failure:** Power failure can cause disruption of entire computing equipments since computing equipments depend on power supply.
 - (ii) **Communication failure:** Failure of communication lines result in inability to transfer data which primarily travel over communication lines. Where the organization depends on public communication lines, e.g. for e-banking, communication failure present a significant threat that will have a direct impact

on operations.

- (iii) **Disgruntled Employees:** A disgruntled employee presents a threat since, with access to sensitive information of the organization, s/he may cause intentional harm to the information processing facilities or sabotage operations.
- (iv) **Errors:** Errors, which may result from technical reasons, negligence or otherwise can cause significant integrity issues. A wrong parameter setting at the firewall to 'allow' attachments instead of 'deny' may result in the entire organization network being compromised with virus attacks.
- (v) **Malicious code:** Malicious code such as viruses and worms which freely access the unprotected networks may affect organizational and business networks that use these unprotected networks.

23. (a) Different phases of the methodology for developing a Business Continuity Plan are given as follows:

- Pre-Planning Activities (Business continuity plan Initiation),
- Vulnerability Assessment and General Definition of Requirements,
- Business Impact Analysis,
- Detailed Definition of Requirements,
- Plan Development,
- Testing Program,
- Maintenance Program, and
- Initial Plan Testing and Plan Implementation.

(b) The best audit tool and technique is a periodic simulation of a disaster. Other audit techniques would include observations, interviews, checklists, inquiries, meetings, questionnaires and documentation reviews. These tools and methods may be categorized as under:

- **Automated Tools:** Automated tools make it possible to review the large computer systems for a variety of flaws in a short time period. They can be used to find threats and vulnerabilities such as weak access controls, weak passwords, lack of integrity of the system software, etc.
- **Internal Control Auditing:** This includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance of laws and regulations.
- **Disaster and Security Checklists:** A checklist can be used against which the system can be audited. The checklist should be based upon disaster recovery policies and practices, which form the baseline. Checklists can also be used to verify changes to the system from contingency point of view.

- **Penetration Testing:** Penetration testing can be used to locate vulnerabilities.
- (c) Two backup options, which may be considered by the security administrators for alternate processing facility arrangements are given as follows:
- *Cold Site:* If an organization can tolerate some downtime, cold-site backup might be appropriate. A cold site has all the facilities needed to install a mainframe system—raised floors, air conditioning, power, communication lines, and so on. An organisation can establish its own cold-site facility or enter into an agreement with another organisation to provide a cold-site facility.
 - *Hot Site:* If fast recovery is critical, an organisation might need hot site backup. All hardware and operations facilities will be available at the hot site. In some cases, software, data and supplies might also be stored there. A hot site is expensive to maintain. They are usually shared with other organizations that have hot-site needs.
24. (a) Major steps involved in the implementation of a typical ERP package are given as follows:
- Identifying the needs for implementing an ERP package;
 - Evaluating the 'As Is' situation of the business i.e., to understand the strength and weakness prevailing under the existing circumstances;
 - Deciding the 'Would be' situation for the business i.e., the changes expected after the implementation of ERP;
 - Reengineering the Business Process to achieve the desired results in the existing processes;
 - Evaluating the various available ERP packages to assess suitability;
 - Finalising of the most suitable ERP package for implementation;
 - Installing the required hardware and networks for the selected ERP package;
 - Finalising the Implementation consultants who will assist in implementation; and
 - Implementing the ERP package.
- (b) Major fears engendered due to ERP implementation are given as follows:
- Job redundancy;
 - Loss of importance as information is no longer an individual prerogative;
 - Change in job profile;
 - An organizational fear of loss of proper control and authorization;
 - Increased stress caused by greater transparency; and

- Individual fear of loss of authority.

Balancing the expectations and fears is a very necessary part of the implementation process.

(c) Some of the popular expectations from ERP implementation are given as follows:

- An improvement in processes;
- Increased productivity on all fronts;
- Total automation and disbanding of all manual processes;
- Improvement of all key performance indicators;
- Elimination of all manual record keeping;
- Real time information systems available to concerned people on a need basis; and
- Total integration of all operations.

25. (a) **Accountants' involvement in Development work:** Many accountants are uniquely qualified to participate in systems development because they may be among the few people in an organization who can combine knowledge of IT, business, accounting, and internal control, as well as behavior and communications, to ensure that new systems meet the needs of the user and possess adequate internal controls. They have specialized skills - such as accounting and auditing - that can be applied to the development project. For example, an accountant might perform the analysis of a proposed system's costs and benefits.

(b) Basic principles of Waterfall Approach are given as follows:

- Project is divided into sequential phases, with some overlap and splash back acceptable between phases.
- Emphasis is on planning, time schedules, target dates, budgets and implementation of an entire system at one time.
- Tight control is maintained over the life of the project through the use of extensive written documentation, as well as through formal reviews and approval/signoff by the user and information technology management occurring at the end of most phases before beginning the next phase.

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

- In case of some software deliverables, especially the large ones, it is difficult to assess the efforts required at the beginning of the software development life cycle.
- There is lack of emphasis on necessary designing and documentation.

- Agile increases potential threats to business continuity and knowledge transfer. By nature, Agile projects are extremely light on documentation because the team focuses on verbal communication with the customer rather than on documents or manuals.
- Agile requires more re-work. Because of the lack of long-term planning and the lightweight approach to architecture, re-work is often required on Agile projects when the various components of the software are combined and forced to interact.
- The project can easily get taken off track if the customer representative is not clear about the final outcome that they want.
- Only senior programmers are capable of taking the kind of decisions required during the development process. Hence, it has no place for newly appointed programmers, unless combined with experienced resources.
- Agile lacks the attention to outside integration. Because Agile teams often do not invest the time in identifying and designing the integration points with other systems in advance, the need for an integration point can become a last-minute surprise that often requires re-work, additional time, removal from scope, or a poor-quality product.