CA - FINAL
COURSE MATERIAL

Quality Education
beyond your imagination...

INFORMATION SYSTEMS
CONTROL AND AUDIT_17e

MASTER MINDS™

CA • CMA • CS • MEC • CEC

GUNTUR | RAJAHMUNDRY | KURNOOL | VIZAG | NELLORE

HYDERABAD | VIJAYAWADA | TIRUPATHI

Cell: 98851 25025 / 26

Visit us @ www.mastermindsindia.com | Mail: mastermindsinfo@ymail.com

Facebook Page: Masterminds For CA | YouTube Channel: Masterminds For CA

INDEX

INFORMATION SYSTEMS CONTROL AND AUDIT

0. INTRODUCTION

Q.No.1. What is software? Explain different types?

Computer software can be divided into two main categories: application software and system software.

a) Application software:

Application software consists of programs for performing specific task. Examples of application software include spreadsheets, database systems, desktop publishing systems and games.

b) Systems Software:

i) A Program or a set of program used for provides ease of use environment for the development and execution of other software is known System software.

ii) System software acts as an interface between the hardware of the computer and the application software that users need to run on the computer.

iii) Some examples of system software includes

- Assembler
- Compiler
- Macro
- Interpreter
- Debugger
- Operating system

Q.No.2. Explain Single User system and Multi User System?

1. Single User System:

a) A single-user operating system provides access to the computer system for a single user at a time. If another user needs access the Computer system, he must wait till the current user finishes what he is doing.

b) Ex: DOS, UNIX, and windows 95/98/me/..Etc

2. Multi-user operating system:

a) More than one user interacts with the system at a time. Access to the computer system is normally provided via a network, so that users access the computer remotely using a terminal or other computer.

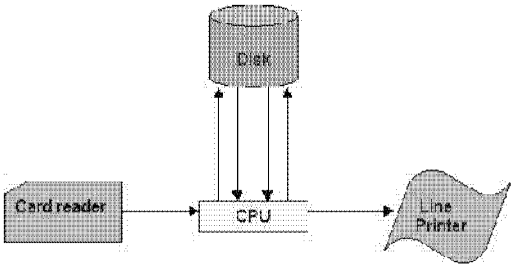
b) Examples of multi-user operating systems are UNIX, Linux etc.

Q.No.3. Explain SPOOLING?

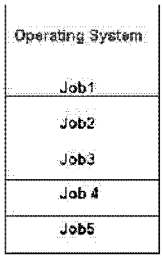
a) Spooling stands for Simultaneous Peripheral on – Line Operation)

b) Spooling is a technique used to increase the speed of data output, particularly printed output.

c) Printers are relatively slow devices, which could, if the CPU was in direct control, cause the processor to have to wait for each line/character to be printed.



Q.No.4 Explain Multiprogramming, Multitasking and Multithreading.



a) **Multi Programming:** Multiprogramming is a method of running several different programs in a computer apparently at the same time. It increases CPU utilization, Throughput is increased.

b) **Multi tasking:** More than one task is under execution state in a single user system.

c) **Multithreading:** More than one thread is under execution at a time in a single process is nothing but Multithreading.

Q.No.5 Explain Parallel System, Distributed System, Real Time System.

1. **Parallel Systems: (Tightly Coupled Systems)**

   a) Parallel systems have more than one processor in close communication, sharing the computer bus, the clock and sometimes memory and peripheral devices.

   b) The Ability to continue providing the service proportional to the level of surviving hardware called graceful degradation.

   c) Systems which are designed for graceful degradation are also called Fault-Tolerant.

2. **Distributed Systems: (Loosely Coupled Systems):** A Distributed system is a collection of processors that do not share the memory or a clock. Instead each processor has its own local memory and the processors communicate one another through the communication lines.

3. **Real Time Systems:**

   a) Real time system is a special purpose operating system. It is used when a rigid requirements on the operation of a processor or the flow of the data etc. this is often used in control device in a dedicated application.

   b) There are two flavors of Real – Time systems:

      i) Hard real-time:

      ii) Soft real-time

   c) Examples of Real time System:

      i) Scientific experiments

      ii) Medical imaging systems

      iii) Weapon systems

Q.No.6. Explain the main functions of activities of Operating System.

1. Performing hardware functions
2. User Interfaces
3. Hardware Independence.
4. Memory Management
5. Networking Capability:
6. File management
7. Logical access security
8. Deadlock Handling
9. Disk Management
10. Process Management

Q.No.2. Write about Cache memory and Virtual Memory?

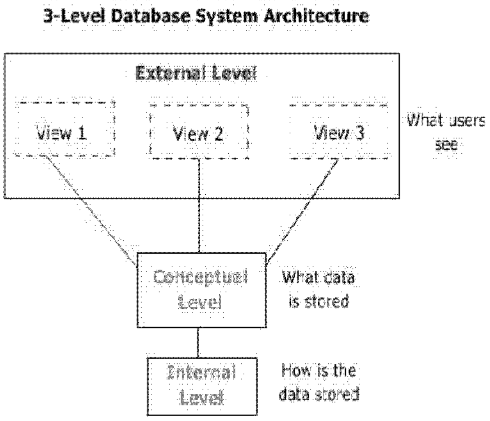
1. **Cache memory:**
   - **a)** There is a huge speed difference between Registers and Primary Memory.
   - **b)** Cache memory can be used in order to bridge the speed differences between Registers and Primary memory.
   - **c)** Cache is a smaller, faster memory, which stores copies of the data from the most frequently used main memory locations.
2. **Virtual memory:**
   - **a)** Sometimes computer lacks the Random Access Memory (RAM) needed to run a Program, in such a case usage of virtual memory to compensate.
   - **b)** Virtual memory is an allocation of hard disk space to help RAM.
   - **c)** Loading of such large size software into smaller size RAM is possible by the facility called Virtual Memory.

Q.No.7. Explain the terms: Metadata, Database, Database system, Data management and DBMS.

1. **Meta Data:** Metadata data is nothing but Data about the data or data that describes the data.
2. **Database:** Database is a collection of related information stored. Or A database is a collection of computerized data files.
3. **Database System:** A computerized record keeping system.
4. **Data Management:** Data management focuses on data collection, storage, and retrieval, thus constitutes a core activity for any organization.
5. **Database Management System [DBMS]:** A DBMS is a software system that allows access to data contained in a database. Data accessing includes insertion, deletion, updation and retrieval of data,

Q.No.8. Write about Three Schema Architecture?

1. A commonly used view of data approach is the three-level architecture suggested by ANSI/SPARC (American National Standards Institute/Standards Planning and Requirements Committee).
2. The main objective of three-schema architecture is to separate database from application programs.
   - **a)** Internal Level or Internal Schema or Physical Level.
   - **b)** Conceptual Level or Conceptual Schema or Logical Level or global level.
   - **c)** External Level or External Schema or View Level.



Q.No.9. Mention the Advantages of DBMS.

- **a)** Minimal Data Redundancy.
- **b)** Improved Data Consistency.
- **c)** Program-Data Independence.
- **d)** Improved Data Sharing.
- **e)** Data Integrity.

f) Improved Productivity of Application Development.

g) Enforcement of Standards.

h) Improved Data Accessibility.

i) Reduced Program Maintenance.

j) Data Security.

Q.No.10. What is meant by a computer network? Explain different Types?

Computer Networks:

A computer network is a collection of computers connected together by a communication system.

Media may be either guided media(wired) or unguided media(wireless).

CATEGORIES OF NETWORKS

a) **LAN (Local Area Network):** Computers that are connected in a limited distance. In a LAN can be as simple as two PC's and a printer in someone's home office, or it can extend throughout a company and include voice, sound, and video peripherals. Ex: - Within an office, within a building etc.,

b) **MAN (Metropolitan Area Network:** It is designed to extend over an entire city. it may be a single network such as a cable television network, or it may be a means of connecting a number of LANs into a larger network so that resources may be shared LAN-to-LAN as well as device-to-device.

c) **WAN (Wide Area Network:** Computers that are connected across a large distance. Several LAN's and MAN 's connected up form a WAN. WAN provides transmission of data, voice, image and video information over large geographical areas that may comprise a country, a continent, or even the whole world.

d) **INTERNET:** Networks of networks are nothing but internet.

Q.No.11. What is a Protocol? Explain its key elements?

Protocols: A protocol is a set of rules that govern data communication. A protocol defines what is communicated, how it is communicated, and when it is communicated

The key elements of a protocol are syntax, semantics, and timing.

a) **Syntax:** Refers to the structure or format of a data.

b) **Semantics:** Refers to the meaning of each section of bits.

c) **Timing:** Refers to two characteristics.

Q.No.12. What is Topology? Explain different types?

TOPOLOGY

a) The term topology refers to the way a network in laid out, either physically or logically. Two or more devices connect to a link; two or more links form a topology.

b) The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to each other.

c) There are five basic topologies:

i) Mesh.

ii) Star.

iii) Tree.

iv) Bus.

v) Ring

Q.No.13. Write about OSI and TCP/IP Models?

OSI Model: The Open System Interconnection (OSI) model is a layered framework for the design of network systems that allows for communication across all types of computer systems.The OSI model is built of seven ordered layers.

i) Physical (L1)

ii) Data link (L2)

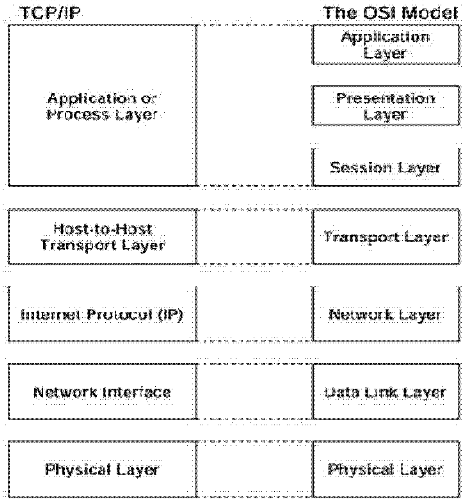
iii) Network (L3)

iv) Transport (L4)

v) Session (L5)

vi) Presentation (L6)

vii) Application (L7)



TCP/IP Model:

1. The protocol used on the Internet is called TCP/IP (Transmission Control Protocol/Internet Protocol) or internet protocol suite
2. TCP/IP consists of five levels or layers of protocols that can be related to the seven layers of the OSI architecture.
3. TCP/IP is used by the Internet and by all Intranets and extranets
4. Five levels of TCP/IP includes:

Q.No.14. Explan Networking and Internetworking connecting devices?

An Internet is an interconnection of individual networks. To create an Internet, we need internetworking devices called routers and gateways.

a) Modem: It is a device that converts a digital computer signal into an analog signal (i.e. it modulates the signal) and converts an analog signal into a digital computer signal (i.e. it demodulates the signal) in a data communication system.

b) Multiplexer: It is a device that allows a single communications channel to carry simultaneous data transmissions from many terminals.

c) Switch: It is a device, which makes connections between telecommunications circuits in a network so that a message can reach its intended destination.

d) Hub: It is a port-switching device, allows for the sharing of the network resources such as servers, LAN workstations, printers, etc.

e) Repeater: It is a device that boosts or amplifies the signal before passing it to the next section of cable in a network.

f) Bridge: It is a communication processor that connects numerous LANs. It magnifies the data transmission signal while passing data from one LAN to another.

g) Router: It is a communication processor that interconnects networks based on different rules or protocols, so that a message can be routed to its destination.

h) Gateway: Gateway is a communication processor that connects networks that use different communication architectures.

Q.No.15. Write about Network security?

NETWORK SECURITY: Network security consists of provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network accessible resources from unauthorized access.

NEED FOR SECURITY: The basic objective of providing network security is to

a) To safeguard assets

b) To ensure and maintain data integrity.

TYPES OF SECURITY:

a) Physical security

b) Logical security

Q.No.16. Explain Threat and Vulnerability?

1. **THREAT:** It is a possible danger that can disrupt the operation, functioning, integrity, or availability of a network or system.

    a) Unstructured threats

    b) Structured threats

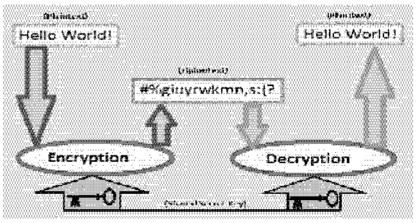
    c) External threats

    d) Internal threats

2. **VULNERABILITY:** Vulnerability is an inherent weakness in the design, configuration or implementation of a network or system that renders it susceptible to a threat. The following facts are responsible for occurrence of vulnerabilities in the software:

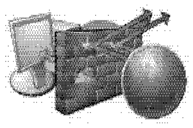
Q.No.17. Writer about Cryptiography and firewall?

Cryptography:



a) Cryptography is the practice and study of techniques for secure communication in the presence of third parties.

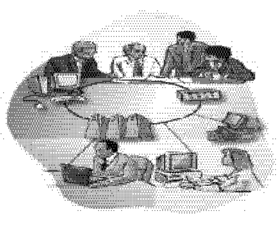
b) It a method of encoding(encryption) and decoding(decryption) of data.



Firewalls: It is a device that forms a barrier (fence) between a secure and an open environment. A firewall is a proved, effective means of protecting the firm's internal resources from unwanted intrusion.

Q.No.18. Write about Intranet and Extranet?

1. **Intranets**



a) An intranet is a network inside an organization that uses Internet technologies such as web browsers and servers, TCP/IP protocols, HTML, databases, and so on, to provide an Internet-like environment within the enterprise.

b) The main purpose is to provide information sharing, resource sharing, communications, collaboration, and the support of business processes.

2. Extranet:

a) Extranet is a private network that uses Internet protocol and public telecommunication systems to securely share part of a business's information or operations with suppliers, vendors, partners, customers or other businesses.

b) It is part of company's intranet that is extended to users outside the company.

c) Simply put, it is the Company's website for its customers and vendors.

THE END

1. CONCEPTS OF GOVERNANCE AND MANAGEMENT OF INFORMATION SYSTEMS

Q.No.1. Explain Governance and Enterprise Governance? (B)

Governance:

1. The term "Governance" is derived from the Greek verb meaning "to steer".
2. A governance system refers to all the means and mechanisms that will enable multiple stakeholders in an enterprise to have an organized mechanism for evaluating options, setting direction and monitoring compliance and performance, in order to satisfy specific enterprise objectives.
3. Governance refers to all processes of governing,
   a) Whether undertaken by a government, market or network,
   b) Whether over a family, tribe, formal or informal organization or territory
   c) Whether through laws, norms, power or language."
4. Governance is a general concept that can refer to all manner of organizations and can be used in different ways.

Enterprise Governance:

- The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization's resources are used responsibly.
- Enterprise governance is an overarching framework into which many tools and techniques and codes of best practice can fit.
- Examples include codes on corporate governance and financial reporting standards.

Q.No. 2. Write about Enterprise Governance Framework? (A) [PM]

Enterprise Governance has two dimensions.

1. **Corporate Governance or Conformance: [Explain the term corporate Governance]**

   (MTP N16- 6M, RTP M 17)

   a) Corporate Governance is defined as the system by which a company or enterprise is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance.
   b) In other words corporate governance refers to the structures and processes for the direction and control of companies.
   c) It concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders.
   d) The corporate governance provides a historic view and focuses on regulatory requirements.
   e) Good corporate governance contributes to sustainable economic development by enhancing the performance of companies and increasing their access to outside capital.
   f) Good corporate governance requires sound internal control practices such as
      i) Segregation of incompatible functions

- **ii)** Elimination of conflict of interest
- **iii)** Establishment of Audit Committee
- **iv)** Risk management and compliance with the relevant laws and standard.

2. **Business Governance or Performance:**

   - **a)** The **Business Governance** is pro-active in its approach.
   - **b)** It is business oriented and takes a forward looking view.
   - **c)** This dimension focuses on strategy and value creation with the objective of helping the board to make strategic decisions, understand its risk appetite and its key performance drivers.
   - **d)** This dimension does not lend itself easily to a regime of standards and assurance as this is specific to enterprise goals and varies based on the mechanism to achieve them.
   - **e)** *It is advisable to develop appropriate best practices, tools and techniques such as balanced scorecards and strategic enterprise systems that can be applied intelligently for different types of enterprises as required.*

Q.No.3. Explain Information Technology and Governance? What are the benefits of Governance? (OR) As an IT consultant, elaborate on the major benefits of Governance to the management of an enterprise. (A) [PM, RTP N16, M15]

- **a)** Information technology governance (ITG) is a part of the overall corporate governance.
- **b)** It mainly focuses on Information Technology systems, their performance, use and associated risks.
- **c)** The use of IT covering all key aspects of business processes of an enterprise impacts not only 'how information is processed' but also 'how computerized information systems are used for strategic and competitive advantage'.
- **d)** Effective IT governance helps ensure that IT supports business goals and appropriately manages IT related risk.

Benefits of Governance:

- **a)** Achieving enterprise objectives by ensuring that each element of the mission and strategy.
- **b)** Provides clearly understood and transparent decisions rights and accountability framework;
- **c)** Defining and encouraging desirable behavior in the use of IT and in the execution of IT outsourcing arrangements;
- **d)** Implementing and integrating the desired business processes into the enterprise;
- **e)** Providing stability and overcoming the limitations of organizational structure;
- **f)** Improving customer, business and internal relationships and satisfaction.
- **g)** Enabling effective and strategically aligned decision making.

Q.No.4. Write about relationship between Corporate Governance and IT Governance? (C)

- **a)** IT is a key enabler of corporate business strategy.
- **b)** **Chief Executive Officers (CEO), Chief Financial Officers (CFO)** and **Chief Information Officers (CIO)** agree that strategic alignment between IT and business objectives are a critical success factor for the achievement of business objectives.

c) IT has to provide critical inputs to meet the information needs of all the required stakeholders or it can be said that enterprise activities require information from IT activities in order to meet enterprise objectives.

d) Hence Corporate governance drives and sets IT governance.

e) "IT Governance is the system by which IT activities in a company or enterprise are directed and controlled to achieve business objectives with the ultimate objective of meeting stakeholder needs.

f) IT Governance is a sub-set of Corporate or Enterprise Governance.

Q.No.5. Write about IT Governance? Explain the Key practices to determine status of IT Governance. (A) [N16 – 4M]

a) The objective of IT Governance is to determine and cause the desired behavior and results to achieve the strategic impact of IT.

b) IT Governance refers to the system in which directors of the enterprise evaluate, direct and monitor IT management to ensure effectiveness, accountability and compliance of IT.

c) The active distribution of decision -making rights and accountabilities among different stakeholders in an organization and the rules and procedures for making and monitoring those decisions to determine and achieve desired behaviors and results.

Key practices:

Some of the Key Practices which determine the status of the IT Governance in the enterprise are:

a) Who makes directing, controlling and executing decisions?

b) How the decisions are made?

c) What information is required to make the decisions?

d) What decision-making mechanisms are required?

e) How exceptions are handled?

f) How the governance results are monitored and improved?

