

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

Question No. 1 is compulsory
Attempt any Four questions from the remaining six questions.

Question 1

- (a) Briefly explain Enterprise Resource Planning(ERP) and describe five of its characteristics.
- (b) Discuss the objectives and goals of Business Continuity planning.
- (c) State the liabilities of companies under section 85 of Information Technology Act, 2000.

(10 + 5 + 5 = 20 Marks)

Answer

- (a) Enterprise Resource Planning (ERP) is the latest high-end solution, that information technology has lent to business applications. ERP solutions streamline and integrate operation processes and information flows in the company to synergise the resources of an organisation namely men, material, money and machine through information. An ERP system is a fully integrated business management system covering functional areas of an enterprise like Logistics, Production, Finance, Accounting and Human Resources.

General Model of ERP

ERP is a global, tightly integrated closed loop business solution package and is multifaceted. It promises one database, one application, and one user interface for the entire enterprise, where once disparate systems ruled manufacturing, distribution,

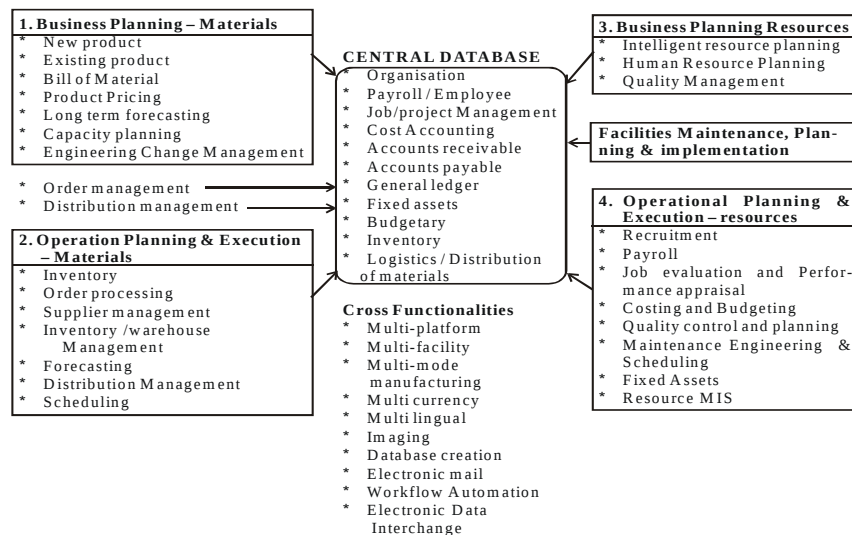


Fig. : General Model of an ERP

finance and sales. Taking information from every function it is a tool that assists employees and managers plan, monitor and control the entire business. A modern ERP system enhances a manufacturer's ability to accurately schedule production, fully utilize capacity, reduce inventory, and meet promised shipping dates. ERP systems are implemented in a three Tier Client Server Architecture; the server stores the data, maintaining its integrity and consistency and processes the requests of the user from the client desktops. The load of data processing and application logic is divided between the server and the client. As companies implementing ERP solutions have multiple locations of operation and control, online data transfer has to be done across locations. To facilitate these transactions, the important enabling technologies for ERP systems are Workflow, Work group, Group Ware, Electronic Data Interchange (EDI), Internet, Intranet, Data warehousing, etc.

ERP Characteristics : An ERP system is not only the integration of various organization processes, any system has to possess few key characteristics to qualify for a true ERP solution. These features are:

Flexibility: An ERP system should be flexible to respond to the changing needs of an enterprise. The client server technology enables ERP to run across various database back ends through Open Database Connectivity (ODBC).

Modular and Open: ERP system has to have open system architecture. This means that any module can be interfaced or detached whenever required without affecting the other modules. It should support multiple hardware platforms for the companies having heterogeneous collection of systems. It must support some third party add-ons also.

Comprehensive: It should be able to support variety of organizational functions and must be suitable for a wide range of business organizations.

Beyond The Company: It should not be confined to the organizational boundaries, rather support the on-line connectivity to the other business entities of the organization.

Best Business Practices: It must have a collection of the best business processes applicable worldwide. An ERP package imposes its own logic on a company's strategy, culture and organisation.

- (b) **Objectives and Goals of Business Continuity Planning:** The primary objective of a business continuity planning is to enable an organisation to survive a disaster and to re-establish normal business operations. In order to survive, the organisation must assure that critical operations can resume normal processing within a reasonable time frame. The key objectives of the contingency plan should be to:
- (i) Provide for the safety and well-being of people on the premises at the time of disaster;
 - (ii) Continue critical business operations;
 - (iii) Minimise the duration of a serious disruption to operations and resources (both information processing and other resources);

- (iv) Minimise immediate damage and losses;
- (v) Establish management succession and emergency powers;
- (vi) Facilitate effective co-ordination of recovery tasks;
- (vii) Reduce the complexity of the recovery effort;
- (viii) Identify critical lines of business and supporting functions.

Therefore, the goals of the business continuity plan should be to:

- (i) Identify weaknesses and implement a disaster prevention program;
 - (ii) minimise the duration of a serious disruption to business operations;
 - (iii) facilitate effective co-ordination of recovery tasks; and
 - (iv) reduce the complexity of the recovery effort
- (c) Liability of Companies under Section 85 of Information Technology Act, 2000: Where a company commits any offence under this Act or any rule thereunder, every person who, at the time of the contravention, was in charge of and was responsible for the conduct of the business of the company shall be guilty of the contravention. However, he shall not be liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent the contravention.

Further, where a contravention has been committed by a company, and it is proved that the contravention took place with the connivance or consent of or due to any negligence on the part of any director, manager, secretary or other officer of the company, such officer shall be deemed to be guilty and shall be liable to be proceeded against and punished accordingly.

For the purposes of this section, 'company' includes a firm or other association of persons and 'director' in relation to a firm means a partner in the firm.

The Information Technology Act will go a long way in facilitating and regulating electronic commerce. It has provided a legal framework for smooth conduct of e-commerce. It has tackled the following legal issues associated with e-commerce:

- Requirement of writing
- Requirement of a document
- Requirement of a signature and
- Requirement of legal recognition for electronic messages,
- Records and documents to be admitted in evidence in a court of law.

Question 2

- (a) State and briefly explain the six stages of System Development Life Cycle (SDLC).

- (b) What is Decision Support System?. Briefly explain three characteristics of Decision Support System.
- (c) Explain Executive Information System(EIS). What purpose does it serve?

(10 + 5 + 5 = 20Marks)

Answer

- (a) System Development Life Cycle : The system development process is initiated when it is realized that a particular business process of the organization needs computerization or improvement. The system development life cycle is a set of six activities which are closely related. These activities after a certain stage can be done parallel to each other. For example the development can be started for some components (sub-systems) which are at the advance stage of designing. The systems development life cycle method consists of the following activities:

- (i) Preliminary investigation
- (ii) Requirements analysis or systems analysis
- (iii) Design of system
- (iv) Development of software
- (v) Systems testing
- (vi) Implementation and maintenance

The activities are briefly explained below:

- (i) Preliminary investigation: When the user comes across a problem in the existing system or a totally new requirement for computerization, a formal request has to be submitted for system development. It consists of three parts; request classification feasibility study and request approval. Generally the request submitted is not stated clearly hence requires detailed study. On receipt of request and identification of needs, the feasibility study is conducted which includes the aspects related to technical, economic and operational feasibility and is normally conducted by a third party depending upon the quantum and size of the requirements. The approval is sought from top management to initiate the system development.
- (ii) Requirements analysis or systems analysis: Once the request of the system development is approved, the detailed requirement study is conducted in close interaction with the concerned employees and managers to understand the detailed functioning, short-comings, bottlenecks and to determine the features to be included in the system catering to the needs and requirements of the users. This process is termed as "System Requirement Study (SRS) or System analysis.

- (iii) Design of the system: This activity evolves the methodology and steps to be included in the system to meet the identified needs and requirements of the system. The analyst designs the various procedures, report, inputs, files and database structures and prepares the comprehensive system design. These specifications are then passed on to the Development Team for program coding and testing.
 - (iv) Acquisition and development of software: Once the system design details are resolved and SRS is accepted by the user, the hardware and software details along with services requirements are determined and procured choosing the best-fit options. Subsequently, choices are made regarding which products to buy or lease from which vendors. The choice depends on many factors such as time, cost and availability of programmers. In case of in-house development, the analyst works closely with the programmers. The analyst also works with users to develop documentation for software and various procedure manuals.
 - (v) Systems testing: Once all the programs comprising the system have been developed and tested, the system needs to be tested as a whole. System testing is conducted with various probable options and conditions to ensure that it does not fail in any condition. The system is expected to run as per the specifications made in the SRS and users' expectations. Live test data are input for processing, and results are examined. If it is found satisfactory, it is eventually tested with actual data from the current system.
 - (vi) Implementation and maintenance: By the time of accomplishment of the above activities, it is ensured that the requisite hardware and software are installed and the users are trained on the new system to carry out operations independently. For sometime, hand-holding may be done by the system development team. The operations are monitored closely to ensure the users satisfaction. The system is maintained and modified to adapt to the changing needs of the users and business to ensure long-term acceptance of the system.
- (b) The Decision Support System(DSS) is considered as more flexible and adaptable to changing decision making requirements than traditional Management reporting system. This system emerged from the developments of interactive display technology, micro computing and easy-to-use software tools. It handles unstructured and partially structured problems giving rise to unpredictable and unstructured information needs.
- DSS can be defined as a system providing tools to the decision making managers to address unstructured/ partially structured problems in their own personalized manner. It empowers the managers in decision making process. A DSS does not require any high technology.