Q.No.6. Explain the key benefits of IT Governance. (OR) Describe the key benefits of IT Governance achieved at highest level in an organization. (A) [PM, N16 - 6M, N15 – 4M]

1. The benefits of IT governance depend by particular organizations environment. At the highest level IT governance provides the following benefits.

- **a)** Increased value delivered through enterprise IT
- **b)** Increased user satisfaction with IT services
- **c)** Improved agility in supporting business needs
- **d)** Better cost performance of IT
- **e)** Improved management and mitigation of IT-related business risk
- **f)** IT becoming an enabler for change.
- **g)** Improved transparency
- **h)** Improved compliance with relevant laws, regulations and policies
- **i)** More optimal utilization of IT resources.

2. For every defined benefit, it is critical to ensure that:

- **a)** Ownership is defined and agreed;
- **b)** It is relevant and links to the business strategy;

c) The timing of its realization of benefit is realistic and documented;

d) The risks, assumptions and dependencies associated with the realization of the benefits are understood, correct and current;

e) An unambiguous measure has been identified

f) Timely and accurate data for the measure is available or is easy to obtain.

Q.No.7. What do you understand by GEIT? Explain key benefits of Governance of Enterprise IT (GIET) (A) [PM, M17 - 4M, M16 - 4M, MTP16 - 4M, RTP N16]

Governance of Enterprise IT (GEIT)

a) **Governance of Enterprise IT** is a sub-set of corporate governance and facilitates implementation of a framework of IS controls within an enterprise as relevant and encompassing all key areas.

b) The primary objectives of GEIT are to analyze and articulate the requirements for the governance of enterprise IT.

c) GEIT provides effective Enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.

Benefits of GEIT:

a) Provides a consistent approach integrated and aligned with the enterprise governance approach.

b) Ensures that IT-related decisions are made in line with the enterprise's strategies and objectives.

c) Ensures that IT-related processes are overseen effectively and transparently.

d) Confirms compliance with legal and regulatory requirements.

e) Ensures that the governance requirements for board members are met.

Q.No.8. Discuss the Key Governance Practices of Enterprise IT (GIET). (B) [MTP16, 17 - 4M]

a) **Evaluate the Governance System:** Evaluate up to date on understanding of the requirements, and make judgment on the current and future design of governance of enterprise IT.

b) **Direct the Governance System:** Senior management involvement, leadership and support is critical. Develop IT setup which support enterprise governance. Define the information required for informed decision making;

c) **Monitor the Governance System:** Monitor the effectiveness and performance of the enterprise's governance of IT. Assess whether the governance system and implemented mechanisms are operating effectively.

Q.No.9. What do you understand by Corporate Governance? Explain the best practices of corporate governance. (A) [MTP16 - 4M]

a) The concept of Corporate Governance has succeeded in attracting a good deal of public interest because of its importance for the economic health of corporations, protect the interest of stakeholders including investors and the welfare of society.

b) Corporate Governance has been defined as the system by which business corporations are directed and controlled.

c) The corporate governance structure specifies the distribution of rights and responsibilities among different participants in the corporation and spells out the rules and procedures for making decisions on corporate affairs.

Some of the best practices of corporate governance:

a) Clear assignment of responsibilities and decision -making authorities, incorporating an hierarchy of required approvals from individuals to the board of directors;

b) Establishment of a mechanism for the interaction and cooperation a among the board of directors, senior management and the auditors;

c) Implementing strong internal control systems, including internal and external audit functions, risk management functions independent of business lines, and other checks and balances;

d) Special monitoring of risk exposures.

e) Financial and managerial incentives to act in an appropriate manner offered to senior management, business line management and employees in the form of compensation, promotion and other recognition

f) Appropriate information flows internally an d to the public.

g) For ensuring good corporate governance, the importance of overseeing the various aspects of the corporate functioning needs to be properly defined.

Q.No.10. Explain Enterprise Risk Management (ERM). (B)

a) ERM is an essential tool for good corporate governance.

b) Enterprises across the globe are facing different types of risk. Risk management is an increasingly important business drive and stake holders have become much more concerned about risk.

c) Overall risk management strategy has to be adapted, which should be designed and promoted by the top management and implemented at all levels of enterprise operations as required in an integrated manner.

d) Regulations require enterprises to adapt a risk management strategy, which is appropriate for the enterprise.

e) Committee of Sponsoring Organizations (COSO) definition of ERM is “Enterprise Risk Management is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

f) It is important for management to ensure that the enterprise risk management strategy considers implementation of information and its associated risks while formulating IT security and controls as relevant.

g) IT security and controls are sub -set of the overall enterprise risk management strategy and encompass all aspects of activities and operations of the enterprise.

Q.No.11. Write about Internal Controls over financial reporting as determined by US SEC ? (B)

a) **The US Security and Exchange Commission (SEC’s)** final rules define “Internal Control over financial reporting” to protect interests of investors.

b) It is process designed by, or under the supervision of, the company’s principal executive and principal financial officers, or persons performing similar functions, and effected by the company’s Board of Directors, Management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles(GAAP).

c) Under the final rules, a company’s annual report must include “An Internal Control report of management” that contains:

i) A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company;

ii) A statement identifying the framework used by management to conduct the required evaluation of the effectiveness of the company's internal control over financial reporting;

iii) Management's assessment of the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year.

iv) Management is not permitted to conclude that the company's internal control over financial reporting is effective if there are one or more material weaknesses in the company's internal control over financial reporting; and

v) A statement that the registered public accounting firm that audited the financial statements included in the annual report has issued an attestation report on management's assessment of the company's internal control over financial reporting."

Q.No.12. Explain the Responsibility for Implementing Internal controls? (C)

a) SOX made a major change in internal controls by holding Chief Executive Officers (CEOs) and Chief Financial Officers (CFOs) personally and criminally liable for the quality and effectiveness of their organization's internal controls.

b) Part of the process is to attest to the public that an organization's internal controls are effective. Internal controls can be expected to provide only a reasonable assurance, not an absolute assurance, to an entity's management and board.

c) An organization must ensure that its financial statements comply with **Financial Accounting Standards (FAS)** and **International Accounting Standards (IAS)** or local rules via policy enforcement and risk avoidance methodology called "Internal Control."

d) There must be a system of checks and balances of defined processes that lead directly from actions and transactions reporting to an organization's owners, investors, and public hosts.

Q.No.13 . Discuss the components of internal control as per COSO (Committee of Sponsoring Organization? (OR) Write short notes on internal controls as per Committee of Sponsoring Organization of trade way commission. (A) [RTP N15, RTP M17]

a) In a computerized environment, the goals of asset safeguarding, data integrity, system efficiency and system effectiveness can be achieved only if an organization's management sets up a system of internal controls.

b) According to COSO, Internal Control is comprised of five interrelate d components:

i) **Control Environment:** This includes the elements that establish the control context in which specific accounting systems and control procedures must operate. For each business process, an organization needs to develop and maintain a control environment including categorizing the criticality and materiality of each business process, plus the owners of the business process.

ii) **Risk Assessment:** This includes the elements that identify and analyze the risks faced by an organization and the way the risk can be managed. Each business process comes with various risks. A control environment must include an assessment of the risks associated with each business process.

iii) **Control Activities:** Control activities must be developed to manage, mitigate, and reduce the risks associated with each business process. It is unrealistic to expect to eliminate risks completely.

iv) **Information and Communication:** These are associated with control activities regarding information and communication systems of the entity. These enable an organization to capture and exchange the information needed to conduct, manage, and control its business processes.

v) **Monitoring:** The internal control process must be continuously monitored with modifications made as warranted by changing conditions.

Q.No. 14. Write about the Clause 49 of SEBI ? (C)

a) **Clause 49** of the listing agreements issued by SEBI in India is on similar lines of SOX regulation and mandates inter alia the implementation of enterprise risk management and internal controls and holds the senior management legally responsible for such implementation.

b) It also provides for certification of these aspects by the external auditors.

c) It may be noted that COSO and COBIT together have been internationally used as best practices framework for complying with SOX.

Q.No. 15. Explain the Role of IT in Enterprises? (A) [PM]

a) In an increasingly digitized world, enterprises are using IT not merely for data processing but more for strategic and competitive advantage too.

b) IT deployment has progressed from data processing to MIS to decision support systems to online transactions/services.

c) IT has not only automated the business processes but also transformed the way business processes are performed. The way in which business processes are performed/services rendered and how an organization is structured could be transformed through right deployment of IT.

d) It is needless to emphasize that IT is used to perform business processes, activities and tasks and it is important to ensure that IT deployment is oriented towards achievement of business objectives.

e) The extent of technology deployment also impacts the way internal controls are implemented in an enterprise.

f) it requires that senior management considers IT not only as an information processing tool but more from a strategic perspective to provide better and innovative services.

g) This makes it imperative to develop an IT strategy, which is aligned with business strategy and ensures value creation and facilitates benefit realization from the IT investments.

Q.No.16. Write about IT Steering Committee? Explain the key functions of IT Steering Committee in brief. (OR) You are appointed as a member of the IT Steering Committee for IT implementation and deployment in a large company. What are the major functions of this committee? (A) [PM, M17-6M, MTP15 - 4M]

IT Steering Committee

a) Planning is essential for determining and monitoring the direction and achievement of the enterprise goals and objectives.

b) As enterprises are dependent on the information generated by information systems, it is important that planning relating to information systems is undertaken by senior management or by the steering committee.

c) Depending on the size and needs of the enterprise, the senior management may appoint a high -level committee to provide appropriate direction to IT deployment and information systems and to ensure that the information technology deployment is in tune with the enterprise business goals and objectives called as the IT Steering Committee

d) It is ideally led by a member of the Board of Directors and comprises of functional heads from all key departments of the enterprise including the audit and IT department.

e) The role and responsibility of the IT Steering Committee and its members must be documented and approved by senior management.

f) As the members comprise of function heads of departments, they would be responsible for taking decisions relating to their departments as required.

g) The IT Steering Committee provides overall direction to deployment of IT and information systems in the enterprises.

Key functions of the committee:

a) To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives;

- **i)** To establish size and scope of IT function and sets priorities within the scope;
- **ii)** To review and approve major IT deployment projects in all their stages;
- **iii)** To approve and monitor key projects by measuring result of IT projects in terms of return on investment, etc.;
- **iv)** To review the status of IS plans and budgets and overall IT performance;
- **v)** To review and approve standards, policies and procedures;
- **vi)** To make decisions on all key aspects of IT deployment and implementation;
- **vii)** To facilitate implementation of IT security within enterprise;
- **viii)** To facilitate and resolve conflicts in deployment of IT and ensure availability of a viable communication system exists between IT and its users;
- **ix)** To report to the Board of Directors on IT activities on a regular basis.

Q.No.17. Discuss different levels of managerial activity that are carried out in an enterprise.(A) [PM, RTP M16]

a) Planning is basically deciding in advance 'what is to be done', 'who is going to do' and 'when it is going to be done'.

b) There are three levels of managerial activity in an enterprise :

- **i) Strategic Planning:** Strategic Planning is defined as the process of deciding on objectives of the enterprise, on changes in these objectives, on the resources used to attain these objectives, and on the policies that are to govern the acquisition, use, and disposition of these resources. Strategic planning is the process by which top management determines overall organizational purposes and objectives and how they are to be achieved. Corporate-level strategic planning is the process of determining the overall character and purpose of the organization, the business it will enter and leave, and how resources will be distributed among t hose businesses.
- **ii) Management Control:** Management Control is defined as the process by which managers assure that resources are obtained and used effectively and efficiently in the accomplishment of the enterprise's objectives.
- **iii) Operational Control:** Operational Control is defined as the process of assuring that specific tasks are carried out effectively and efficiently.

c) IT strategic plans provide direction to deployment of information systems and it is important that key functionaries in the enterprise are aware and are involved in its development and implementation.

d) Management should ensure that IT long and short-range plans are communicated to business process owners and other relevant parties across the enterprise.

e) Management should establish processes to capture and report feedback from business process owners and users regarding the quality and usefulness of long and short -range plans. The feedback obtained should be evaluated and considered in future IT planning.

Q.No.18. Explain Classification of Strategic planning? (B) [MTP15 - 4M]

a) In the context of Information Systems, **Strategic Planning** refers to the planning undertaken by top management towards meeting long -term objectives of the enterprise.

b) IT Strategy planning in an enterprise could be broadly classified into the following categories:

i) Enterprise Strategic Plan: Business Planning determines the overall plan of the enterprise. The enterprise strategic plan provides the overall charter under which all units in the enterprise, including the information systems function must operate. It is the primary plan prepared by top management of the enterprise that guides the long run development of the enterprise. It includes a statement of mission, a specification of strategic objectives, an assessment of environmental and organization factors that affect the attainment of these objectives, a statement of strategies for achieving the objectives.

ii) Information Systems Strategic Plan: The IS strategic plan in an enterprise has to focus on striking an optimum balance of IT opportunities and IT business requirements as well as ensuring its further accomplishment. This would require the enterprise to have a strategic planning process undertaken at regular intervals giving rise to long -term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals.

- Some of the enablers of the IS Strategic plan are:
  - Enterprise business strategy,
  - Definition of how IT supports the business objectives,
  - Inventory of technological solutions and current infrastructure,
  - Monitoring the technology markets,
  - Timely feasibility studies and reality checks,
  - Existing systems assessments,
  - Enterprise position on risk, time-to-market, quality, and
  - Need for senior management buy-in, support and critical review.

iii) Information Systems Requirements Plan: Every enterprise needs to have clearly defined information architecture with the objective of optimizing the organization of the information systems. This requires creation and continuous maintenance of a business information model and also ensuring that appropriate systems are defined to optimize the use of this information.

- Some of the key enablers of the information architecture are as follows:
  - Automated data repository and dictionary,
  - Data syntax rules,
  - Data ownership and criticality/security classification,
  - An information model representing the business, and
  - Enterprise information architectural standards.

iv) Information Systems Applications and Facilities Plan: On the basis of the information systems architecture and its associated priorities, the information systems management can develop an information systems applications and facilities plan. This plan includes:

- Specific application systems to be developed and an associated time schedule,
- Hardware and Software acquisition/development schedule,
- Facilities required, and
- Organization changes required.

Q.No.19. Discuss the key management practices, which are required for aligning IT strategy with enterprise strategy.(OR) What are the key management practices which are required for aligning IT strategy of BB with its Enterprise strategy. (A)
[PM, M16-5M, RTP M 15, M15 – 6M]

The key management practices, which are required for aligning IT strategy with enterprise strategy, are highlighted here:

a) **Understand enterprise direction:** Consider the current enterprise environment and business processes, as well as the enterprise strategy and future objectives. Consider also the external environment of the enterprise (industry drivers, relevant regulations, basis for competition).

b) **Assess the current environment, capabilities and performance:** Assess the performance of current internal business and IT capabilities and external IT services, and develop an understanding of the enterprise architecture in relation to IT. Identify issues currently being experienced and develop recommendations in areas that could benefit from improvement. Consider service provider differentiators and options and the financial impact and potential costs and benefits of using external services.

c) **Define the target IT capabilities:** Define the target business and IT capabilities and required IT services. This should be based on the understanding of the enterprise environment and requirements; the assessment of the current business process and IT environment and issues; and consideration of reference standards, best practices and validated emerging technologies or innovation proposals.

d) **Conduct a gap analysis:** Identify the gaps between the current an d target environments and consider the alignment of assets (the capabilities that support services) with business outcomes to optimize investment in and utilization of the internal and external asset base. Consider the critical success factors to support strategy execution.

e) **Define the strategic plan and road map:** Create a strategic plan that defines, in co - operation with relevant stakeholders, how IT- related goals will contribute to the enterprise's strategic goals. Include how IT will support IT -enabled investment programs, business processes, IT services and IT assets. IT should define the initiatives that will be required to close the gaps, the sourcing strategy, and the measurements to be used to monitor achievement of goals, then prioritize the initiatives and combine them in a high- level road map.

f) **Communicate the IT strategy and direction:** Create awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy, through communication to appropriate stakeholders and users throughout the enterprise.

Q.No.20. Write about the Business Value from Use of IT ? (OR) Discuss key management practices, which need to be implemented for evaluating ' Whether business value is derived from IT', in an organization. (B) [PM]

a) Business value from use of IT is achieved by ensuring optimization of the value contribution to the business from the business processes, IT services and IT assets resulting from IT -enabled investments at an acceptable cost.

b) *The benefit of implementing this process will ensure that enterprise is able to secure optimal value from IT-enabled initiatives services and assets, cost - efficient delivery of solutions and services, and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.*

c) The key management practices, which need to be implemented for evaluating ' Whether business value is derived from IT', are highlighted as under:

   i) **Evaluate Value Optimization:** Continually evaluate the portfolio of IT enabled investments, services and assets to determine the likelihood of achieving enterprise objectives and delivering value at a reasonable cost. Identify and make judgment on any changes in direction that need to be given to management to optimize value creation.

ii) **Direct Value Optimization:** Direct value management principles and practices to enable optimal value realization from IT enabled investments throughout their full economic life cycle.

iii) **Monitor Value Optimization:** Monitor the key goals and metrics to determine the extent to which the business is generating the expected value and benefits to the enterprise from IT-enabled investments and services. Identify significant issues and consider corrective actions.

Q.No.21. 'The success of the process of ensuring business value from use of IT can be measured by evaluating the benefits realized from IT enabled investments and services portfolio and how transparency of IT costs, benefits and risk is implemented'. Explain some of the key metrics, which can be used for such evaluation. (A) [PM, RTP N15]

a) Percentage of IT enabled investments where benefit realization monitored through full economic life cycle;

b) Percentage of IT services where expected benefits realized;

c) Percentage of IT enabled investments where claimed benefits met or exceeded;

d) Percentage of investment business cases with clearly defined and approved expected IT related costs and benefits;

e) Percentage of IT services with clearly defined and approved operational costs and expected benefits; and

f) Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of IT financial information.

Q.No. 22. Explain about Risk Management in the governance structure. (C)

a) Enterprise Risk Management and IT Risk Management are key components of an effective IT governance structure of any enterprise.

b) Effective IT governance helps to ensure close linkage to the enterprise risk management activities, including Enterprise Risk Management (ERM) and IT Risk Management.

c) IT governance has to be an integral part of overall corporate risk management efforts so that appropriate risk mitigation strategies are implemented based on the enterprise risk appetite.

d) The risk assessment approach adapted has to consider business impact of IS risk and different types of risks.

e) There has to be timely and regular communication of status of residual risks to key stakeholders so that appropriate action is taken to manage the IT risk profile.

Q.No.23. What do you understand by "Information System Risks"? Discuss broadly the characteristics of risk? (B) [RTP M17]

Information Systems Risks and Risk Management

a) Risk is the possibility of something adverse happening, resulting in potential loss/exposure. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk.

b) Risk management involves identifying, measuring, and minimizing uncertain events affecting resources.

c) Any Information system based on IT has its inherent risks. These risks cannot be eliminated but they can be mitigated by appropriate security.

d) This security has to be implemented as per required control system envisaged by the management of the enterprise.

e) Auditors are required to evaluate whether the available controls are adequate and appropriate to mitigate the risks.

f) If controls are unavailable or inadequate or inappropriate, then there would be a control weakness, which has to be reported to auditee management with appropriate recommendations to mitigate them.

g) The risks in IT environment are mitigated by providing appropriate and adequate IS Security.

h) IS security is defined as "procedures and practices to assure that computer facilities are available at all required times, that data is processed completely and efficiently and that access to data in computer systems is restricted to authorized people".

i) Some of the common sources of risk are :

- **i)** Commercial and Legal Relationships,
- **ii)** Economic Circumstances,
- **iii)** Human Behavior,
- **iv)** Natural Events,
- **v)** Political Circumstances,
- **vi)** Technology and Technical Issues,
- **vii)** Management Activities and controls, and
- **viii)** Individual Activities.

j) Broadly, risk has the following characteristics:

- **i)** Loss potential that exists as the result of threat/vulnerability process;
- **ii)** Uncertainty of loss expressed in terms of probability of such loss; and
- **iii)** The probability/likelihood that a threat agent mounting a specific attack against a particular system.

Q.No. 24. Explain terms: Assets, Vulnerability, Threat, Exposure, Likelihood: Attack. (A) [PM]

1. Asset:

a) Asset can be defined as something of value to the organization; e.g., information in electronic or physical form, software systems, employees.

b) Assets have one or more of the following characteristics:

- **i)** Recognized to be of value to the organization.
- **ii)** They are not easily replaceable without cost, skill, time, resources or a combination.
- **iii)** Data Classification of asset would normally be Proprietary, Highly confidential or even Top Secret.

2. Vulnerability:

a) Vulnerability is the weakness in the system safeguards that exposes the system to threats.

b) It may be a weakness in information system/s, cryptographic system (security systems), or other components that could be exploited by a threat. Vulnerabilities potentially “allow” a threat to harm or exploit the system.

c) For example, vulnerability could be a poor access control method allowing dishonest employees (the threat) to exploit the system to adjust their own records.

d) Some examples of vulnerabilities are:

i) Leaving the front door unlocked makes the house vulnerable to unwanted visitors.

ii) Short passwords (less than 6 characters) make the automated information system vulnerable to password cracking or guessing routines.

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

i) *'Allows an attacker to execute commands as another user' or*

ii) *'Allows an attacker to access data that is contrary to the specified access restrictions for that data' or*

iii) *'Allows an attacker to pose as another entity' or*

iv) *'Allows an attacker to conduct a denial of service'.*

3. **Threat:**

a) Any entity, circumstance, or event with the potential to harm the software system or component through its unauthorized access, destruction, modification, and/or denial of service is called a Threat.

b) 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 organization.

c) A threat cannot exist without a target asset. Threats are typically prevented by applying some sort of protection to assets.

4. **Exposure:**

a) An exposure is the extent of loss the enterprise has to face when a risk materializes. It is not just the immediate impact, but the real harm that occurs in the long run.

b) For example - loss of business, failure to perform the system's mission, loss of reputation, violation of privacy and loss of resources etc.

5. **Likelihood:**

a) Likelihood of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event.

b) The presence, tenacity and strengths of threats, as well as the effectiveness of safeguards must be considered while e assessing the likelihood of the threat occurring.

6. **Attack:**

a) An attack is an attempt to gain unauthorized access to the system's services or to compromise the system's dependability. In software terms, an attack is a malicious intentional fault, usually an external fault that has the intent of exploiting vulnerability in the targeted software or system.

b) Basically, it is a set of actions designed to compromise **CIA (Confidentiality, Integrity or Availability**), or any other desired feature of an information system.

Q.No.25. What do you understand by Risk and what are the common sources of Information systems risk? (B) [MTP15-4M]

Risk:

a) A Risk can be defined as the potential harm caused if a particular threat exploits a particular vulnerability to cause damage to an asset, and risk analysis is defined as the process of identifying security risks and determining their magnitude and impact on an organization.

b) Risk assessment includes :

i) Identification of threats and vulnerabilities in the system;

- **ii)** Potential impact or magnitude of harm that a loss of CIA, would have on enterprise operations or enterprise assets, should an identified vulnerability be exploited by a threat; and
- **iii)** The identification and analysis of security controls for the information system.

c) 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. The gap is caused by:

- **i)** Widespread use of technology;
- **ii)** Interconnectivity of systems;
- **iii)** Elimination of distance, time and space as constraints;
- **iv)** Unevenness of technological changes;
- **v)** Devolution of management and control;
- **vi)** Attractiveness of conducting unconventional electronic attacks against organizations;
- **vii)** External factors such as legislative, legal and regulatory requirements or technological developments.

d) It means there are new risk areas that could have a significant impact on critical business operations, such as:

- **i)** External dangers from hackers, leading to denial of service and virus attacks, extortion and leakage of corporate information;
- **ii)** Growing potential for misuse and abuse of information system affecting privacy and ethical values; and
- **iii)** Increasing requirements for availability and robustness.

Q.No.26. Explain Counter Measures and Residual Risk. (A) [PM]

Counter Measure: An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system is referred as Counter Measure. For example, well known threat 'spoofing the user identity', has two countermeasures:

a) Strong authentication protocols to validate users; and

b) Passwords should not be stored in configuration files instead some secure mechanism should be used.

Residual Risk:

a) Any risk remaining after the counter measures are analyzed and implemented is called residual risk.

b) An organization's management of risk should consider these two areas: acceptance of residual risk and selection of safeguards. Residual risk is a risk, that is kept even if risk management process is already applied.

c) Even when safeguards are applied, there is probably going to be some residual risk. The risk can be minimized, but it can seldom be eliminated.

d) Residual risk must be kept at a minimal, acceptable level. As long as it is kept at an acceptable level, (i.e. the likelihood of the event occurring or the severity of the consequence is sufficiently reduced) the risk can be managed.

Q.No.27. Explain the Risk management Strategies in detail? (A) [PM, MTP N16-6M, RTP M17]

a) When risks are identified and analyzed, it is not always appropriate to implement controls to counter them. Some risks may be minor, and it may not be cost effective to implement expensive control processes for them. Risk management strategy is explained and illustrated below:

b) **Tolerate/Accept the risk**. One of the primary functions of management is managing risk. Some risks may be considered minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.

   i) **Terminate/Eliminate the risk**. It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.

   ii) **Transfer/Share the risk**. Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risks associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organization. Risk also may be mitigated by transferring the cost of realized risk to an insurance provider.

   iii) **Treat/mitigate the risk**. Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects.

   iv) **Turn back**. Where the probability or impact of the risk is very low, then management may decide to ignore the risk.

Q.No. 28. Explain Key Governance Practices of Risk Management? (OR) Discuss the key governance practices for evaluating risk management. (A) [MTP16-4M, RTP N16, M15, M15-6M]

The key governance practices for evaluating risk management are given as follows:

a) **Evaluate Risk Management:** Continually examine and make judgment on the effect of risk on the current and future use of IT in the enterprise. Consider whether the enterprise's risk appetite is appropriate and that risks to enterprise value related to the use of IT are identified and managed;

b) **Direct Risk Management:** Direct the establishment of risk management practices to provide reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite; and

c) **Monitor Risk Management:** Monitor the key goals and metrics of the risk management processes and establish how deviations or problems will be identified, tracked and reported on for remediation.

Q.No.29. Describe key management practices for implementing risk management. (OR) The Management of IT related risks are a key part of Enterprise Governance. Name the key management practices to achieve this objective. (A) [PM]

Key Management Practices for implementing Risk Management are given as follows:

a) **Collect Data:** Identify and collect relevant data to enable effective IT related risk identification, analysis and reporting.

b) **Analyze Risk:** Develop useful information to support risk decisions that take into account the business relevance of risk factors.

c) **Maintain a Risk Profile:** Maintain an inventory of known risks and risk attributes, including expected frequency, potential impact, and responses, an d of related resources, capabilities, and current control activities.

d) **Articulate Risk:** Provide information on the current state of IT - related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.

e) **Define a Risk Management Action Portfolio:** Manage opportunities and reduce risk to an acceptable level as a portfolio.

f) **Respond to Risk:** Respond in a timely manner with effective measures to limit the magnitude of loss from IT related events.

Q.No.30. What are the Metrics of Risk Management? (B) [N15 - 4M]

Enterprises have to monitor the processes and practices of IT risk management by using specific metrics. Some of the key metrics are as follows:

a) Percentage of critical business processes, IT services and IT-enabled business programs covered by risk assessment;

b) Number of significant IT related incidents that were not identified in risk Assessment

c) Percentage of enterprise risk assessments including IT related risks; and

d) Frequency of updating the risk profile based on status of assessment of risks.

Q.No.31. Explain COBIT 5 Business Framework – Governance and Management of Enterprise IT. (B)

a) **Control Objectives for Information and Related Technology (COBIT)** is a set of best practices for Information Technology management developed by **Information Systems Audit & Control Association (ISACA)** and IT Governance Institute in 1996.

b) **COBIT 5** is the only business framework for the governance and management of enterprise Information Technology.

c) This evolutionary version incorporates the latest thinking in enterprise governance and management techniques, and provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems.

d) **As** per COBIT 5, Information is the currency of the 21st century enterprise. Information, and the technology that supports it, can drive success, but it also raises challenging governance and management issues.

e) It explains the need for using the approach and latest thinking provided by globally recognized framework COBIT 5 as a benchmark for reviewing and implementing governance and management of enterprise IT.

f) It explains the principles and enablers of COBIT 5 and how it can be as an effective tool to help enterprises to simplify complex issues, deliver trust and value, manage risk, reduce potential public embarrassment, protect intellectual property and maximize opportunities.

Q.No.32. Explain the need of Enterprises to Use COBIT 5? (B) [MTP15 - 6M]

a) Enterprises depend on good, reliable, repeatable data, on which they can base good business decisions. COBIT 5 provides good practices in governance and management to address these critical business issues.

b) COBIT 5 is a set of globally accepted principles, practices, analytical tools and models that can be customized for enterprises of all sizes, industries and geographies. It helps enterprises to create optimal value from their information and technology.

c) COBIT 5 provides the tools necessary to understand, utilize, implement and direct important IT related activities, and make more informed decisions through simplified navigation and use.

d) COBIT 5 is intended for enterprises of all types and sizes, including non - profit and public sector and is designed to de liver business benefits to enterprises, including:

- **i)** Increased value creation from use of IT;
- **ii)** User satisfaction with IT engagement and services;
- **iii)** Reduced IT related risks and compliance with laws, regulations and contractual requirements;

iv) Development of more business-focused IT solutions and services; and

v) Increased enterprise wide involvement in IT-related activities.

Q.No. 33. Discuss how COBIT 5 is Integrated with Other Frameworks? (B) [PM, MTP15-4M]

a) **COBIT 5** builds and expands on COBIT 4.1 by integrating other major frameworks, standards and resources, including ISACA's Val IT and Risk IT, Information Technology Infrastructure Library (ITIL®) and related standards from the International Organization for Standardization (ISO).

b) COBIT 5 is based on an enterprise view and is aligned with enterprise governance best practices enabling GEIT to be implemented as an integral part of wider enterprise governance.

c) COBIT5 also provides a basis to integrate effectively other frameworks, standards and practices used such as **Information Technology Infrastructure Library (ITIL)**, **The Open Group Architecture Framework (TOGAF)** and ISO 27001. It is also aligned with The GEIT standard ISO/IEC 38500:2008, which sets out high-level principles for the governance of IT, covering responsibility, strategy, acquisition, performance, compliance and human behavior that the governing body (e.g., board) should evaluate, direct and monitor. Thus , COBIT 5 acts as the single overarching framework, which serves as a consistent and integrated source of guidance in a non-technical, technology-agnostic common language.

d) The framework and resulting enablers should be aligned with and in harmony with (amongst others) the:

i) Enterprise policies, strategies, governance and business plans, and audit approaches ;

ii) Enterprise risk management framework; and

iii) Existing enterprise governance organization, structures and processes.

Q.No. 34. What are the components in COBIT? (B) [PM, RTP M15]

a) **Framework** - Organize IT governance objectives and good practices by IT domains and processes, and links them to business requirements ;

b) **Process Descriptions** - A reference process model and common language for everyone in an organization. The processes map to responsibility areas of plan, build, run and monitor.

c) **Control Objectives** - Provide a complete set of high-level requirements to be considered by management for effective control of each IT process.

d) **Management Guidelines** - Help assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes.

e) **Maturity Models** - Assess maturity and capability per process and helps to address gaps.

Q.No.35. State the Benefits of COBIT 5? (A) [PM, RTP M16]

COBIT 5 frameworks can be implemented in all sizes of enterprises.

a) A comprehensive framework such as COBIT 5 enables enterprises in achieving their objectives for the governance and management of enterprise IT.

b) The best practices of COBIT 5 help enterprises to create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use.

c) Further, COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT related interests of internal and external stakeholders.

d) COBIT 5 helps enterprises to manage IT related risk and ensures compliance, continuity, security and privacy.

e) COBIT 5 enables clear policy development and good practice for IT management including increased business user satisfaction.

f) The key advantage in using a generic framework such as COBIT 5 is that it is useful for enterprises of all sizes, whether commercial, not -for-profit or in the public sector.

g) COBIT 5 supports compliance with relevant laws, regulations, contractual agreements and policies.

Q.No. 36. Explain how to customizing COBIT 5 as per Requirement? (C)

COBIT 5 can be tailored to meet an enterprise's specific business model, technology environment, industry, location and corporate culture. Because of its open design, it can be applied to meet needs related to:

a) Information security,

b) Risk management,

c) Governance and management of enterprise IT,

d) Assurance activities,

e) Legislative and regulatory compliance , and

f) Financial processing or CSR reporting.

Enterprises can select required guidance and best practices from specific publications and processes of COBIT 5.

Q.No. 37. What are Five Principles of COBIT 5? (A) [MTP15-6M, PM, M15 – 4M]

The five key principles for governance and management of enterprise IT in COBIT 5 taken together enable the enterprise to build an effective governance and management framework that optimizes information and technology investment and use for the benefit of stakeholders.

a) **Principle 1: Meeting Stakeholder Needs:** Enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources. COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT. Enterprise can customize COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific; IT related goals and mapping these to specific processes and practices.

b) **Principle 2: Covering the Enterprise End -to-End:** COBIT 5 considers all IT related governance and management enablers to be enterprise-wide and end-to-end, i.e., inclusive of everything and everyone - internal and external that is relevant to governance and management of enterprise information and related IT.

c) **Principle 3: Applying a Single Integrated Framework:** There are many IT related standards and best practices, each providing guidance on a subset of IT activities. COBIT 5 is a single and integrated framework as it aligns with other latest relevant standards and frameworks, thus allows the enterprise to use C OBIT 5 as the overarching governance and management framework integrator.

d) **Principle 4: Enabling a Holistic Approach:** Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components. COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise.

e) **Principle 5: Separating Governance from Management:** The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organizational structures and serve different purposes.

Q.No. 38. Explain COBIT 5 Process Reference Model? (C)

a) COBIT 5 includes a Process Reference Model, which defines and describes in detail a number of governance and management processes of enterprise IT.

b) **Governance:** It ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

c) **Management:** It contains four domains, in line with the responsibility areas of **Plan, Build, Run and Monitor (PBRM)**, providing the end-to-end coverage of IT in alignment with the direction set by the governance body to achieve the enterprise objectives.

d) The COBIT 5 process reference model is the successor of the COBIT 4.1 process model, incorporating the both the Risk IT and Val IT frameworks.

e) The complete COBIT 5 enabler model includes a total of 37 governance and management processes .

i) **Governance Processes**

- Evaluate, Direct and Monitor Practices (EDM) - 5 processes (EDM01 to EDM05)

ii) **Management Processes**

- Align, Plan and Organize (APO) - 13 processes (APO01 to APO13)
- Build, Acquire and Implement (BAI) - 10 processes (BAI01 to BAI10)
- Deliver, Service and Support (DSS) - 6 processes (DSS01 to DSS06)
- Monitor, Evaluate and Assess (MEA) - 3 processes (MEA01 to MEA03)

Q.No.39. The COBIT 5 describes seven categories of enablers. Discuss them in brief. (OR) Discuss seven enables of COBIT 5? (OR) What are the enablers described by COBIT 5 Framework? (A) [PM, RTP N15, N16, MTP16, M17-6M, N16-5M]

a) Enablers are factors that, individually and collectively, influence whether something will work; in this case, governance and management over enterprise IT.

b) Enablers are driven by the goals cascade, i.e., higher-level IT related goals defining 'what the different enablers should achieve'.

c) The COBIT 5 framework describes seven categories of enablers are :

i) **Principles, Policies and Frameworks** are the vehicle to translate the desired behavior into practical guidance for day-to-day management.

ii) **Processes** describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT -related goals.

iii) **Organizational structures** are the key decision-making entities in an enterprise.

iv) **Culture, Ethics and Behavior** of individuals and of the enterprise is very often underestimated as a success factor in governance and management activities.

v) **Information is** pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.

vi) **Services, Infrastructure and Applications** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.

vii) **People, Skills and Competencies** are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

Q.No.40. Explain the Risk Management in COBIT 5 ? (B)

a) The COBIT framework provides excellent guidance on risk management strategy and practices from governance and management practice.

b) The Governance domain contains five governance processes, one of which focuses on stakeholder risk-related objectives: "**EDM03: Ensure risk optimization**".

c) This process ensures that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of IT is identified and managed.

d) This process provides guidance on how to ensure that IT -related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.

e) COBIT framework has management domain of "Align, Plan and Organize", which contains a risk-related process: "**APO12: Manage risk**".

f) This process requires continually identifying, assessing and reducing IT-related risk within levels of tolerance set by enterprise executive management.

g) The primary purpose of this process is to integrate the management of IT - related enterprise risk with overall ERM, and balance the costs and benefits of managing IT - related enterprise risk.

h) All enterprise activities have associated risk exposures resulting from environmental threats that exploit enabler vulnerabilities.

Q.No. 41. List out the basic requirements for implementation of GRC program and also state the goals and metrics, which are used in measuring success of GRC program. (B)

1. GRC program implementation requires the following:

a) Defining clearly what GRC requirements are applicable;

b) Identifying the regulatory and compliance landscape ;

c) Reviewing the current GRC status;

d) Determining the most optimal approach;

e) Setting out key parameters on which success will be measured ;

f) Using a process oriented approach;

g) Adapting global best practices as applicable; and

h) Using uniform and structured approach which is auditable.

2. Success of a GRC program can be measured by using the following goals and metrics:

a) The reduction of redundant controls and related time to execute (audit, test and remediate);

b) The reduction in control failures in all key areas;

c) The reduction of expenditure relating to legal, regulatory and review area s;

d) Reduction in overall time required for audit for key business areas;

e) Improvement through streamlining of processes and reduction in time through automation of control and compliance measures;

f) Improvement in timely reporting of regular compliance issues and remediation measures;

g) Dashboard of overall compliance status and key issues to senior management on a real - time basis as required.