There are three characteristics of a Decision Support System namely:

- (i) Semistructured or unstructured decision-making.
- (ii) Adaptable to the changing needs of decision makers, and
- (iii) Ease of learning and use.

Each of these are briefly discussed below:

- (i) Semistructured and Unstructured Decisions: Unstructured decisions and semistructured decisions are made when information obtained from a computer system is only a portion of the total knowledge needed to make the decision. DSS is well adapted to help with semistructured and unstructured decisions. A well-designed DSS helps in decision making process with the depth to which the available data can be tapped for useful information.
 - (ii) Ability to adapt to changing needs: Semistructured and unstructured decisions often do not conform to a predefined set of decision-making rules. DSS provides flexibility to enable users to model their own information needs. Rather than locking the system into rigid information producing requirements, capabilities and tools are provided by DSS to enable users to meet their own output needs.
 - (iii) Ease of Learning and Use: DSS software tools employ user-oriented interfaces such as grids, graphics, non-procedural fourth – generation languages (4GL), natural English, and easily read documentation. These interfaces make it easier for users to conceptualize and perform the decision-making process.
- (c) An Executive Information System (EIS) is a tool that provides direct on-line access to relevant information in a useful and navigable format. The relevant information is timely, accurate, and actionable information about aspects of a business that are of particular interest to the senior manager. An EIS is easy to navigate so that managers can identify broad strategic issues, and then explore the information to find the root causes of those issues.

EIS serves the following purpose:

- (i) The primary purpose of an Executive Information System is to support managerial learning about an organization, its work processes, and its interaction with the external environment.
- (ii) A secondary purpose is to allow timely access to information so that based on the answers to questions, strategic decisions could be taken by a manager in time.
- (iii). It directs the attention of the management to specific areas of the organization or specific business problems. It makes managers and subordinates to work together to determine the root causes of issues highlighted by EIS

Question 3

- (a) What do you understand by classification of information? Explain different classifications of information.
- (b) Explain software testing and state its objectives.
- (c) Briefly explain the formal change management policies, and procedures to have control over system and program changes. (10 + 5 + 5 = 20 Marks)

Answer:

- (a) Information classification does not follow any predefined rules. It is a conscious decision to assign a certain sensitivity level to information that is being created, amended, updated, stored, or transmitted. The sensitivity level depends upon the nature of business in an organization and the market influence.

The classification of information further determines the level of control and security requirements. Classification of information is essential to understand and differentiate between the value of an asset and its sensitivity and confidentiality. When data is stored, whether received, created or amended, it should always be classified into an appropriate sensitivity level to ensure adequate security.

For many organizations, a very simple classification criteria is as follows:

Top Secret : The information is classified as Top Secret/ confidential that can cause serious damage to the organisation if lost or made public. Information relating to pending mergers or acquisitions; investment strategies; plans or designs etc. is highly sensitive. Many restrictions are imposed on the usage of such information and is protected at the highest level of security possible.

Highly Confidential : This class of information, is considered critical for the ongoing business operations and can cause serious impediment, if shared around the organization e.g. sensitive customer information of bank's, solicitors and accountants etc., patient's medical records and similar highly sensitive data. It should not be copied or removed without the consent of appropriate authority and must be kept under operational vigilance. Security at this level should be very high.

Proprietary: Information relating to Procedures, operational work routines, project plans, designs and specifications are of propriety in nature. Such information is for proprietary use to authorised personnel only. Security at this level is high.

Internal Use only : This class of information cannot be circulated outside the organisation where its loss would inconvenience the organisation or management but disclosure is unlikely to result in financial loss or serious damage to credibility. Internal memos, minutes of meetings, internal project reports are examples of such information. Security at this level is controlled but normal.

Public Documents: This Information is published in the public domain; annual reports, press statements etc.; which has been approved for public use. Security at this level is minimal.

- (b) Testing is a process used to identify the correctness, completeness and quality of developed computer software. In other words, testing is nothing but CRITICISM or COMPARISON, i.e. comparing the actual value with expected one.

One definition of testing is "the process of questioning a product in order to evaluate it", where the "questions" are things the tester tries to do with the product, and the product answers with its behaviour in reaction to the probing of the tester. The word testing means the dynamic analysis of the product—putting the product through its paces. Testing helps in verifying and validating if the software is working as it is intended to be working.

Objectives of Software Testing include:

- Testing is a process of executing a program with the intent of finding an error.
- A good test case is one that has a high probability of finding a yet undiscovered error.
- A successful test is one that uncovers a yet undiscovered error.

The data collected through testing can also provide an indication of the software's reliability and quality. However, testing cannot show the absence of defect, it can only show that software defects are present.

- (c) Formal change management control policies and procedure for system and program changes include the following:
- Periodically review all systems for needed changes.
 - Require all requests to be submitted in a standardized format.
 - Log and review requests from authorised users for changes and additions to systems.
 - Assess the impact of requested changes on system reliability objectives, policies and standards.
 - Categorize and rank all changes using established priorities.
 - Implement specific procedures to handle urgent matter, such as logging all emergency changes that required deviations from standard procedures and having management review and approve them after the fact. Make sure there is an audit trail for all urgent matters.
 - Communication of all changes to management and keep change requestors informed of the status of their requested changes.
 - Require IT management to review, monitor, and approve all changes to hardware, software, and personnel responsibilities.
 - Assign specific responsibilities to those involved in the change and monitor their work. Make sure that the specific assignments result in an adequate segregation of duties.

- Control system access rights to avoid unauthorised systems and data access.
- Make sure all changes go through the appropriate steps (development, testing, and implementation).
- Test all changes to hardware, infrastructure, and software extensively in a separate, non production environment before placing it into live production mode.
- Make sure there is a plan for backing out of any changes to mission-critical systems in the event that it does not work or does not operate properly.
- Implement a quality assurance function to ensure that all standards and procedures are followed and to assess if change activities achieve their stated objectives. These findings should be communicated to user departments, information systems management, and top management.
- Update all documentation and procedures when changes are implemented.

Question 4

- (a) What do you understand by Software Process Maturity? Discuss five levels of Software Process Maturity of Capability Maturity Model(CMM).
- (b) Discuss various types of Information Security polices and their hierarchy.
- (c) State and briefly explain the contents of a Standard Information System Audit Report.

(10 + 5 + 5 = 20 Marks)

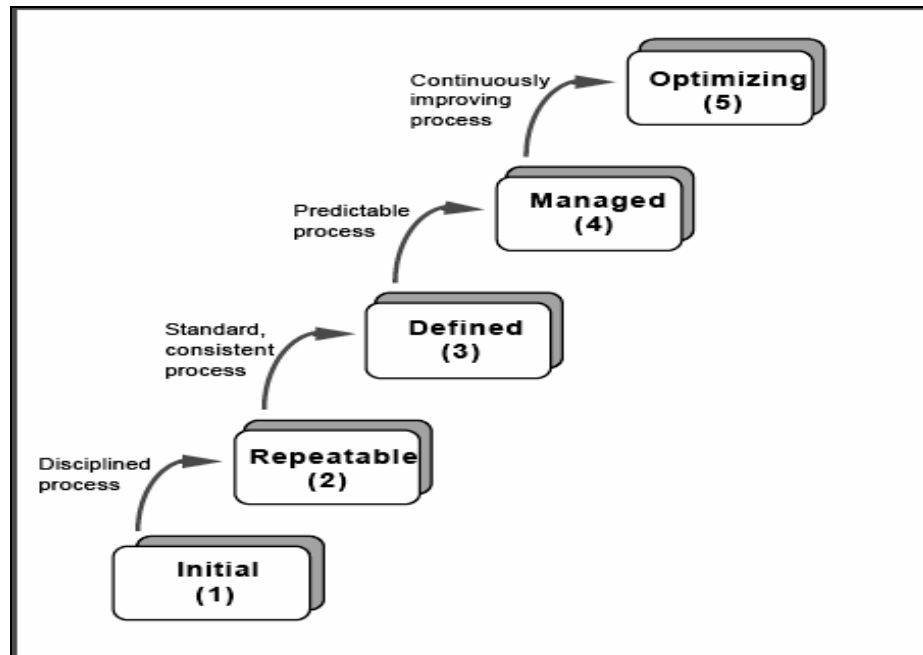
Answer

- (a) A software process is a set of activities, methods, practices, and transformations that are used to develop and maintain software and the associated products such as project plans, design documents, code, test cases, and user manuals.