Q.No. 42. Write about IT COMPLIANCE REVIEW ? (B)

a) Effective implementation of ERM requires consideration of multiple factors such as using a holistic approach , which encompasses enterprise from end-to-end, top down approach, best practices framework, technology deployment, related regulatory requirements and business needs.

b) As IT is a key enabler for most enterprises, it makes good economic sense to implement IT GRC as a sub -set of overall GRC under the regulatory umbrella of corporate governance.

c) In the US, Sarbanes Oxley Act has been passed to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.

d) In India, Clause 49 of listing agreement issued by **Security and Exchange Board of India (SEBI)** mandates similar implementation of enterprise risk management and internal controls as appropriate for the enterprise.

e) All listed Companies in India have to enter into an agreement with the Stock Exchange and this agreement is called the Listing Agreement. This agreement is more or less defined by SEBI and all Stock Exchanges have similar wordings.

f) Apart from other clauses in the agreement some of the clauses in the listing agreement require additional disclosures from the listed companies and compliance with corporate governance and other requirements.

g) One such clause is Clause 49 of the Listing Agreement that prescribes certain addition disclosure requirements and also corporate governance requirements. This requirement is similar to the requirement of the Sarbanes Oxley Act of the USA and there are similar legislations in Australia, Japan and other countries.

h) In USA, the Public Company Accounting Oversight Board (PCAOB) has come out with detailed guidelines on Compliance by Auditors and Companies under the Act. In India, no such guidance is available for Companies and Auditors other than limited guidance from the ICAI to its members , which focuses primarily on audit requirements.

i) The Internal control requirements of Clause 49 are similar to SOX requirements. For example: Under section F.i.6, the agreement requires the Directors to cover their internal controls systems and their adequacy in the Management Analysis and Discussion.

Q.No.43. Write about Compliance in COBIT 5? (B)

a) The Management domain of "**Monitor, Evaluate and Assess (MEA)**" contains a compliance focused process: "**MEA03 Monitor, Evaluate and Assess Compliance with External Requirements**".

b) This process is designed to evaluate that IT processes and IT supported business processes are compliant with laws, regulations and contractual requirements.

c) This require that the enterprise has processes in place to obtain assurance and that these requirements have been identified and complied with, and integrate IT compliance with overall enterprise compliance.

d) The primary purpose of this process is to ensure that the enterprise is compliant with all applicable external requirements.

e) Legal and regulatory compliance is a key part of the effective governance of an enterprise, hence its inclusion in the GRC term and in the COBIT 5 Enterprise Goals and supporting enabler process structure (MEA03).

f) The COBIT 5 framework includes the necessary guidance to support enterprise GRC objectives and supporting activities.

g) The Governance activities related to GEIT are covered in the five processes of the Governance domain.

h) The Risk management process and supporting guidance for risk management across the GEIT space meet the compliance nee d of regulations such as SOX and other similar regulations across the world.

i) COBIT has a specific focus on compliance activities within the framework and explains how they fit within the complete enterprise picture.

Q.No.44. Explain the Key Management Practices of IT Compliance? (A) [PM, N16, 15 - 4M]

COBIT 5 provides key management practices for ensuring compliance with external compliances as relevant to the enterprise. The practices are given as follows:

a) Identify External Compliance Requirements: On a continuous basis, identify and monitor for changes in local and international laws, regulations, and other external requirements that must be complied with from an IT perspective.

b) Optimize Response to External Requirements: Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated.

c) Confirm External Compliance: Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual l requirements

d) Obtain Assurance of External Compliance: Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.

Q.No. 45. Write about Key Metrics for Assessing Compliance Process? (B)

1. **Compliance with External Laws and Regulations:** :
   - **a)** Cost of IT non-compliance, including settlements and fines ;
   - **b)** Number of IT related non-compliance issues reported to the board or causing public comment or embarrassment;
   - **c)** Number of non-compliance issues relating to contractual agreements with IT service providers;
   - **d)** Coverage of compliance assessments.
2. **IT Compliance with Internal Policies:**:
   - **a)** Number of incidents relatsed to non compliance to policy.
   - **b)** Percentage of stakeholders who understand policies;
   - **c)** Percentage of policies supported by effective standards and working practices ;
   - **d)** Frequency of policies review and updates.

Q.No. 46. Write about Information System Assurance? (C)

a) Information systems are extensively used for managing business functions.

b) Management ensures effective use of information and technology investments and related IT for not only supporting enterprise goals but also to maintain compliance.

c) This dynamic changing environment provides a challenge for Chartered Accountants to provide assurance with the required level of confidence.

d) However, with the right type of skills and toolsets, this provides an excellent opportunity for Chartered Accountants to act as consultants, who provide relevant IT enabled services.

e) A key component of this knowledge base is usage of globally accepted good practices and frameworks and developing a holistic approach, which meets the needs of stakeholders.

Using COBIT 5 for Information System Assurance

a) COBIT 5 has been engineered to meet expectations of multiple stakeholders.

b) It is designed to deliver benefits to both an enterprise's internal stakeholders, such as the board, manage ment, employees, etc. as well as external stakeholders - customers, business partners, external auditors, shareholders, consultants, regulators, etc.

c) It is written in a non -technical language. It is usable for all people for understanding and addressing IT related issues as relevant to them.

d) Globally from the GRC perspective, COBIT has been widely used with COSO by management, IT professionals, regulators and auditors (internal/external) for implementing or evaluating Governance and management practices from an end-to-end perspective.

e) COBIT has been used as an umbrella framework under which other standards and approaches, such as ITIL, ISO 27001 etc. have been integrated into overall enterprise governance.

Q.No. 47. How to Evaluate IT Governance Structure and Practices by Internal Auditors? (OR) Discuss the activities performed by an internal auditor as suggested by the Institute of Internal Auditors (IIA). (A) [RTP M16, MTP17 - 6M]

1. IT Governance can be evaluated by both external as well internal auditors.

2. The following guidance is from internal audit perspective as issued by **The Institute of Internal Auditors (IIA).**

3. It defines specific areas and critical aspects relating to governance structure and practices, which can be reviewed as part of internal audit.

4. Internal audit activities in evaluating the IT governance structure and practices within an enterprise can evaluate several key components that lead to effective IT governance.

5. These are briefly explained here.

  a) Leadership: Auditor can verify the involvement of IT leadership in the development and on-going execution of the organization's strategic goals. He can also determine how IT will be measured in helping the organization achieve these goals. Auditor also Review the role of senior management and the board in helping establish and maintain strong IT governance

  b) Organizational Structure: It determines the roles and reporting relationships to allow IT to meet the needs of the organization. Auditor can review how organization management and IT personnel are interacting and communicating current and future needs across the organization.

  c) Processes: auditor can evaluate IT process activities and the controls in place to mitigate risks to the organization and whether they provide the necessary assurance regarding processes and systems.

d) **Risks:** Auditor can review the processes used by the IT organization to identify, assess, and monitor/mitigate risks within the IT environment.

e) **Controls:** Auditor can assess key controls that are defined by IT to manage its activities and the support of the overall organization. Ownership, documentation, and reporting of self - validation aspects should be reviewed by the internal audit activity.

f) **Performance Measurement/Monitoring:** Evaluate the framework and systems in place to measure and monitor organizational outcomes where support from IT plays an important part in the internal outputs in IT operations and developments.

Q.No.48. Discuss the areas, which should be reviewed by internal auditors as a part of the review of Governance, Risk and Compliance. (A) [PM]

Sample Areas of GRC for Review by Internal Auditors: Institute of Internal Auditor (IIA) provides areas, which can be reviewed by internal auditors as part of review of Governance, Risk and Compliance (GRC) areas.

a) **Scope:** The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes (GRC) using a systematic and disciplined approach.

b) **Governance:** The internal audit activity must assess and make appropriate recommendations for improving the governance process by accomplishment of the following objectives:

i) Promoting appropriate ethics and values within the organization;

ii) Ensuring effective organizational performance management and accountability;

iii) Communicating risk and control information to appropriate areas of the organization;

iv) Coordinating the activities of and communicating information among the board, external and internal auditors, and management.

c) **Evaluate Enterprise Ethics:** The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics related objectives, programs, and activities.

d) **Risk Management:** The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

e) **Interpretation:** Determining whether risk management processes are effective in a judgment resulting from the internal auditor's assessment that:

i) Organizational objectives support and align with the organization's mission;

ii) Significant risks are identified and assessed;

iii) Appropriate risk responses are selected that align risks with the organization's risk appetite; and

iv) Relevant risk information is captured and communicated in a timely manner.

f) **Risk Management Process:** The internal audit activity may gather the information to support this assessment during multiple engagements. Risk management processes are monitored through on-going management activities, separate evaluations, or both.

g) **Evaluate Risk Exposures:** The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems.

h) **Evaluate Fraud and Fraud Risk:** The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.

i) **Address Adequacy of Risk Management Process:** During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks.

Q.No. 49. Explain the Sample Areas of Review of Assessing and Managing risks. (B)

a) This review covers the Controls over the IT process of assessing and managing risks and is expected to provide assurance to the management that the enterprise has identified all the risks relevant to the enterprise/business as relevant to IT Implementation.

b) It considers IT risk -identification and impact analysis, involving multi -disciplinary functions and taking cost-effective measures to mitigate risks.

c) The specific areas can be evaluated for accessing and managing risk are:

i) Risk management ownership and accountability;

ii) Different kinds of IT risks (technology, security, continuity, regulatory, etc.);

iii) Defined and communicated risk tolerance profile ;

iv) Root cause analyses and risk mitigation measures;

v) Quantitative and/or qualitative risk measurement;

vi) Risk assessment methodology; and

vii) Risk action plan and Timely reassessment.

Q.No. 50. Explain how to evaluate and assess the System of Internal controls. (B) [M17]

a) COBIT 5 has specific process: "**MEA 02 Monitor, Evaluate and Assess the System of Internal Control**", which provides guidance on evaluating and assessing internal controls implemented in an enterprise.

b) The objective of such a review is to:

i) Continuously monitor and evaluate the control environment, including self -assessments and independent assurance reviews;

ii) Enable management to identify management deficiencies and inefficiencies and t o initiate improvement actions.

iii) Plan, organize and maintain standards for internal control assessment and assurance activities.

Q.No.51.Discuss the key management practices for assessing and evaluating the system of internal controls in an enterprise in detail. (OR) You are appointed by a leading enterprise to assess and to evaluate its system of IT internal controls. What are the key management practices to be followed to carry out the assignment complying with COBIT5. (OR) under COBIT 5, discuss various key management practices for accessing and evaluating the system on internal controls in an enterprise. (A) [PM, M17-6M, MTP15-6M]

The key management practices for assessing and evaluating the system of internal controls in an enterprise are given as follows:

a) Monitor Internal Controls: Continuously monitor, benchmark and improve the IT control environment and control framework to meet organizational objectives.

b) Review Business Process Controls Effectiveness: Review the operation of controls, including a review of monitoring and test evidence to ensure that controls within business processes operate effectively.

c) Perform Control Self-assessments: Encourage management and process owners to take positive ownership of control improvement through a continuing program of self - assessment to evaluate the completeness and effectiveness of management's control over processes, policies and contracts.

d) **Identify and Report Control Deficiencies:** Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.

e) **Ensure that assurance providers are independent and qualified:** Ensure that the entities performing assurance are independent from the function, groups or organizations in scope. The entities performing assurance should demonstrate an appropriate attitude and appearance, competence in the skills and knowledge necessary to perform assurance, and adherence to codes of ethics and professional standards .

f) **Plan Assurance Initiatives:** Plan assurance initiatives based on enterprise objectives and conformance objectives, assurance objectives and strategic priorities, inherent risk resource constraints, and sufficient knowledge of the enterprise.

g) **Scope assurance initiatives:** Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.

h) **Execute assurance initiatives:** Execute the planned assurance initiative. It also includes Report on identified finding, provides recommendations for improvement of assurance initiatives.

THE END

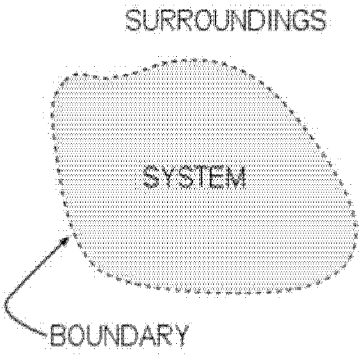
2. INFORMATION SYSTEM CONCEPTS

Q.No.1. Define a System, Give some examples of systems. [B]

a) A system is a group of interconnected components working together to accomplish common goal by accepting inputs and producing outputs in an ordered transformation process.

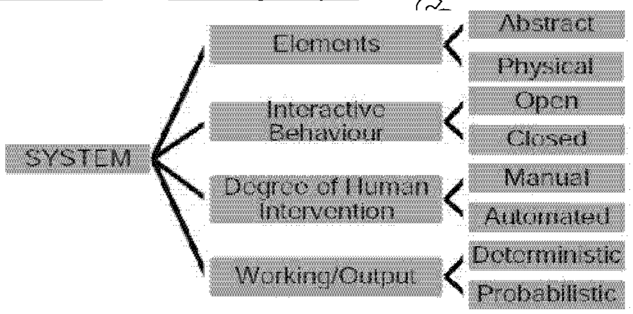
b) *Input is the data entering the system. Processing is the manipulation of the input data. Output is the information given by the system after processing and storage refers to the storage of data for current or future use.*

c) For example, a business is said to be system because it contains input e.g. people, machine, money, materials etc., which are processed by means of different processes such as production, marketing, finance etc. and produces output i.e. services and goods.



Q.No.2. Write about the classification of systems? [A] (PM)

1. Systems can be classified on the basis of various parameters like elements, interactive behavior, degree of human intervention and working output.



Classification of System

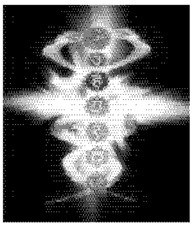
2. **On the basis of Elements**: Systems may be categorized as **Abstract or Physical** on the basis of the elements used in the system. **(RTP M15)**

   a) Abstract System:

   i) Abstract System is also known as Conceptual System.

   ii) It is defined as an orderly arrangement of interdependent ideas or constructs or concepts.

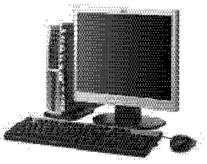
   iii) For example, a system of spirituality is an orderly arrangement of ideas about God and the relationship of humans to God.



   b) Physical System:

   i) A physical system is a set of tangible elements which operate together to accomplish an objective.

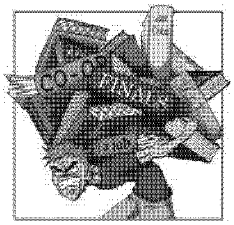
   ii) E.g. Computer system, University system etc.



3. **On the basis of Interactive behavior**: Systems may be classified as Open system or closed system based on 'how the system interacts with environment'. **(RTP-M16, M17)**

   a) Open System:

   i) A system that interacts with its environment by taking input and returning output is termed as an Open System.

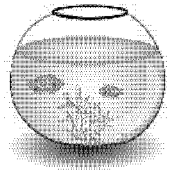


ii) With change of environment, an open system also changes to match itself with the environment.

iii) For example, the education system or any business process system will quickly change when the environment changes.

iv) *Information systems are open systems because they accept inputs from environment and sends outputs to environment.*

b) **Closed System:**

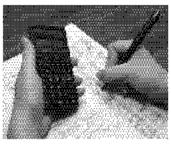


i) A closed system that does not interact with the environment.

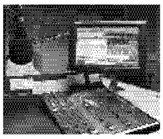
ii) Such systems are insulated from the environment and are not affected with the changes in environment

iii) Eg: Consider a 'throw - 2 - away' type sealed digital watch.

4. **On the basis of degree of human intervention:** According to the degree of human intervention, systems may be classified as manual or automated systems.



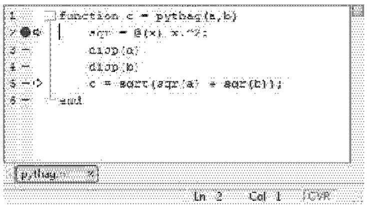
a) **Manual Systems:** Manual Systems are the systems where data collection, manipulation, maintenance and final reporting are carried out absolutely by human efforts.



b) **Automated Systems:** Automated Systems are the systems where computers are used to carry out all the tasks.

5. **On the basis of working/output:** On the basis of working style and the output, systems can be classified as deterministic and probabilistic systems. M-14 Q.P

a) **Deterministic System:**

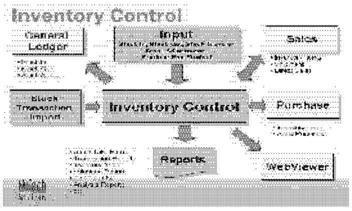


```
function c = pythag(a,b)
    sqr = @(x) x.^2;
    disp(a)
    disp(b)
    c = sqrt(sqr(a) + sqr(b));
end
```

i) A deterministic system operates in a predictable manner wherein the interaction among the parts is known with certainty.

ii) An example is a correct computer program, which performs exactly according to a set of instructions.

b) **Probabilistic System:**



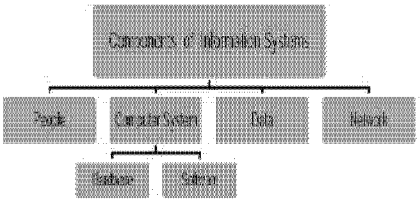
i) The probabilistic system can be described in terms of probable behavior, but a certain degree of error is always attached to the prediction of what the system will do.

ii) An inventory system is an example of a probabilistic system.

Q.No.3. Explain the key components of Computer Based Information System (CBIS)? (OR) Discuss Information System and its components. What are the activities carried out by Information System in general? [B] [MTP – F15]

1. A computer based Information system (CBIS) is a combination of people, IT and business processes that helps management in taking important decisions to carry out the business successfully.

2. A CBIS consist of



Components of Information Systems

a) **People:** this includes Users, Programmers, Analyst, Administrators etc. The success of CBIS depends upon the people.

b) **Computer System:** It includes components in terms of hardware and software.

i) **Hardware:** It includes physical components of the computers such as servers, CPU, RAM, Hard disk etc.

ii) **Software:** Software means the programs which include system software (e.g. UNIX, LINUX, WINDOWS etc), application software (programs designed to perform specific task) and utility software (e.g. tools).

c) **Data:** The data may be alphanumeric, text, image, video, audio, and other forms.

d) **Network:** The network means collection of computers connected through communication media (internet, intranet, extranet etc.).

3. **An information system model consists of following steps:**

a) Data collection.

b) Input of data to information system.

c) Processing of data using data processing software.

d) Processed data is either stored in the storage device or communicated to users as output.