Software process maturity 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 institutionalization in software process building takes place.

The Five Levels of Software Process Maturity

Continuous process improvement is based on many small, evolutionary steps rather than revolutionary innovations. The CMM provides a framework for organizing these evolutionary steps into five maturity levels that lay successive foundations for continuous process improvement. These five maturity levels are discussed below and shown in the figure:



- (i) Level 1 - The Initial Level: At the Initial Level, the organization typically does not provide a stable environment for developing and maintaining software. At this Level, capability is a characteristic of the individuals, not of the organization. During a crisis of software success depends entirely on having an exceptional manager and a seasoned and effective software team. But if someone leaves the project, it is difficult to handle the crises and a challenging task.
- (ii) Level 2 - The Repeatable Level: At this Level, policies for managing a software project and procedures to implement those policies are established. Planning and managing new projects is based on experience with similar projects. An effective process can be characterized as one which is practiced, documented, enforced, trained, measured, and able to improve. This Level makes the organizations to install basic software management controls. Software project standards are defined. The project's process is under the effective control of a project management system, following realistic plans based on the performance of previous projects.
- (iii) Level 3 - The Defined Level: At this Level, documentation for development and maintenance is prepared. This standard process is referred to throughout the CMM as the organization's standard software process, to help the software managers and technical staff perform more effectively. A group of experts standardize the process. An organization-wide training program is implemented to ensure that the staff and managers have the knowledge and skills required to fulfil

their assigned roles. This process capability is based on a common, organization-wide understanding of the activities, roles, and responsibilities in a defined software process.

- (iv) Level 4 - The Managed Level: At the Managed Level, the organization sets quantitative quality goals for both software products and processes. Productivity and quality are measured for important software process activities across all projects as part of an organizational measurement program. An organization-wide software process database is used to collect and analyze the data available from the projects' defined software processes.

This level of capability allows an organization to product trends in process and product quality within qualitative limits. Because of the stability and measured data when some exceptional circumstance occurs, the special cause of variation can be identified and addressed. The software products are of predictably high quality.

- (v) Level 5 - The Optimizing Level: The entire organization is focused on continuous process improvement. The organization has the means to identify weaknesses and strengthen the process proactively, with the goal of preventing the occurrence of defects. Data on the effectiveness of the software process is used to perform cost benefit analyses of new technologies and proposed changes to the organization's software process. In short, the cost of development is cut, best engineering practices are developed and used. Continuous improvement is done. Technology and process improvements are planned and managed as ordinary business activities.

- (b) Various types of information security policies are:

1. Information Security Policy - This policy provides a definition of Information Security, its overall objective and the importance that applies to all users.
2. User Security Policy – This policy sets out the responsibilities and requirements for all IT system users. It provides security terms of reference for Users, Line Managers and System Owners.
3. Acceptable Usage Policy – This sets out the policy for acceptable use of email and Internet services.
4. Organisational Information Security Policy – This policy sets out the Group policy for the security of its information assets and the Information Technology (IT) systems processing this information. Though it is positioned at the bottom of the hierarchy, it is the main IT security policy document.
5. Network & System Security Policy – This policy sets out detailed policy for system and network security and applies to IT department users

6. Information Classification Policy - This policy sets out the policy for the classification of information
7. Conditions of Connection – This policy sets out the Group policy for connecting to their network. It applies to all organizations connecting to the Group, and relates to the conditions that apply to different suppliers' systems.

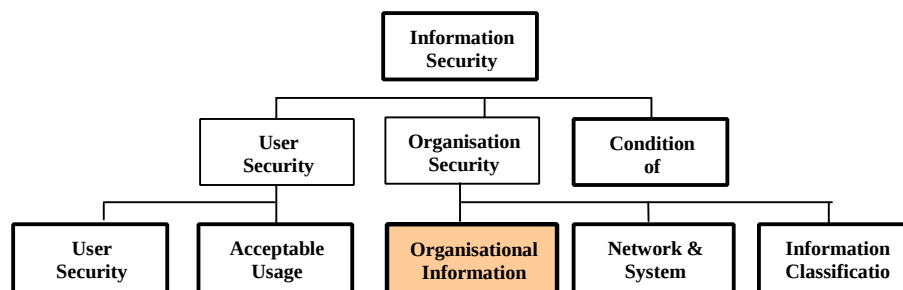


Fig. : The hierarchy of Information Security Policies.