Q.No.4. Discuss the important characteristics of computerized based information system in brief? [A] (PM, RTP N15, M17)

Some of the important characteristics of Computer Based Information Systems are as follows:

1. All systems work for predetermined objectives.
2. A system has a number of interrelated and interdependent subsystems or components.
3. Every sub system depends on other subsystems for its inputs. No subsystem can function in isolation.
4. If one subsystem or component of a system fails then the whole system does not work.
5. The way a subsystem works with another subsystem is called interaction in order to achieve the goal of the system.
6. The work done by individual subsystems is integrated to achieve the central goal of the system.
7. The goal of individual subsystem is of lower priority than the goal of the entire system.

Q.No.5. What are the major areas of computer based applications? [A] (RTP- M16, M 17)

The Major areas of computer based applications are:

1. **Finance and Accounting:**

a) The main goal of this subsystem is to ensure the financial viability of the organization, enforce financial discipline and plan and monitor the financial budget.

b) It also helps in forecasting revenues, determining the best resources and uses of funds and managing other financial resources.

c) Typical sub-application areas in finance and accounting are:

i) Financial accounting
ii) General ledger
iii) Accounts receivable/payable
iv) Asset accounting
v) Investment management
vi) Cash management
vii) Treasury management
viii) Fund management and Balance sheet.

2. **Marketing and Sales:**

The objective of this subsystem is to maximize sales and ensure customer satisfaction.

Marketing:

a) Facilitates the chances of order procurement by marketing the products of the company.

b) Creating new customers.

c) Advertising the products etc.

Sales:

a) It uses an order processing system to keep status and track of orders and Generate bills for the orders.

b) Offers servicing functions to the customers.

c) Strategies for rendering services during warranty period.

d) Analyzing the sales data by category.

e) Helps the corporate managers to take decisions in many crucial areas.

3. **Production or Manufacturing:**

a) The objective of this subsystem is to optimally deploy man, machine and material to maximize production or service.

b) It generates production schedules and schedules of material requirements.

c) Monitors the product quality.

d) Plans for replacement or repairing the machinery.

e) It also helps in overhead cost control and waste control.

4. **Inventory /Stores Management:**

a) The inventory management system is designed with a view to keeping the track of materials in the stores and maintains optimal level stock of raw materials, components and equipments.

b) The inventory management system is designed with a view to

i) Identification of important items in terms stock value

ii) Identification of most frequently moving items

iii) Provides important information for production schedules and marketing/sales strategies and semi-finished and finished goods.

5. **Human Resource Management:**

a) Utilization of this resource in most effective and efficient way is an important function for any enterprise.

b) Skill database maintained in HRM system helps the management for allocating manpower to right activity.

c) An HRM system may have the following modules:

i) Personnel administration

ii) Recruitment management

iii) Travel management

iv) Benefit administration

v) Salary administration

vi) Promotion management etc.

	System Type	***Justification***
i) *Marketing system*	*Open System*	*The marketing system plays a pivotal role in the running of a business in the competitive environment. The objective of the system is to maximize customer satisfaction by providing a free interactive environment. The system takes input/feedbacks and facilitates the outcomes as products of the company and to create new customers.*
ii) *Communication System*	*Open System*	*The communication system in a organization is a point of contact to balance the external influence and render its services to the customers. The system interacts freely with its environment by taking input and returning output.*

iii) *Manufacturing System*	*Closed System*	*This system is in place to meet a particular objective. It does not interact neither with the environment nor changes with the change in the environment. A manufacturing unit is completely isolated from its environment for its operation*
iv) *Pricing System*	*Probabilistic and Open System*	*The system has a probable behavior and interacts freely with its environment by taking inputs and returning outputs. The pricing system is a dynamic one which influences the form of profit and goodwill of an organization.*
v) *Hardware-Software System*	*Closed Deterministic System*	*Since the interaction among the parts of the system is known with certainty and does not interact with the environment and does not change with the change in the environment. Here the requirements of the hardware and software inventory are known with certainty. The operational state of these systems is in a predictable manner.*

Q.No.6. Explain the different types of information systems? [B] (RTP - M15)

a) Operational Level Systems:

i) This supports operational managers by keeping track of the elementary activities and transactions of the enterprises e.g. sales, payroll, receipts etc.

ii) These are primarily needed to answer routine questions and keep track of flow of transactions though the enterprises.

b) Knowledge Level Systems:

i) This type of system supports the business to integrate new knowledge into the business and control the flow of paperwork.

ii) It helps the organization's knowledge and data workers and is especially in the form of workstations.

iii) It is the fastest growing application in business today.

c) Management Level Systems:

i) It supports the middle managers in monitoring, decision-making and administrative activities.

ii) At this level, managers plan, organize, lead and control the activities of other managers.

d) Strategic Level Systems:

i) It supports the senior level management to tackle and address strategic issues and long term trends, both inside organization and the outside world.

ii) It answers questions like what products should be launched to increase the profit and capture the market. It helps in long term planning.

(OR)

1. Management at different levels takes decision matching to their position or hierarchy in the organization.

2. Different types of information systems are designed and developed for management and business applications.

3. Information system can be categorizes as:

a) Operations support system (OSS):

OSS supports day-to –day operations. It includes:

i) Transaction processing system (TPS)

- **ii)** Process control system (PCS)
- **iii)** Enterprise collaboration system (ECS)

b) Management support system (MSS):

MSS supports managerial uses of information for effective planning and decision making. It includes:

- **i)** Management information system (MIS)
- **ii)** Decision support system (DSS)
- **iii)** Executive information system (EIS)

c) Office automation system (OAS):

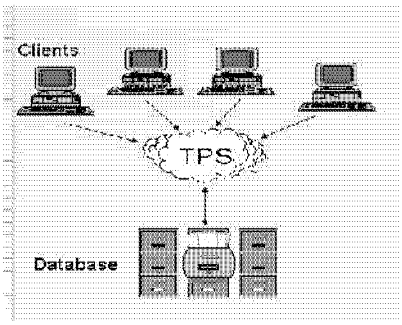
OAS supports quality and efficient document writing, management and analysis etc. it includes:

- **i)** Text processing system
- **ii)** Electronic document management system (EDMS)
- **iii)** Electronic communication systems (ECS)
- **iv)** Teleconferencing and video conferencing system (TVCS).

Q.No.7. Write short notes Operations Support Systems (OSS)? [B]

1. Operation Support System supports day to day data processing activities of organization.
2. OSS produces a variety of information for internal and external use.
3. It improves the operational efficiency and effectives of the organization.
4. *Its role is to effectively process business transactions, control industrial processes, support enterprise communications and collaborations and update corporate database.*
5. These are further classified into three categories.
   - **a)** Transaction support system (TPS).
   - **b)** Process control system (PCS).
   - **c)** Enterprise collaboration system (ECS).

Q.No.8. What do you understand by TPS? Briefly discuss the key activities involved in TPS? [A] (PM, RTP- N14, M-14)



1. TPS operates at the lowest level of management in an information system.
2. TPS manipulates data from business transactions.
3. Any business activity such as sales, purchase, production, delivery, payments or receipts involves transaction and these transactions are to be organized and manipulated to generate various information products for external use.
4. Typically TPS involves the following activities
   - **a)** Capturing data to organize in the form of files or databases.
   - **b)** Processing of files/databases using application software.
   - **c)** Generating information in the form of reports.
   - **d)** Processing of queries from various areas of the organization.
5. A transaction processing system may follow periodic data preparation and batch processing (as in payroll application) or on-line processing (as in inventory control application).

Q.No.9. What are the principle components of TPS? Discuss in brief? [A] (PM)

The main components of a TPS include inputs, processing, storage and outputs.

1. **Inputs:** Source documents, such as customer orders, sales, slips, invoices, purchase orders, and employee time cards, are the physical evidence of inputs into the Transaction Processing System.
2. **Processing:** This involves the use of journals and registers to provide a permanent and chronological record of inputs. Journals are used to record financial accounting transactions, and registers are used to record other types of data not directly related to accounting. *Some of the common journals are sales journal, purchase journal, cash receipts journal etc.*
3. **Storage:** Ledgers and files provide storage of data on both manual and computerized systems. *The general ledger, the accounts/vouchers payable ledgers, and the accounts receivable ledger are the records of final account that provide summaries of a firm's financial accounting transactions.*
4. **Output:** Any document generated in the system is output. For example - a customer invoice is an output from the order-entry application system and input document to the customer.

Q.No.10. Explain the basic features of TPS? [A] (PM, MTP- N14)

1. **Large volume of data:** As TPS is transaction – oriented, it generally consists large volumes of data and thus requires greater storage capacity. *Their primary objective is to ensure that the data regarding the economic events in the enterprises are captured quickly and correctly.*
2. **Automation of basic operations:** Any TPS aims at automating the basic operations of a business enterprise and plays a critical role in the day-to-day functioning of the enterprise. Any failure in the TPS for a short period of time can play havoc with the functioning of the enterprise. *TPS is an important source of up-to-date information regarding the operations in the enterprise.*
3. **Benefits are easily measurable:** TPS reduces the workload of the people associated with the operations and improves their efficiency by automating some of the operations. Most of these benefits of the TPS are tangible and easily measurable.
4. **Source of input for other systems:** TPS is the basic source of internal information for other information systems. *Heavy reliance by other information systems on TPS makes TPS important for tactical and strategic decisions as well.*

Q.No.11. Write short notes on PCS and ECS? [B]

1. **Process Control System (PCS):**
   - a) In this type of system, computer is used to control ongoing physical processes. The computers are designed to automatically make decisions, which adjust the physical production process.
   - b) For example- the assembly lines of the automated factories.
2. **Enterprise Collaboration Systems (ECS):** These systems use a variety of technologies to help people work together. It supports collaboration to communicate ideas, share resources and co-ordinate cooperative work efforts. Its objective is to use IT to enhance the productivity and creativity of teams in enterprises.

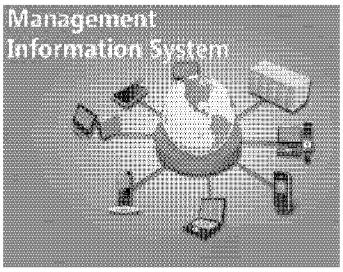
Q.No.12. Write short notes on Management Support Systems (MSS)? [B]

1. MSS supports managers in effective decision making by providing relevant and required information at the right time to the right people.

2. These are generally categorized into
   a) Management Information System
   b) Decision Support Systems c) Executive Information Systems.

Q.No.13. What do you understand by MIS? Discuss major Characteristics of an effective MIS? (OR) 'MIS supports the manager at different levels to take decisions to fulfill the organizational goals'. Explain the major characteristics of MIs to achieve these goals. (OR) State the factors to be considered for designing an effective Management Information System. [A] (PM, MTP- M16, S16, N15 - 6M)

1. An integrated user-machine system designed for providing information to support operational control, management control and decision making functions in an organization.
2. In other words "MIS is a computer based system that provides flexible and speedy access to accurate data".
3. MIS supports the managers at different levels to take strategic (at top level) or tactical (at middle level) management decisions to fulfill the organizational goals.
4. MIS at different levels has different flavors and they are available in the form of reports, tables, graphs and charts or in presentation format using some automated tools.



5. MIS at the top level is much more comprehensive but is condensed or summarized compared to the information provided to those at middle level management.
6. MIS provide reports to management that can help in making effective, structured types as applicable to decisions of day-to-day operations.
7. These reports and displays can be made available on demand, periodically or whenever exceptional conditions occurred.
8. MIS is designed to provide accurate, relevant and timely information to managers at different levels and in different functional areas throughout the organization for decision-making purpose.

Important characteristic of an MIS:

1. **Management Oriented:** It means that effort for the development of the information system should start from an appraisal of management needs and overall business objectives. *Such a system is not necessarily for top management only but may also meet the information requirements of middle level or operating levels of management as well.*
2. **Management Directed:** Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts.
3. **Integrated:** Development of information system should be an integrated one which means that all the functional and operational information sub-system should be tied together into one entity which generated more meaningful information to management.
4. **Common Data Flows:** It means the use of common input, processing and output procedures and media whenever required. Data is captured by system analysts only once and as close to its original source as possible. *They, then, try to utilize a minimum of data processing procedures and sub-systems to process the data and strive to minimize the number of output documents and reports produced by the system.*
5. **Heavy Planning Element:** An MIS usually takes 3 to 5 years and sometimes even longer period to get established firmly within a company. MIS designer must be present in MIS development who should consider future objectives and requirements of information as per the organization structure.

6. **Sub System Concept:** Even though the information system is viewed as a single entity, it must be broken down into digestible sub-systems which can be implemented one at a time by developing a phasing plan.
7. **Common Database:** Database holds the functional systems together. It is defined as a "super-file" which consolidates and integrates data records formerly stored in many separate data files. The organization of a database allows it to be accessed by several information sub-systems and eliminates the necessity of duplication in data storage, updating, deletion and protection.
8. **Computerized:** MIS can be implemented without using a computer; the use of computers increases the effectiveness of the system and it can handle a wide variety of applications by providing their information requirements quickly. It also provides accuracy and consistency in processing data and reduction in clerical staff.

Q.No.14. Explain various Misconceptions about MIS? [A] (PM, RTP- N14, MTP-O15-F16)

Following are the major misconceptions about MIS:

1. Any computer based information system is a MIS
2. Any reporting system is MIS
3. MIS is a Management technique
4. MIS is a bunch of technologies
5. MIS is about use of computers:
6. More data in reports means more information for managers
7. Accuracy in reporting is of vital import for decision making.

Q.No.15. What are the main Pre-requisites of an effective MIS? Explain them briefly. (Or) Discuss the prerequisites of an effective MIS? [A] (N16–6M)

The main pre-requisites of an effective MIS are as follows:

1. **Database:**
   a) It is collection of files, which is collection of records and records are nothing but collection of data.
   b) The data in database is organized in such a way that accessing to the data is improved and redundancy is reduced.
   c) The Main characteristics of database are given as follows:
      i) It is user–oriented.
      ii) It is capable of being used as a common data source to various users, helps in avoiding duplication of efforts in storage and retrieval of data and information.
      iii) It is available to authorized persons only.
      iv) It is controlled by a separate authority established for the purpose, known as Database Management System (DBMS).
2. **Qualified system and management staff:**
   a) MIS should be manned by qualified officers. These officers who are expert in the field should understand clearly the views of their fellow officers.
   b) For this, the organizational management base should comprise of two categories of officers
      i) **Systems and Computer experts** these are capable of understanding management concepts to facilitate the understanding of problems faced by the concern and also be clear about the process of decision making and information requirements for planning and control functions.

ii) **Management experts** should also understand quite clearly the concepts and operations of a computer. This basic knowledge of computers will be useful to place them in a comfortable position.

3. **Support of Top Management:**

a) MIS should have the full support of top management.

b) An effective MIS requires total involvement of top management of MIS development, because subordinates will not accept the MIS unless top management is involved in it.

4. **Control and maintenance of MIS:**

a) **Control** of the MIS means the operation of the system as it was designed to operate.

b) Some time, users develop their own procedures or short cut methods to use the system, which reduce its effectiveness.

Q.No.16. Write about Evaluation of MIS? [B]

1. An effective MIS should be capable of meeting the information requirements of its executives in future as well.
2. This capability can be maintained by evaluating the MIS and taking appropriate timely action.
3. The evaluation of MIS should take into account the following points.

a) Examining whether enough flexibility exists in the system, to cope with any expected or unexpected information requirement in future.

b) Ascertaining the view of users and the designers about the capabilities and deficiencies of the system.

c) Guiding the appropriate authority about the steps to be taken to maintain effectiveness of MIS.

Q.No.17. What are the major constraints in operating a MIS? (OR) "There are various constraints which come in the way of operating an MIS? Explain any four such constraints in briefly. [A] (PM, RTP- N14)

Major constraints which come in the way of operating an information system are the following:

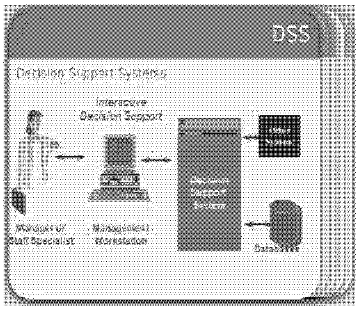
1. **Non-availability of experts:** It is always difficult to find experts who can identify the information needs of the organization for decision making process and can design and implement an effective MIS as per the information need.
2. **Problem of selecting the sub-system of MIS to be installed and operated upon:** Sometimes it becomes a major constraint to select first sub systems for which MIS can installed and operated upon because failure in acceptance of first sub systems affects the acceptance for total systems.
3. **Non-standardization of MIS:** Due to varied objectives normally MIS is non standardized product, i.e. each organization requires MIS as per their own needs. This causes a problem in designing, implementing and maintaining the MIS.
4. **Non-availability of cooperation from staff:** Change is a major problem i.e. normally staff resists for acceptance of computerized system. Educating the staff may solve this problem. *This task should be carried out by organizing lecturers, showing films and also explaining to them the utility of the system.*

Q.No.18. Explain the Limitations of MIS? [B] (PM, RTP M14-N16, M17- 5M)

1. MIS based on quantity and quality of input and processes.
2. MIS is not a substitute for effective management which means that it cannot replace managerial judgment in making decisions in different functional areas.
3. MIS may not have requisite flexibility to quickly update itself with the changing needs of time, especially in fast changing and complex environment.
4. MIS cannot provide tailor-made information packages suitable for the purpose of every type of decision made by executives.
5. MIS takes into account mainly quantitative factors.
6. MIS is less useful for making non-programmed decisions.
7. The effectiveness of MIS is reduced in organizations, where the culture of hoarding information and not sharing with other holds.
8. MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.

Q.No.19. What is Decision Support System (DSS)? [A] (PM, RTP-M14)

1. DSS is a type of computerized information system that supports business and organizational decision-making activities.
2. A decision support system (DSS) can be defined as a system that provides tools to managers to assist them in solving semi structured and unstructured problems in their own.
3. A DSS is not intended to make decisions for managers, but rather to provide managers with a set of capabilities that enables them to generate the information required by them in making decisions.
4. A DSS support the human decision making process, rather than providing a means to replace it.



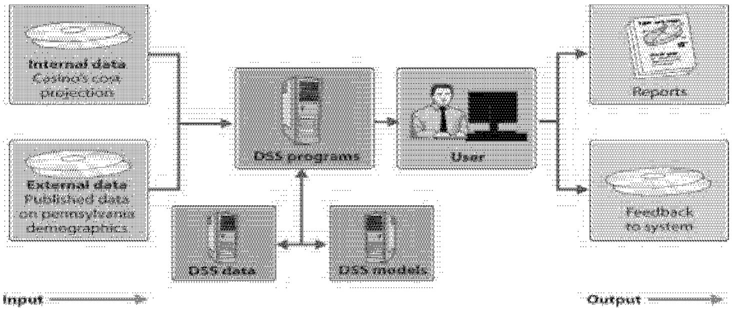
5. *A properly designed DSS is an interactive software-based system intended to help decision makers to gather useful information from raw data, documents, personal knowledge, and/or business models to identify and solve problems and make decisions.*

Q.No.20. Explain various key Characteristics of DSS? [A] (PM, RTP-M14)

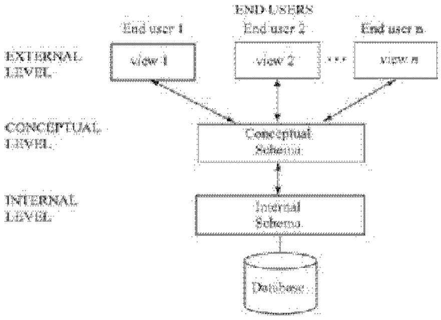
1. DSS provides solutions of unstructured and semi structures problems.
2. Supports decision making at all levels of management.
3. DSS support is provided to individuals as well as groups.
4. DSS is flexible and adaptable
5. DSS provides user-friendly features and it is easy to use.
6. DSS focuses on decision rather than data and information.
7. DSS should be extensible and evolve overtime.
8. DSS utilizes both internal and external database.