- (c) According to the recommendations, IS Audit reports broadly include the following sections: title page, table of contents, summary including the recommendations, introduction, findings and appendices. These components of an audit report are discussed below:
- (i) Cover and Title Page: Audit reports should use a standard cover, with a window showing the title: "Information System Audit" or "Data Audit", the department's name and the report's date of issue (month and year). These items are repeated at the bottom of each page. The title page may also indicate the names of the audit team members.
 - (ii) Table of Contents : The table lists the sections and sub-sections with page numbers including summary and recommendations, introduction, findings (by audit field) and appendices (as required).
 - (iii) Summary / Executive Summary : The summary gives a quick overview of the salient features at the time of the audit in light of the main issues covered by the report. It should not normally exceed three pages, including the recommendations.
 - (iv) Introduction : Since readers will read the summary, the introduction should not repeat details. It should include the following elements:
 - Context: This sub-section briefly describes conditions in the audit entity during the period under review, for instance, the entity's role, size and organisation especially with regard to information system management, significant pressures on information system management during the period

under review, events that need to be noted, organisational changes, IT disruptions, changes in roles and programs, results of internal audits or follow-up to our previous audits, if applicable.

- Purpose: This sub-section is a short description of what functions and special programs were audited and the clients' authorities.
 - Scope: The scope lists the period under review, the issues covered in each function and program, the locations visited and the on-site dates.
 - Methodology: This section briefly describes sampling, data collection techniques and the basis for auditors' opinions. It also identifies any weaknesses in the methodology to allow the client and auditee to make informed decisions as a result of the report.
- (v) Findings: Findings constitute the main part of an audit report. They result from the examination of each audit issue in the context of established objectives.
- (vi) Opinion: If the audit assignment requires the auditor to express an audit opinion, the auditor shall do so in consonance to the requirement.
- (vii) Appendices: Appendices can be used when they are essential for understanding the report. They usually include comprehensive statistics, quotes from publications, documents, and references.

Question 5

- (a) Explain the following terms with reference to Information Systems:
- (i) Risk
 - (ii) Threat
 - (iii) Vulnerability
 - (iv) Exposure
 - (v) Attack
- (b) "There always exist some Common threats to the computerized environment." Explain these threats.
- (c) What do you understand by "Risk Assessment"? Discuss the various areas that are to be explored to determine the risk. (10 + 5 + 5 = 20 Marks)

Answer

- (a) (i) Risk: It is the likelihood that an organisation would face a vulnerability being exploited or a threat becoming harmful. Information systems can generate many direct and indirect risks. These risks lead to a gap between the need to protect systems and the degree of protection applied. Some of the factors that cause gaps

are widespread use of technology, Interconnectivity of systems and devolution of management and control etc.

- (ii) Threat: A threat is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organisation. Threat is any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data and denial of services
 - (iii) Vulnerability: It is the weakness in the system safeguards that exposes the system to threats. It may be weakness in an information system, cryptographic system, internal controls etc, that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system.
 - (iv) Exposure: It is the extent of loss the organisation has to face when a risk materialises. It is not just the immediate impact, but the real harm that occurs in the long run. For example, loss of business, failure to perform the system's mission, loss of reputation, violation of privacy, loss of resources.
 - (v) Attack is a set of actions designed to compromise confidentiality, integrity, availability or any other desired feature of an information system. It is an attempt to defeat IS safeguards. The type of attack and its degree of success will determine the consequence of the attack.
- (b) Any computerised environment is dependent on people. They are a critical links in making the entire enterprise computing happen and are responsible for the threats and attacks. The professionals such as analysts, programmers, data administrator, etc. are key links in ensuring that the IT infrastructure delivers to the user requirements and are target key persons who may leak the sensitive information of the enterprise. A few common threats to the computerised environment can be:
- (i) Power Loss: Power failure can cause disruption of entire computing equipments since computing equipments depends on power supply.
 - (ii) Communication failure: Failure of communication lines result in inability to transfer data which is a back bone of the system. Such failures present a significant threat that will have a direct impact on operations. For example, organisations which use communication lines for e-banking, railway reservation –e-ticketing etc., failure of communication link presents a significant threat.
 - (iii) Disgruntled Employees: Such employees presents a threat since, with access to sensitive information of the organisation, they 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 organisation network being compromised with virus attacks.