Q.No.21. Explain the basic Components of DSS? [A]

Component of DSS includes:



1. **Users:**
   - **a)** Usually, the user of a DSS is a manager with some unstructured or semi-structured problem.
   - **b)** The manager may be at any level of authority in the organization (e.g. either top level or middle level or bottom level managers).
   - **c)** Generally, users do not need computer knowledge to use a decision support system.
2. **Databases:**
   - **a)** Decision support systems include one or more databases.
   - **b)** These databases contain both routine and non-routine data from both internal and external sources.
   - **c)** Some data may come from internal sources. An organization generates this type of data in the normal course of operations - for example data from financial and managerial accounting systems.
   - **d)** The database may also capture data from other subsystems such as marketing, production and personnel.
   - **e)** External data include assumptions about variables such as interest rates, market prices and level of competition.
   - **f)** Implementation of Database - Database is implemented at three levels as listed below:
     - **i) Physical level:** It involves the implementation of the database on the hard disk i.e. storage of data in the hard disk.
     - **ii) Logical Level:** It is designed by professional programmers, who have complete knowledge of DBMS. It deals with the nature of data stored, the scheme of the data.
     - **iii) External level:** The logical level defines schema, which is divided into smaller units known as sub-schemas and given to the managers in numbers of views.



3. **Planning languages:**

   (Distinguish between General-purpose planning languages and Special-purpose planning languages) (RTP M16 - N16)

   Two types of planning languages are commonly used in DSS.

   - **a) General Purpose planning language:** These languages allow users to perform many routine tasks viz., retrieving data from a database or performing statistical analysis, budgeting, forecasting and worksheet oriented problems. The languages used in most of the spread sheets are the good examples.

b) **Special purpose planning language:** Special purpose planning languages are statistical languages viz., SAS, SPSS and Mini Tab. These languages perform statistical and mathematical operations.

4. **Model base:**

a) The model base is the "brain" of the decision support system because it processes data with the help of data provided by the user and the database.

b) There are many types of model bases, but most of them are custom developed models that do some type of mathematical functions - for example, regression analysis, time series analysis, linear programming and financial computations.

c) The analysis provided by model base is the key for user's decision.

Q.No.22. Discuss various examples of Decision Support Systems in Accounting? (OR) "Decision support systems are widely used as part of an Organization's Accounting Information system". Give examples to support this statement. [B] (PM, RTP-N15)

1. Decision support systems are widely used as part of an organization's AIS.
2. Many DSS's are developed in-house, to solve specific problems.
3. Some examples of DSS in accounting are:

a) **Cost Accounting system:** Cost structure is very complex in health care industry. It is very difficult to divide costs in the areas of supplies, expensive machinery, technology and a variety of personnel. Cost accounting applications help health care organizations to calculate product costs for individual products or services.

b) **Capital Budgeting System:** Companies require new tools to evaluate high-technology investment decisions. Decision makers need to supplement analytical techniques such as NPV and IRR with decision support systems.

c) **Budget Variance Analysis System:** Financial institutions rely heavily on their budgeting systems for controlling costs and evaluating managerial performance.

d) **General DSS:** DDSs use general purpose planning languages that can analyze different types of problems. In a sense these systems act as tools to decision makers. To use this type of systems the user has to input data and answer questions about a specific problem.

Q.No.23. Difference between the DSS and the traditional MIS? [B] (MTP-N16-4M)

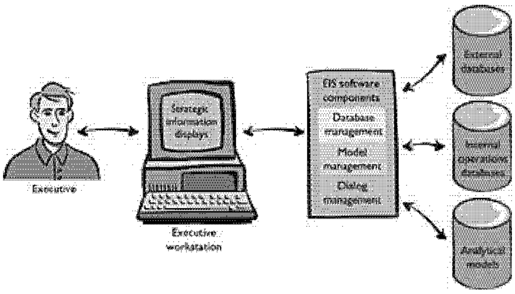
Dimensions	DSS	Traditional MIS
Philosophy	Providing integrated tools, data, models and languages to end users.	Providing structured information to end users.
Orientation	External orientation	Internal orientation
Flexibility	Highly flexible	Relatively inflexible
Analytical capability	More analytical capability	Little analytical capability
System analysis	Emphasis on tools to be used in decision process	Emphasis on information requirement analysis.
System design	Interactive process	System development based on static information requirements.

Q.No.24. What is EIS? Explain its major characteristics? [A] (PM, RTP - M14 - N14 - N15)

1. An executive information system (EIS) is a DSS that is designed to meet the special needs of top-level managers.
2. It is a tool that provides direct on-line access to relevant information in a useful and navigable format.
3. ESS is sometimes referred to as an Executive Support System (ESS).
4. *It serves the strategic level i.e. top level managers of the organization.*

Characteristics of EIS: Major Characteristics of an EIS are given as follows:

1. EIS is a Computer-based-information system that serves the information need of top executives.
2. EIS enables users to extract summary data and model complex problems without the need to learn query languages statistical formulas or high computing skills.
3. EIS provides rapid access to timely information and direct access to management reports.



4. EIS is capable of accessing both internal and external data.
5. EIS provides extensive online analysis tool like trend analysis, market conditions etc.
6. EIS can easily be given a DSS support for decision making.

Q.No.25. Write about Executive Decision - Making Environment? (OR)
The intuitive character of executive decision making is reflected strongly in the types of information found most useful to executives". Discuss characteristics of the types of information used in executive decision making. [A] (N16 – 6M)

1. In the Executive Decision Making Environment, the executives have to take several broad decisions. For this they require information.
2. The intuitive character of executive decision-making is reflected strongly in the types of information found most useful to executives.
3. Five characteristics of the types of information used in executive decision making are given as follows:

   a) **Lack of structure:** Many of the decisions made by executives are relatively unstructured. For instance, what general direction should the company take? So, it is not always obvious which data are required or how to weight available data when reaching a decision.

   b) **High degree of uncertainty:** Executives work in a decision space that is often characterized by a lack of precedent. So, the information required also may not have a clear precedent.

   c) **Future orientation:** Strategic-planning decisions are made in order to shape future events. As conditions change, organizations must change also. Consequently, the information may be required for future trends etc.

   d) **Informal source:** Executives, more than other types of managers, rely heavily on informal source for key information. Some sources of information are Business meals, meetings, brainstorming with a colleague, social events, media etc.

   e) **Low level of detail:** Most important executive decisions are made by observing broad trends. This requires the information to be focusing on large overview than the tiny items.

Q.No.26. 'There is a practical set of principles to guide the design of measures and indicators to be included in an EIS' . Explain those principles in brief. [A] (PM)

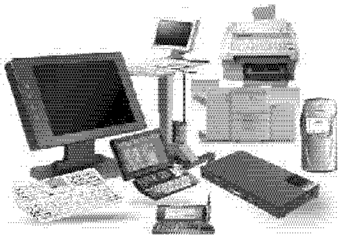
A practical set of principles to guide the design of measures and indicators to be included are:

1. EIS measures must be easy to understand and collect the data.
2. EIS measures must be based on a balanced view of the organization's objective.
3. Performance indicators in an EIS must reflect everyone's contribution in a fair and consistent manner.
4. EIS measures must encourage management and staff to share ownership of the organization's objectives.
5. EIS information must be available to everyone in the organization.
6. EIS measures must evolve to meet the changing needs of the organization.

Q.No.27. Difference between the EIS and Tradition information system? [B] (PM)

Dimensions of Difference	Executive Information System	Traditional Information System
Level of management	For top or near top executives	For lower staff
Nature of information Access	Specific issues/problems and aggregate reports	Status reporting
Nature of information provided	Online tools and analysis	Offline status reporting
Information Sources	More external less internal	internal
Drill down facility to go through details at successive levels	Available	Not available
Information format	Text with graphics	Tabular
Nature of interface	User-friendly	Computer-operator generated

Q.No.28. Write about Office Automation Systems (OAS)? (OR) Office Automation Systems (OAS) is the most rapidly expanding system. Describe the broad groups of OAS based on the types of its operations. [A] (RTP - M16, MTP-N16, M15 – 6M



1. **Office Automation System (OAS)** is among the newest and most rapidly expanding computer based information systems.
2. All the activities are simple and effective by the use of computers.
3. Different office activities can be broadly grouped in to the following types of operations:
   a) **Document Capture:** Documents originating from outside sources like incoming mails, notes, handouts, charts, graphs etc. need to be preserved.
   b) **Document Creation:** This consists of preparation of documents, dictation, editing of texts etc. and takes up major part of the secretary's time.
   c) **Receipts and Distribution:** This basically includes distribution of correspondence to designated recipients.
   d) **Filling, Search, Retrieval and Follow up:** This is related to filling, indexing, searching of documents, which takes up significant time.
   e) **Calculations:** These include the usual calculator functions like routine arithmetic, operations for bill passing, interest calculations, working out the percentages and the like.
   f) **Recording Utilization of Resources:** This includes record keeping in respect to specific resources utilized by office personnel.

Q.No.29. What are the Benefits of Office Automation System? [B] (PM)

1. OAS improves communication within an organization and between organizations.
2. OAS reduces the cycle time between preparation of messages and receipt of messages at the recipients' end.
3. OAS reduces the costs of office communication both in terms of time spent by executives and cost of communication links.
4. OAS ensures accuracy of communication flows.

**Q.No.30. What is Computer based office automation system? (Or)
Office automation is the most rapidly expanding system. Describe the broad groups of OAS based on the types of its operation. [C] (PM)**

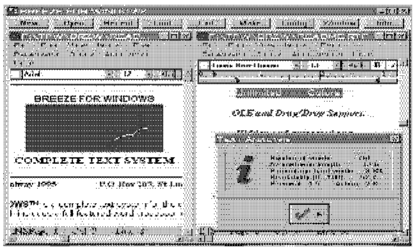
Major computer based OAS includes

a) Text processing systems **b)** Electronic document management systems

c) Electronic message communication systems **d)** teleconferencing and video conferencing.

Q.No.31. Explain the Text Processing Systems? [C]

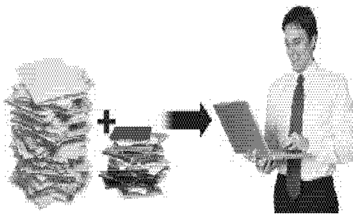
1. Text processing systems are the most commonly used components of the OAS, because a large portion of the office communication takes place in writing using words of a natural language.
2. Text processing systems automate the process of development of documents such as letters, reports, memos etc.
3. They permit use of standard stored information to produce personalized documents.
4. Such automation reduces keying effort and minimizes the chances of errors in the document.



5. The text processor may be simple word processing systems or desktop publishing systems which help in quick production of multiple copies of the document with quality printing.

Q.No.32. Write short notes Electronic Document Management System (EDMS)? [B] (MTP- N15 - 4M)

1. The computer based document management systems are used for capturing the information contained in documents, storing for future reference and retrieved whenever needed.
2. These systems are linked to the office automation systems such as text processors, electronic message communication systems etc.
3. These systems are very useful in remote access of documents that is almost impossible with manual document management systems.



4. For example, a customer may have a complaint concerning delivery of goods not being in accordance with the delivery instructions in the order.

Q.No.33. What is Electronic Message Communication Systems? Explain components? [B]

1. Business enterprises have been using a variety of communication systems for sending and receiving messages. These include telephone, mail and facsimile (Fax), etc.
2. The computer based message communication systems offers a lot of economy, reliability and cost of communication.

Components of Message Communication Systems:

1. **E-mail:**

   Following are the features of E-Mail: (RTP-N15)

   a) **Electronic Transmission:** The transmission of messages with email is electronic and message delivery is very quick and confirmation of transmission is also quick and the reliability is very high.

   b) **Online development and editing:** The email message can be developed and edited online before transmission. The online development and editing eliminates the need for use of paper in communication.

   c) **Broadcasting and Rerouting:** Email permits sending a message to a large number of target recipients. The E-mail has the advantage of being integrated with the other information systems.

   d) **Portability:** Email renders the physical location of the recipient and sender irrelevant. The email can be accessed from any Personal computer equipped with the relevant communication hardware, software and link facilities.

   e) **Economical:** The advancements in communication technologies and competition among the communication service providers have made e-mail is the most economical mode of sending messages.

2. **Facsimile (Fax):**

   a) Facsimile (Fax) is electronic communication of images of documents over telephone lines.

   b) The computer based fax technology automates fax communication and permits sharing of fax facilities.

   c) It uses special software and fax servers to send and receive fax messages using common communication resources.

3. **Voice Mail:**

   a) Voice mail is a variation of the email in which messages are transmitted as digitized voice.

   b) The recipient of the voice mail has to dial a voice mail service or access the e-mail box using the specified equipment and he can hear the spoken message in the voice of the sender.

4. **Teleconferencing and Video-conferencing Systems:**

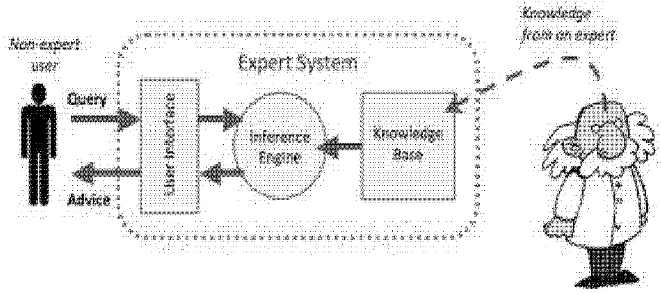
   a) Teleconferencing is conducted a business meeting involving more than two persons located at two or more different places.

   b) It helps in reducing the time and cost of meetings.

   c) Teleconferencing may be audio or video conferencing with or without use of computer systems.

Q.No.34. What is an Expert System? Discuss some of the business applications of expert system in brief. [A] (PM, RTP - M15, MTP M16, N16 N16, N14- 3M)

1. An expert system (ES) is a computerized information system that allows non-experts to make decisions comparable to that of an expert.
2. Expert systems are used for complex or unstructured tasks that require experience and specialized knowledge.
3. Expert System is software systems that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from experts.



Some of the business applications of Expert Systems are:

1. **Accounting and Finance:** It provides tax advice and assistance, helping with credit authorization decisions, selecting forecasting models, providing investment advice.
2. **Marketing:** It provides establishing sales quotas, responding to customer inquiries, referring problems to telemarketing centers, assisting with marketing timing decisions, determining discount policies.
3. **Manufacturing:** It helps in determining whether a process is running correctly, analyzing quality and providing corrective measures, maintaining facilities, scheduling of tasks, selecting transportation routes, assisting with product design and facility layouts.
4. **Personnel:** It is useful in assessing applicant qualifications, giving employees assisting at filling out forms
5. **General Business:** It helps in assisting with project proposals, recommending acquisition strategies, educating trainees, evaluating performance.

Q.No.35. Explain the need of expert systems? [A] (RTP- M15, MTP N16, N16, N15-3M)

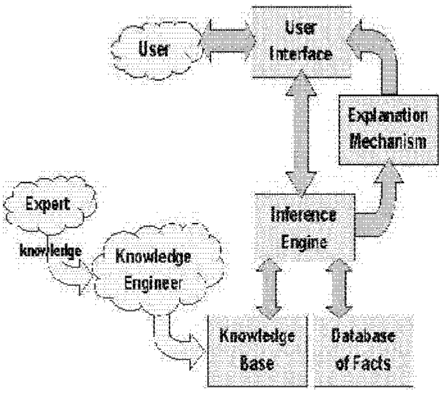
1. Expert labor is expensive and scarce. Knowledge workers employee who routinely work with data and information to carry out their day to day duties are not easy to find and keep and companies are often faced with a shortage of talent in key positions.
2. Moreover, no matter how bright or knowledgeable certain people are, they often can handle only a few factors at a time.
3. Both these limitations imposed by human information processing capability and the rushed pace at which business is conducted today put a practical limit on the quality of human decision making this putting a need for expert systems.

Q.No.36. What are the Components of Expert Systems? [A]

Expert systems typically contain the following components:

1. **Knowledge base:** This includes data, knowledge, relationships, heuristics and decision rules used by experts to solve a particular type of problem. A knowledge base in a computer is equal to the knowledge of an expert or group of experts developed through years of experience in their field.

2. **Inference engine:** This program consists of logic and reasoning mechanism that can simulate the expert's logic process and deliver advice. It uses data obtained from both knowledge base and the user to make associations and inferences, form conclusions and recommend a course of action. Two techniques which model different reasoning methods: backward and forward chaining; some operate with both.



3. **User interface:** A user interface is the method by which an expert system interacts with a user. This program allows the user to design, create, update, use and communicate with the expert system. It can be through dialog boxes, command prompts, forms, or other input methods.
4. **Explanation facility:** With the help of this facility user can know the logic being followed by the expert system to arrive at the conclusion.
5. **Knowledge acquisition facility:** Building a knowledge base, known as knowledge engineering, involves both human expert and a knowledge engineer. The knowledge engineer extracts an individual's expertise and uses the knowledge acquisition facility to enter it into knowledge base.
6. **Database of facts**: It extracts the user problem as much as details and also prompts the user about the problem details, the quantity and quality of given details produces quality of decision.

Q.No.37. Explain the Major Benefits of Expert Systems? [A] (PM, MTP N16, N15 - 3M)

1. Expert Systems preserve the expertise of an expert, leaving the organisation.
2. They provide a cost-effective alternative to human experts.
3. Expert Systems are not subject to human feelings such as fatigue, being too busy, or being emotional.
4. They can outperform a single expert because their knowledge is gained from several experts.
5. They are faster and more consistent and do not get over worked or stressed out.
6. They produce better-quality decisions.
7. They can increase productivity.
8. Expert Systems can be effectively used as a strategic tool is the areas of marketing products, cutting costs and improving products.
9. *Expert Systems put information into an active-form so it can be summoned almost as a real-life expert might be summoned.*
10. *Expert Systems assist novices in thinking the way experienced professional do.*

Q.No.38. Briefly explain some of the properties that potential applications should possess to qualify for Expert System development. [A] (N14 - 3M)

1. An Expert System is highly developed Decision Support System (DSS) that utilizes the knowledge generally possessed by an expert to solve a problem.
2. Expert Systems are software systems that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from such expert systems.
3. Major properties that an application should possess to qualify for Expert System development are given as follows:
   a) **Availability:** One or more experts are capable of communicating 'how they go about solving the problems to which the Expert System will be applied.'

b) **Complexity:** Solution of the problems for which the Expert Systems will be used is a complex task that requires logical inference processing, which would not be easily handled by conventional information processing.

c) **Domain:** The domain, or subject area, of the problem is relatively small and limited to a relatively well-defined problem area.

d) **Expertise:** Solutions to the problem require the efforts of experts. That is, only a few possess the knowledge, techniques, and intuition needed.

e) **Structure:** The solution process must be able to cope with ill-structured, uncertain, missing, and conflicting data, and a dynamic problem-solving situation.