- (v) Malicious Code: Malicious code such as viruses and worms which freely access the unprotected networks may affect organisational and business networks that use these unprotected networks.
 - (vi) Abuse of access privileges by employees: The security policy of the company authorises employees based on their job responsibilities to access and execute select functions in critical applications.
 - (vii) Natural disasters: Natural disasters such as earthquakes, lighting, floods, tornado, tsunami, etc. can adversely affect the functioning of the IS operations due to damage to IS facilities.
 - (viii) Theft or destruction of computing resources: Since the computing equipment forms the back-bone of information processing, any theft or destruction of the resource can result in compromising the competitive advantage of the organisation.
 - (ix) Downtime due to technology failure: IS facilities may become unavailable due to technical glitches or equipment failure. The period of downtime the facility is not available may vary in criticality depending on the nature of business and the critical business process that the technology supports.
 - (x) Fire, etc.: Fire due to electric short circuit or due to riots, war or such other reasons can cause irreversible damage to the IS infrastructure.
- (c) Risk assessment is a critical step in disaster and business continuity planning. Risk assessment is necessary for developing a well tested contingency plan. 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. Risk assessment is a useful technique to assess the risks involved in the event of unavailability of information, to prioritise applications, identify exposures and develop recovery scenarios.

Various areas that are to be explored to determine the risk are briefly discussed below:

- (i) Prioritisation: All applications are inventoried and critical ones identified. Each of the critical applications is reviewed to assess its impact on the organisation, in case a disaster occurs. Subsequently, appropriate recovery plans are developed.
- (ii) Identifying critical applications: It is necessary to identify critical applications of the currently running applications. 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 organisation: Business continuity planning should not concentrate only on business disruption but should also take into account other organisational functions which may be affected. The areas to be considered include:
- Legal liabilities,
 - Interruptions of customer services.
 - Possible losses,
 - 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 organisation incurs severe losses. This critical time depends upon the nature of operations.
- (v) Assess Insurance coverage: The information system insurance policy should be a multi-peril policy, designed to provide various types of coverage. It may cover the cost of hardware, software reconstruction, business interruption etc.
- (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.

Question 6

- (a) What do you understand by the term Disaster? What procedural plan do you suggest for disaster recovery?
- (b) Describe the methodology of developing a Business Continuity Plan.
- (c) Briefly explain the various types of system's back-up for the system and data together.

(10 + 5 + 5 = 20 Marks)

Answer

- (a) The term disaster can be defined as an incident which jeopardizes business operations and/or human life. It could be due to sabotage (human) or natural. Following is the procedural plans for disaster recovery.

Disaster Recovery Procedural Plan: Normally disaster recovery procedural plan is made when the system is normally working. After visualizing the disaster the action to be taken by different people of the organization are to be documented. This recovery and planning document may include the following areas:

- (i) The conditions for activating the plans, which describe the process to be followed before each plan, are activated.

- (ii) Emergency procedures, which describe the actions to be taken following an incident which jeopardises business operations and/or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities e.g. police, fire, services and local government.
- (iii) Fallback procedures which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time-scale.
- (iv) Resumption procedures, which describe the actions to be taken to return to normal business operations.
- (v) A maintenance schedule, which specifies how and when the plan will be tested, and the process for maintaining the plan.
- (vi) Awareness and education activities, which are designed to create an understanding of the business continuity, process and ensure that the business continues to be effective.
- (vii) The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
- (viii) Contingency plan document distribution list.
- (ix) Detailed description of the purpose and scope of the plan.
- (x) Contingency plan testing and recovery procedure.
- (xi) List of vendors doing business with the organisation, their contact numbers and address for emergency purposes.
- (xii) Checklist for inventory taking and updating the contingency plan on a regular basis.
- (xiii) List of phone numbers of employees in the event of an emergency.
- (xiv) Emergency phone list for fire, police, hardware, software, suppliers, customers, back-up location, etc.
- (xv) Medical procedure to be followed in case of injury.
- (xvi) Back-up location contractual agreement, correspondences.
- (xvii) Insurance papers and claim forms.
- (xviii) Primary computer centre hardware, software, peripheral equipment and software configuration.

- (xix) Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
 - (xx) Alternate manual procedures to be followed such as preparation of invoices.
 - (xxi) Names of employees trained for emergency situation, first aid and life saving techniques.
 - (xxii) Details of airlines, hotels and transport arrangements.
- (b) The methodology for developing a business continuity plan can be sub-divided into eight different phases. The extent of applicability of each of the phases has to be tailored to the respective organisation. The methodology emphasises on the following:
- (i) Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
 - (ii) Obtaining commitment from appropriate management to support and participate in the effort;
 - (iii) Defining recovery requirements from the perspective of business functions;
 - (iv) Documenting the impact of an extended loss to operations and key business functions;
 - (v) Focusing appropriately on disaster prevention and impact minimisation, as well as orderly recovery;
 - (vi) Selecting business continuity teams that ensure the proper balance required for plan development;
 - (vii) Developing a business continuity plan that is understandable, easy to use and maintain; and
 - (viii) Defining how business continuity considerations must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.
- (c) Types of system's Back-ups: When the back-ups are taken of the system and data together, they are called total system's back-up. System back-up may be a full back-up, an incremental back-up or a differential back-up.
- (i) Full Backup: 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. This is the simplest form of backup with a single restoring session for restoring all backed-up files.
 - (ii) Differential Backup: It contains all the files that have changed since the last full backup. This is in contrast to incremental backup generation, which holds all the

files that were modified since the last full or incremental backup. It is faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