Q.No.39. Write short notes on the following? [C]
a) Knowledge Management Systems **b) Functional Business Information Systems**
c) Strategic Information Systems **d) Cross Functional Information Systems**

a) **Knowledge Management Systems:** These are knowledge based systems that support the conception, association and propagation of business knowledge within the enterprise.

b) **Functional Business Information Systems**: These systems support the operational and managerial applications of the basic enterprises of an industry.

c) **Strategic Information Systems:** These systems provide an industry strategic products, services and capabilities for competitive advantage.

d) **Cross Functional Information Systems:** It is also known as integrated information system that combines most of information systems and is designed to produce information and support decision making for different levels of management and business functions. Ex: ERP

Q.No.40. State the vital roles performed by Information Systems in Enterprise Processes. [B]

Information Systems perform following three vital roles in business firms:

1. **Support an organization's business processes and operations:** This includes operations support systems such as Transaction Processing Systems, Process Control Systems.

2. **Support business decision-making:** This includes Management Information Systems, Decision Support Systems, and Executive Information Systems.'

3. **Support strategic competitive advantage:** This includes Expert Systems, Knowledge Management Systems, Strategic Information Systems, and Functional Business Systems.

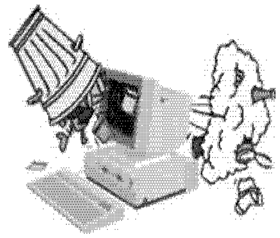
Q.No.41. Discuss some of the important implications of Information systems in business? (OR) Discuss some of the important advantages of Information Systems in business. [B] (PM)

Following are some of the important implications of information systems in business:

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

Q.No.42. What is Information? What are the characteristics of effective and useful Information? (OR) "Information has become a key resource for any type of business activity" Briefly describe the various attributes of information
[A] (PM, RTP - M15, M16, M17-6M, MTP- N14)

1. Information is data that have been put into a meaningful and useful context, and is of real or perceived value in current or progressive decision.



2. For example, data regarding sales by various salesmen can be merged to provide information regarding total sales through sales personnel.
3. This information is of vital importance to a marketing manager who is trying to plan for future sales.
4. The quality of raw materials is crucial. Quality of input fed in determines the quality of information produced. This phenomenon is also known as garbage in garbage out (GIGO).
5. **Attributes of Information:** Some of the important attributes of useful and effective information are as follows:

   a) **Availability:** Availability or Timeliness is a very important property of information. If information is not available at the time of need, it is useless. Data is organized in the form of facts and figures in databases and files from where various information is derived for useful purpose.

   b) **Purpose :** It helps in creating new concepts, identifying problems, solving problems, decision making, planning, initiating, and controlling

   c) **Mode and format:** Information is usually visual, verbal or in written form. All the statistical rules of compiling statistical tables and presenting information by means of diagram, graphs, curves, etc., should be considered and appropriate one followed.

   d) **Decay:** Value of information usually decays with time and usage and so it should be refreshed from time to time

   e) **Rate:** The rate of transmission/reception of information may be represented by the time required to understand a particular situation.

   f) **Frequency:** The frequency with which information is transmitted or received affects its value. Frequency has some relationship with the level of management also it should be related to an operational need.

   g) **Completeness:** The information should be as complete as possible. With the complete information; the manager is in a much better position to decide whether or not to undertake the venture.

   h) **Reliability:** The information should be extracted from reliable sources. Reliable information is a measure of failure or success of using information for decision-making.

   i) **Validity:** It measures the closeness of the information to the purpose which it supports to serve. For example, some productivity measure may not measure, for the given situation, what they are supposed to do e.g., the real rise or fall in productivity.

   j) **Quality:** Quality refers to the correctness of information. Information should, be accurate otherwise it will not be useful.

   k) **Transparency:** If information does not reveal directly what we want to know for decision-making, it is not transparent.

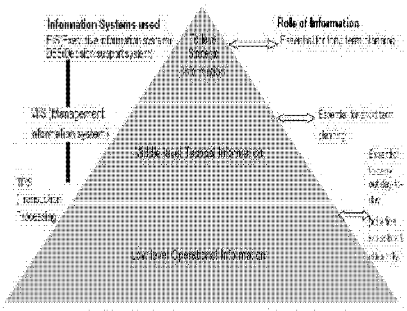
   l) **Cost benefit analysis:** Benefits derived from the information must justify the cost incurred in procuring information.

m) **Value of information:** It is defined as difference between the value of the change in decision behavior caused by the information and the cost of the information. If new information causes a different decision to be made, the value of the new information is the difference in value between the outcome of the old decision and that of the new decision, less the cost of obtaining the information.

n) **Adequacy:** To be useful, information must be adequate so that the desired actions can be initiated. Required information should flow on different directions within the organization and to and from its environment.

Q.No.43. Explain the Role of Information in Business? [B]

1. In a dynamic business environment, it becomes mandatory to have complete information and knowledge of customer buying habits and market strategy for any enterprise.
2. Timeliness, accurate, meaningful and action oriented information enhances an organization ability and capacity to deal with and develop in mission, competition, performance and change.
3. The information can be categorized on the basis of its requirement by the top, middle and lower level management.


Information Systems used
EIS (Executive information systems)
DSS (Decision support system)
Top level Strategic Information
Role of Information
Essential for long term planning
MIS (Management information system)
Essential for short term planning
Middle level Tactical Information
TPS (Transaction Processing)
Essential for carry out day-to-day
Low level Operational Information

Types of Information Systems at Different Management Levels

4. **Top Level Management:**
   a) The top management generally comprise of owners/shareholders, board of directors, its chairman, managing director, or the chief executive, or the managers committee having key officers.
   b) Top level management strives for the information that can help them in major policy decisions such as establishment of new plant, launching of new product etc.
   c) The top management requires strategic information that helps them in making strategy of an enterprise in terms of scope of products, targets of products i.e. customers, competition with market i.e. price, quality, long term planning etc.

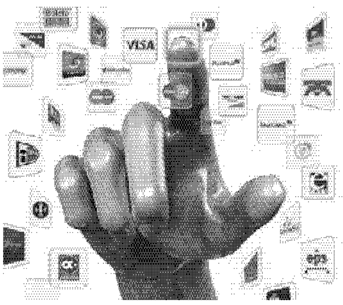
5. **Middle Level Management:**
   a) The middle management comprise of heads of functions departments e.g. purchase manager, production manager, marketing managers, financial controller, and divisional sectional officers working under these functional heads.
   b) Middle managements require tactical information that helps in implementing decisions taken by the top management.
   c) Tactical information is used for short term planning whereas strategy information is used for long term planning.
6. **Lower Level Management:**
   a) The lower level managers are superintendents, supervisor, etc.
   b) The lower management requires operational information, which is required in day- to-day activities.
   c) The operational information mainly comprises of information about stock on hand, information about customer order pending, information about bill payable by customer etc.
   d) These are essential for smooth running of the daily activities of a business at primary level.

Q.No.44. Explain Relative Importance of Information Systems from Strategic and Operational Perspectives? [B]

1. *A business model can be defined as an outline of 'how business is to be done by a company to generate maximum revenue'.*
2. A business strategy is defined as a long term planning for success i.e. tactics that are applied to manage business for increasing business revenue.
3. *A good business strategy is one that enables company to satisfy customers, uses resources efficiently and explore business opportunities outside of the standard business practice to help inspire company expansion.*
4. *An information system can be large or small depending upon the size of the company and can help in decision making, produce high quality of products and perform logistical functions.*
5. In operations management, information systems design can apply to production control, research, development, and manufacturing to produce desired results of the products in terms of quality and cost.
6. Information systems also support logistical processes in various ways, such as real time inquiries to track an item from the point of shipment, receiving and storage of the item and inventory status of the item. Not only this, information systems can also provide the structure for programmers, database managers and data administrators to collaborate on new and existing projects.
7. ERP, Data Mining tools, Data warehouse, Business intelligence, MIS, internet, intranet, extranet etc. are the information systems and information technologies that support managers in every step of business.
8. There are different kinds of systems depending upon the different interest, specialties and levels in an organization.

Q.No.45. Explain the Various types of Business Applications? (OR) Discuss the impact of IT on Information Systems for different sectors? [B] (RTP-N16)

1. IT has increased the communication between executives by providing for online meeting and instant exchange of information.
2. Information system also contributes to an organization's success by providing information that provides innovative ideas to managers and helps them in decision making.
3. Different types of business and enterprises where information systems and IT are popular.
4. **The Accounting Information System:**
   a) The accounting information system comprises of the processes, procedures, and systems that capture accounting data from business processes; record the accounting data in the appropriate records; process the detailed accounting data by classifying, summarizing and consolidating the report the summarized accounting data to internal and external users.
   b) The impact of IT on information systems for different sectors are:
5. **E-business:**
   a) This is also called electronic business and includes purchasing, selling, production management, logistics, communication, sup port services and inventory management through the use of internet technologies.



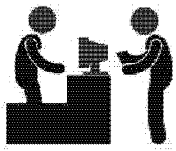
   b) The primary components of E-business are infrastructure (computers, routers, communication media e.g. wire, satellite etc., software and programmers), electronic commerce and electronically linked devices and computer aided networks.

6. **Financial Service Sector:**

a) The financial services sector (banks, bu ilding societies, life insurance companies and short term insurers) manages large amounts of data and processes enormous numbers of transactions every day.

b) Owing to application of IT, all the major financial institutions operate nationally and have wide networks of regional offices and associated electronic networks.

7. **Wholesaling and Retailing:**



a) Retail business uses IT to carry out basic functions including till systems for selling items, capturing the sales data by item, stock control, buying, management reports, customer information and accounting.

b) IT can be used in wholesale for supply chain logistics management, planning, space management, purchasing, re-ordering, and analysis of promotions.

c) E-commerce among partners (suppliers, wholesalers, retailers, distributors) helps in carrying out transactions.

8. **Public sectors:**

a) It includes services provided by the government mainly hospitals, police stations, universities etc. IT/IS can be used to keep records of the cases, respective people involved it, other related documents and can consult the existing data warehouse or databases to take appropriate actions.

b) For example, IS like ERP can be implemented in a university to keep record of its employees in terms of their designation, leaves availed, department, achievements that can be used further in analyzing their performance.

9. **Others:** IT is efficiently used in entertainment industry (games, picture collection etc.), agriculture industry (information is just a mouse click away to the farmers), Tour industry (railway, hotel and airline reservations) and consultancy etc.

Q.No.46. Provide Overview of underlying IT technologies for Businesses. (Or) What are the IT tools you consider for the business growth. (Or) Modern business used information technology to carry out basic functions including systems for sales, advertisement, purchase, management reports etc. Briefly discuss some of the tools of the IT tools crucial for business growth. [A] (MTP-N15)(N14, M16 - 5M)

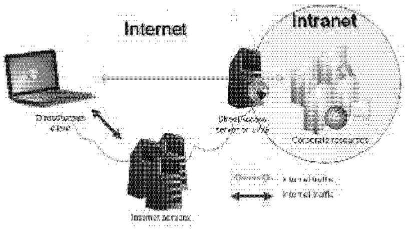
1. Now day's business uses IT to carry out basic functions including systems for selling items, capturing the sales data by item, stock control, buying, management reports, customer information, decision making, accounting etc.

2. Some of the IT tools crucial for business growth includes:

a) **Business Website:**

i) By having a website, enterprise/business becomes reachable to large amount of customers. These websites can be designed by using HTML, XML, ASP, NET etc.

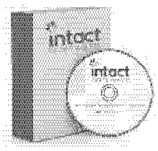
b) **Internet and Intranet:**



i) It is the best source of communication. Intranet is system that permits the electronic exchange of business data within an organization.

ii) E-commerce among partners using intranets, e-mail etc. provides new platform to the business world for conducting business in a faster and easier way.

c) Software and Packages:



i) DBMS, data warehousing, data mining tools, knowledge discovery can be used for getting information that plays important role in decision making that can boost the business in the competitive world.

ii) Enterprise Resource Planning (ERP) Packages:

- An ERP System is a multi module software system that integrates all business process and functions of the entire Enterprise into a single software system, using a single integrated database.
- Each module is intended to collect, process, and store data of a functional area of the organization and to integrate with related processes.

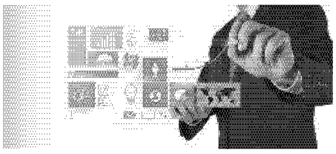
[What is data mining & its applications?]

iii) Data Mining (DM) can be applied in database analysis and decision support i.e. market analysis and management by finding patterns that are helpful in target marketing, customer relation management, market basket analysis, cross selling, market segmentation, risk analysis, customer retention, improved underwriting, quality control, competitive analysis and fraud detection.

iv) Other applications of DM are:

- Text mining
- Web analysis,
- Customer profiling - it can list out what types of customers buy what products by using clustering or classification.
- Identifying customer requirements- it can identify the most demanding and appropriate products for different customers, and also can list the factors that will attract new customers by using prediction etc.,
- Provide summary information i.e. various multidimensional summary reports and statistical summary information,
- Finance planning and asset evaluation
- Cross-sectional and time series analysis
- Resource planning- it can summarize and compare the resources and spending.

d) Business Intelligence (BI):



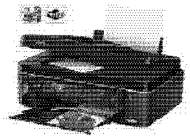
i) Business Intelligence (BI) refers to applications and technologies that are used to collect retrieve and analyze data and information about companies operations.

ii) BI software consists of range of tools.

iii) Some BI applications are used to analyze performance or internal operations and to store, analyze data and manage the human resources.

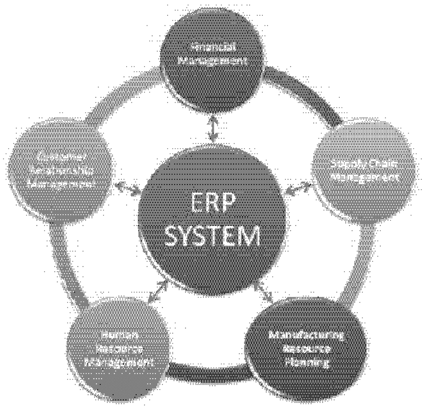
iv) A complete BI provides consistent and standard information essential in enterprise operations.

e) Computers, Scanners, Laptop, Printer, Webcam, Smart Phone etc.:



i) Webcam, microphone etc. are used in conducting long distance meeting. Use of computer systems, printer, and scanner increases accuracy, reduce processing times, enable decisions to be made more quickly and speed up customer service.

Q.No.47. Write about Enterprise Resource Planning (ERP) Packages? [A]


Financial Management
Supply Chain Management
ERP SYSTEM
Manufacturing Resource Planning
Human Resource Management
Customer Relationship Management

1. An Enterprise Resource Planning (ERP) system is a fully integrated business management system, covering functional areas of an enterprise like Procurement, Inventory, Production, Sales, Logistics, Finance, Accounting and Human Resources.
2. "Enterprise Resource Planning has become a powerful tool in the hands of management for effective use of resources and to improve efficiency of an enterprise"
3. It organizes and integrates operation processes and information flows to make optimum use of resources such as men, material, money and machine.
4. ERP promises one database, one application, and one user interface for the entire enterprise.
5. The basis of ERP is to make easy the flow of information among all business functions in the internal boundaries of the organization and control the connections to external stakeholders.
6. ERP software provides competent and efficient administration, and mechanized business activities.
7. *It is a complete software solution package for enhancing the performance in large organizations and meeting their requirements with ease and efficiency.*

Q.No.48. Write about Knowledge Management System (KMS)? [A] (RTP-M16, MTP-N15 4M)

1. Knowledge Management (KM) is the process of capturing, developing, sharing, and effectively using organizational knowledge.
2. It refers to a multi-disciplined approach to achieving organizational objectives by making the best use of knowledge.
3. Knowledge Management Systems (KMS) refers to any kind of IT system that stores and retrieves knowledge, improves collaboration, locates knowledge sources, mines repositories for hidden knowledge, captures and uses knowledge, or in some other way enhances the KM process.
4. KMS treats the knowledge component of any organization's activities as an explicit concern reflected in strategy, policy, and practice at all levels of the organization.
5. There are two broad types of knowledge - Explicit and Tacit.
6. KMS makes a direct connection between an organization's intellectual assets both Explicit [recorded] and Tacit [personal know-how] — and positive results.

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

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

   For example – hand-on skills, special know-how, employee experiences.

Q.No.49. What is ERP? Explain the component and benefits of ERP? [A]
(RTP M16, MTP - N16, N15 - 4M, M16 - 4M)

Enterprise Resource Planning (ERP) -

1. Enterprise resource planning (ERP) is process management software that allows an organization to use a system of integrated applications to manage the business and automate many back office functions related to technology, services and human resources.
2. ERP software integrates all categories of an organization such as operation, product planning, and development, manufacturing, sales and marketing.
3. ERP software is considered an enterprise application as it is designed to be used by larger businesses and often requires dedicated teams to customize and analyze the data and to handle upgrades and deployment.
4. **Components of ERP**
   - **a) Software Component:** The software component is the component that is most visible part and consists of several modules such as Finance, Human Resource, Supply Chain Management, Supplier Relationship Management, Customer Relationship, and Business Intelligence.
   - **b) Process Flow:** It is the model that illustrates the way how information flows among the different modules within an ERP system. By creating this model makes it easier to understand how ERP work.
   - **c) Customer mindset:** By implementing ERP system, the old ways for working which user understand and comfortable with have to be changed and may lead to users' resistance. For example, some users may say that they have spent many years doing an excellence job without help from ERP system. In order to lead ERP implementation to succeed, the company needs to eliminate negative value or belief that users may carry toward utilizing new system.
   - **d) Change Management:** In ERP implementation, change needs to be managed at several levels - User attitude; resistance to change; and Business process changes.
5. **Benefits of ERP (MTP-M16)**
   - **a)** Streamlining processes and workflows with a single integrated system.
   - **b)** Reduce redundant data entry and processes and in other hand it shares information across the department.
   - **c)** Establish uniform processes that are based on recognized best business practices.
   - **d)** Improved workflow and efficiency.
   - **e)** Improved customer satisfaction based on improved on-time delivery, increased quality, shortened delivery times.
   - **f)** Reduced inventory costs resulting from better planning, tracking and forecasting of requirements.
   - **g)** Turn collections faster based on better visibility into accounts and fewer billing and/or delivery errors.
   - **h)** Decrease in vendor pricing by taking better advantage of quantity breaks and tracking vendor performance.
   - **i)** Track actual costs of activities and perform activity based costing.
   - **j)** Provide a consolidated picture of sales, inventory and receivables.