- (iii) Incremental Backup: Only the files that have changed since the last full backup / differential backup / or incremental backup are saved. 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, it is difficult to restore as you have to start with recovering the last full backup, and then recovering from every incremental backup taken since.
- (iv) Mirror back-up: It 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.

Question 7

Write short notes on the following:

- (a) Advantages of Application Packages
- (b) Key elements in System Development and Acquisition Control
- (c) Powers of Cyber Appellate Tribunal
- (d) Information System Maintenance. (4 × 5 = 20 Marks)

Answer

- (a) The four most compelling advantages of using pre-written application packages are:
 - (i) Rapid implementation: Application packages are readily available to implement after they are purchased. In contrast, software developed in-house may take months or even years until it is ready for implementation.
 - (ii) Low risk: Since the application package is available in the finished form, the organisation knows what it is going to get for the price it has paid. With in-house developed software, the long development time breeds uncertainty with regard to both the quality of the final product and its final cost.
 - (iii) Quality: The firms engaged in application package developments are typically specialist in their products' niche area. Generally, they have a lot of experience in their specialised application field and hence can provide better software. In contrast, in-house programs often have to work over a wide range of application areas; they may not be possessing expertise for undertaking proposed software development.
 - (iv) Cost: Software cost can be leveraged as copies are generated and sold. Application packages, sometimes, turn out to be cheaper compared to in-house developed software.

- (b) Key elements in System Development and Acquisition Control: It is important to have a formal, appropriate, and proven methodology to govern the development, acquisition, implementation, and maintenance of information systems and related technologies. Methodology should contain appropriate controls for management review and approval, user involvement, analysis, design, testing, implementation, and conversion.

Key elements in system Development and acquisition controls and given in following table:

Control Category	Threats/Risks	Controls
System development and acquisition controls	System development projects consume excessive resources.	Long-range strategic master plan, data processing schedules, assignment of each project to a manager and team, project development plan, project milestones, performance evaluations, system performance measurements.
Change management controls	Systems development projects consume excessive resources, unauthorised systems changes.	Change management control policies and procedures, periodic review of all systems for needed changes, standardized format for changes, log and review change requests, assess impact of changes on system reliability, categorise and rank all changes, procedures to handle urgent matters, communicate changes to management and users, management approval of changes, assign specific responsibilities while maintaining adequate segregation of duties etc.

- (c) Powers of Cyber Appellate Tribunal: Section 58 provides for the procedure and powers of the Cyber Appellate Tribunal. The Tribunal shall also have the powers of the Civil Court under the Code of Civil Procedure, 1908. Some of the powers specified are in respect of the following matters:
- (i) summoning and enforcing the attendance of any person and examining him on oath;
 - (ii) requiring the discovery and production of documents or other electronic records;
 - (iii) receiving evidence on affidavits;

- (iv) issuing commissions for the examination of witnesses or documents;
- (v) reviewing its decisions;
- (vi) dismissing an application for default or deciding it ex parte;
- (vii) any other matter which may be prescribed.

The appellant may either appear in person or may be represented by a legal practitioner to present his case before the Tribunal.

- (d) Information Systems Maintenance: Most information systems require at least some modification after development. The need for modification arises from a failure to anticipate all requirements during system design and/or from changing organisational requirements. Hence periodic system maintenance is required for most Information Systems. Systems maintenance involves adding new data elements, modifying reports, adding new reports, changing calculations, etc. Maintenance can be categorised in the following two ways:

1. Scheduled maintenance is anticipated and can be planned for. For example, the implementation of a new inventory coding scheme can be planned in advance.
2. Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate solution. A system that is properly developed and tested should have few occasions of rescue maintenance.

One problem that occurs in systems development and maintenance is that as more and more systems are developed, a greater portion of systems analyst and programmer time is spent on maintenance. An information system may remain in an operational and maintenance mode for several years. The system should be evaluated periodically to ensure that it is operating properly and is still workable for the organisation. When a system becomes obsolete i.e. new opportunities in terms of new technology are available or it no longer satisfies the organisation's needs, the information system may be replaced by a new one generated from a fresh system development process.