Q.No.50. What is Core Banking System (CBS)? Mention the elements of CBS? [A]

1. Core Banking is a banking services provided by a group of networked bank branches where customers may access their bank account and perform basic transactions from any of the member branch offices.

2. Normal core banking functions will include transaction accounts, loans, mortgages and payments.
3. Banks make these services available across multiple channels like ATMs, Internet banking, and branches.
4. Core Banking System (CBS) may be defined as a back-end system that processes daily banking transactions, and posts updates to accounts and other financial records.
5. These systems typically include deposit, loan and credit processing capabilities, with interfaces to general ledger systems and reporting tools. *Core banking functions differ depending on the specific type of bank.*
6. Examples of core banking products include Infosys' Finacle, Nucleus FinnOne and Oracle's Flexcube application (from their acquisition of Indian IT vendor i-flex).
7. Elements of core banking include:

   a) Making and servicing loans.

   b) Opening new accounts.

   c) Processing cash deposits and withdrawals.

   d) Processing payments and cheques.

   e) Calculating interest.

   f) Managing Customer Relationship Management (CRM) activities.

   g) Managing customer accounts.

   h) Establishing criteria for minimum balances, interest rates, number of withdrawals allowed and so on.

   i) Establishing interest rates.

   j) Maintaining records for all the bank's transactions.

Q.No.51. Write short notes on Operating system security. [A] (PM, N14 4M)

Operating System Security involves policy, procedure and controls that determine, 'who can access the operating system', 'which resources they can access', and 'what action they can take'. The following security components are found in secure operating system:

a) Log-in Procedure: A log-in procedure is the first line of defense against unauthorized access. When the user initiates the log -on process by entering user- id and password, the system compares the ID and password to a database of valid users. If the system finds a match, t hen log-on attempt is authorized.

b) Access Token: If the log on attempt is successful, the Operating System creates an access token that contains key information about the user including user -id, password, user group and privileges granted to the user. The information in the access token is used to approve all actions attempted by the user during the session.

c) Access Control List: This list contains information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compasses his or her user-id and privileges contained in the access token with those contained in the access control list. If there is a match, the user is granted access.

d) Discretionary Access Control: The system administrator usually determines; who is granted access to specific resources and maintains the access control list. However, resource owners in distributed systems may be granted discretionary access control which allows them to grant access privileges to other users.

Q.No.52 A business manager should have adequate knowledge to operate information systems effectively. Elaborate [A] (PM)

To operate Information Systems (IS) effectively and efficiently, a business manager should have following knowledge about it.

a) **Foundation Concepts:** It includes fundamental business, and managerial concepts e.g. 'what are components of a system and their functions', or 'what competitive strategies are required'.

b) **Information Technologies (IT):** It includes operation, development and management of hardware, software, data management, networks, and other technologies.

c) **Business Applications:** It includes major uses of IT in business steps i.e. processes, operations, decision making, and strategic/competitive advantage.

d) **Development Processes:** It comprise how end users and IS specialists develop and execute business/IT solutions to problems.

e) **Management Challenges:** It includes 'how the functionality and IT resources are maintained' and utilized to attain top performance and build the business strategies.

Q.No.53 Distinguish between Operational Level Systems and Management Level Systems. [A] (RTP – M 17)

Operational-Level Systems:

a) These support operational managers in tracking elementary activities. These can include tracking customer orders, invoice tracking, etc.

b) Operational level systems or Operational Support Systems (OSS) ensure that business procedures are followed.

c) Information systems are required to process the data generated and used in business operations. OSS produces a variety of information for internal and external use.

d) Its role is to effectively process business transactions, control industrial processes, support enterprise communications and collaborations and update corporate database.

e) The main objective of OSS is to improve the operational efficiency of the enterprise. These are further categorized as follows:

Management-Level Systems:

a) These support the middle managers in monitoring, decision-making and administrative activities and are helpful in answering questions like - Are things working well and in order?

b) These provide periodic reports rather than instant information on operations. For example - a college control system gives report on the number of leaves availed by the staff, salary paid to the staff, funds generated by the fees, finance planning etc.

c) These types of systems mainly answer "what if" questions. For example - What would be quality of teaching if college must achieve top ranking in academics?

d) These types of questions can be answered only after getting new data from outside the organization, as well as data from inside which cannot be easily obtained from existing operational level systems. Management Information System and Decision Support Systems are types of Management Level systems.

QUESTIONS FOR ACADEMIC INTEREST – FOR STUDENT SELF STUDY

Q.No.54 What do you understand by a Decision Support System (DSS)? Briefly explain three characteristics of a DSS. [C] (RTP – M 14)

Decision Support System (DSS): 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/ semi-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 major characteristics of a Decision Support System namely:

(i) Semi-structured or unstructured decision-making;

(ii) Adaptable to the changing needs of decision makers; and

(iii) Ease of learning and use.

These are briefly discussed as follows:

(i) **Semi-structured 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 semi-structured 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:** Semi-structured 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 readable documentation. These interfaces make it easier for users to conceptualize and perform the decision-making process.

THE END

3. PROTECTION OF INFORMATION SYSTEMS

Q.No.1. What is information system security? (C)

1. Information Systems (IS) Security relates to the protection of valuable Information Systems Assets against loss, disclosure, or damage.
2. Organizations are increasingly relying on Information Technology (IT) for information and transaction processing.
3. The growth of E-commerce supported by the growth of the Internet has completely revolutionized and generated need for reengineered business processes.
4. In reality, the technology-enabled and technology-dependent organizations are more vulnerable to information security threats than ever before.

Q.No.2. Explain the need for protection of information systems? (A) (N16 MTP1)

1. There are many direct and indirect risks relating to the information systems. These risks have led to a gap between the need to protect systems and the degree of protection applied.
2. **This gap is caused by:**
   - **a)** Widespread use of technology;
   - **b)** Interconnectivity of systems;
   - **c)** Elimination of distance, time, and space as constraints;
   - **d)** Unevenness of technological changes;
   - **e)** Devolution of management and control;
   - **f)** Attractiveness of conducting unconventional electronic attacks over more conventional physical attacks against organizations; and
   - **g)** External factors such as legislative, legal, and regulatory requirements or technological developments.

Q.No.3. What form of threat arises to information security? (B)

1. Threats to information systems may arise from intentional or unintentional acts and may come from internal or external sources.
2. The threats may emanate from, among others,
   - **a)** Technical conditions (program bugs, disk crashes),
   - **b)** Natural disasters (fires, floods),
   - **c)** Environmental conditions (electrical surges),
   - **d)** Human factors (lack of training, errors, and omissions),
   - **e)** Unauthorized access (hacking) or viruses.
3. In addition to these, other threats, such as business dependencies (reliance on third party communications carriers, outsourced operations, etc.) that can potentially result in a loss of management control and oversight are increasing in significance.

Q.No.4. What are the objectives of information security? (B) (M15 RTP)

1. The objective of information system security is "the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity".
2. **For any organization, the security objective comprises three universally accepted attributes:**
   a) **Confidentiality:** Data and information are disclosed only to those who have a right to know it
   b) **Integrity:** Data and information are protected against unauthorized modification
   c) **Availability:** Information systems are available and usable when required

Q.No.5. What kind of information is considered sensitive by a business organization? Discuss the factors that should be considered while deciding about the level of protection needed for origination? (B)

The following examples highlight some of the factors, necessary for a company to succeed.

1. **Strategic Plans:**
   a) Most organizations readily acknowledge that strategic plans are crucial to the success of a company. But most of the companies fail to really make an effort to protect these plans.
   b) For example, a competitor learns that a company is testing a new product line in a specific geographic location.
2. **Business Operations:**
   a) Business operations consist of an organization's process and procedures, most of which are deemed to be proprietary.
   b) They provide a market advantage to the organization.
3. **Finances:**
   a) Financial information, such as salaries and wages, are very sensitive and should not be made public.
   b) While general salary ranges are known within industry sectors, precise salary information can provide a competitive edge. This information if available can help competitive enterprises to understand and reconfigure their salary structure accordingly.

Q.No.6. What is Information Security Policy? (C)

1. An information security policy is the statement of intent by the management about how to protect a company's information assets.
2. Information security policy is a document that describes an organization's information security controls and activities.
3. The policy does not specify technologies or specific solutions.
4. It defines a specific set of intentions and conditions that help protect a company's information assets and ability to conduct business.
5. It provides guidance to the people, who build, install, and maintain information systems.
6. **Information Security policy invariably includes rules intended to:**
   a) Preserve and protect information from any unauthorized modification, access or disclosure;
   b) Limit or eliminate potential legal liability from employees or third parties; and

c) Prevent waste or inappropriate use of the resources of an organization.

7. An information security policy should be in written form.

8. It provides instructions to employees about 'what kinds of behavior or resource usage are required and acceptable', and about 'what is unacceptable'.

Q.No.7. The information security policy of an organization has been defined and documented as given below:
"Our organization is committed to ensure information security through established goals and principles. Responsibilities for implementing every aspect of specific applicable proprietary and general principles, standards and compliance requirements have been defined. This is reviewed at least once a year for continued suitability with regard to cost and technological changes." Discuss information security policy and also identify the salient components that have not been covered in the above policy. (B) (PM, N15, J09)

Security Policy:

1. A Policy is a plan or course of action, designed to influence and determine decisions, actions and other matters.

2. The security policy is a set of laws, rules, and practices that regulates how assets including sensitive information are managed, protected, and distributed within the user organization.

3. An information Security policy addresses many issues such as disclosure, integrity and availability concerns.

Issues to address:

This policy does not need to be extremely extensive, but clearly state senior management's commitment to information security, be under change and version control and be signed by the appropriate senior manager. The policy should at least address the following issues:

a) A definition of information security,

b) Reasons why information security is important to the organization, and its goals and principles,

c) A brief explanation of the security policies, principles, standards and compliance requirements,

d) Definition of all relevant information security responsibilities, and reference to supporting documentation.

e) The auditor should ensure that the policy is readily accessible to all employees and that all employees are aware of its existence and understand its contents.

f) The policy may be a standalone statement or part of more extensive documentation that defines how the information security policy is implemented in the organization.

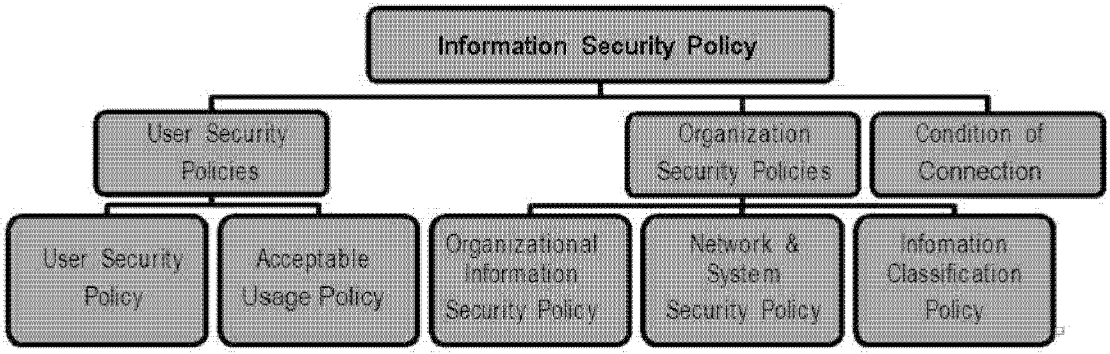
g) The auditor should also ensure that the policy has an owner who is responsible for its maintenance and that it is updated responding to any changes affecting the basis of the original risk assessment.

(Define IS policy. What are the major issues that are addressed by the IS policy?) (M16 - 4M, N16 MTP1)

In the stated scenario of the question, the ISMS Policy of the given organization does not address the following issues:

- Definition of information security,
- Reasons why information security is important to the organization,
- A brief explanation of the security policies, principles, standards and compliance, and
- Reference to supporting documents.

Q.No.8. Write short notes on the hierarchy of Information Security Policies? (N08, 11, N16 RTP) (OR) Discuss Various Types of Information Security Polices and their Hierarchy. (A) (PM)


Information Security Policy
User Security Policies
Organization Security Policies
Condition of Connection
User Security Policy
Acceptable Usage Policy
Organizational Information Security Policy
Network & System Security Policy
Infomation Classification Policy

The Hierarchy of Information Security Policies

<u>**INFORMATION SECURITY POLICY:**</u> This policy provides a <u>definition</u> of Information Security, its overall objective and the importance that <u>applies to all users</u>. Various types of information security policies are:

a) <u>**User Security Policies**</u> – These include User Security Policy and Acceptable Usage Policy

i) **User Security Policy:** This policy sets out the <u>responsibilities and requirements</u> for all IT system users. It provides <u>security</u> terms of <u>reference</u> for Users, Line Managers and <u>System Owners</u>.

ii) **Acceptable Usage Policy:** This sets out the policy for <u>acceptable</u> use of email and <u>Internet services.</u>

b) <u>**Organization Security Policies**</u> – These include Organizational Information Security Policy, Network & System Security Policy and Information Classification Policy

i) **Organizational Information Security Policy:** This policy sets out the Group policy for the security of its information assets and the Information Technology (IT) <u>systems processing</u> this information. Though it is positioned at the bottom of the <u>hierarchy</u>, it is the main IT <u>security policy document</u>.

ii) **Network & System Security Policy:** This policy sets out detailed policy for <u>system and network security</u> and applies to IT <u>department users</u>.

iii) **Information Classification Policy:** This policy sets out the policy for the <u>classification of information.</u>

c) <u>**Conditions of Connection:**</u> This policy sets out the Group policy for connecting to their network. It applies to all organizations <u>connecting</u> to the Group, and relates to the conditions that apply to <u>different suppliers' systems</u>.

Q.No.9. What are the key components of a good IS policy? Explain in brief. (A) (PM, N15 - 6M, M16 RTP, N14 RTP, N15 MTP2,M17 MTP)

A good security policy should clearly state the following:

a) Purpose and Scope of the Document and the intended audience,

b) The Security Infrastructure,

c) Security policy document maintenance and compliance requirements,

d) Incident response mechanism and incident reporting,

e) Security organization Structure,

f) Inventory and Classification of assets,

g) Description of technologies and computing structure,

h) Physical and Environmental Security,

i) Identity Management and access control,

j) IT Operations management,

k) IT Communications,

l) System Development and Maintenance Controls,

m) Business Continuity Planning,

n) Legal Compliances,

o) Monitoring and Auditing Requirements

p) Underlying Technical Policy.

Q.No.10. Define information systems control and Information Systems Auditing? (C)

Information system controls:

a) Controls are the Policies, Procedures, Practices and Organizational Structures, Designed to Provide Reasonable Assurance that Business Objectives will be achieved and that Undesired Events will be Prevented or Detected and Corrected.

b) Controls pertaining specifically to the Information Systems are referred as Information Systems Controls.

Information Systems Auditing: It is the process of attesting Objectives that focus on asset safeguarding and data integrity and Management Objectives that include not only attest objectives but also effectiveness and efficiency objectives.

Q.No.11. Explain the need for controls in Information Systems? (B)

1. Today's dynamic global enterprises need information integrity, reliability and validity for timely flow of accurate information throughout the organization.

2. Safeguarding assets to maintain data integrity to achieve system effectiveness and efficiency is a significant control process.

3. A well designed information system should have controls built in for all its sensitive or critical sections.

4. IS control procedure may include:

- **a)** Strategy and direction,
- **b)** General Organization and Management,
- **c)** Access to IT resources, including data and programs,
- **d)** System development methodologies and change control,
- **e)** Operation procedures,
- **f)** System Programming and technical support functions,
- **g)** Qualify Assurance Procedures,
- **h)** Physical Access Controls,
- **i)** BCP and DRP,
- **j)** Network and Communication,
- **k)** Database Administration, and
- **l)** Protective and detective mechanisms against internal and external attacks.

Q.No.12. Explain major objectives of Information System Controls? (B)

1. The basic purpose of information system controls in an organization is to ensure that the business objectives are achieved and undesired risk events are prevented, detected and corrected.
2. This is achieved by designing and effective information control framework, which comprise policies, procedures, practices, and organization structure that gives reasonable assurances that the business objectives will be achieved.
3. **Objective of Controls:**

   a) The objective of controls is to reduce or if possible eliminate the causes of the exposure to potential loss.

   b) Exposures are potential losses due to threats materializing. All exposures have causes.

   c) Some categories of exposures are:

   i) Errors or omissions in data, procedure, processing, judgment and comparison;

   ii) Improper authorizations and improper accountability with regards to procedures, processing, judgment and comparison

   iii) Inefficient activity in procedures, processing and comparison.

   d) Some of the critical control lacking in a computerized environment are:

   i) Lack of management understanding of IS risks and related controls;

   ii) Absence or inadequate IS control framework

   iii) Absence of weak general controls and IS controls;

   iv) Lack of awareness and knowledge of IS risks and controls amongst the business users and even IT staff;

   v) Complexity of implementation of controls in distributed computing environments and extended enterprise s;

   vi) Lack of control features or their implementation in highly technology driven environments;

   vii) Inappropriate technology implementations or inadequate security functionality in technologies implemented.

   e) The control objectives serve two main purposes:

   i) Outline the policies of the organization as laid down by the management

   ii) A benchmark for evaluating whether control objectives are met.

Q.No.13. Discuss the impact of technology on internal controls? (A)
(M16 - 4M, M16 RTP, M16 MTP1, N15 MTP2)

1. **Competent and Trustworthy Personnel:** Personnel should have proper skill and knowledge to discharge their duties. Substantial power is often needed for identifying error and responsible for the computer-based information systems developed, implemented, operated, and maintained within organizations.
2. **Segregation of duties:**

   a) A key control in an information system. Segregation basically means that the stages in the processing of a transaction are split between different people, such that one person cannot process a transaction through from start to finish. **(M15 RTP)**

   b) In a computerized system, the auditor should also be concerned with the segregation of duties within the IT department.

3. **Authorization procedures:** In manual systems, auditors evaluate the adequacy of procedures for authorization of examining the work of employees. In computer systems, authorization procedures often are embedded within a computer program

4. **Adequate Documents and Records:** This includes written or typed explanations of actions taken on specific transactions. *In a manual system, adequate documents and records are needed to provide an audit trail of activities within the system. In computer systems, documents might not be used to support the initiation, execution, and recording of some transactions.*

5. **Physical Control over Assets and Records:** Physical control over access and records is critical in both manual systems and computer systems. In the manual systems, protection from unauthorized access was through the use of locked doors and filing cabinets. Computerized financial systems have not changed the need to protect the data.

6. **Adequate Management Supervision:** This refers to review of specific work by a supervisor but this control requires a sign -off on the documents by the supervisor. In computer system, however, data communication facilities can be used to enable employees to be closer to the customers they service. Thus supervision of employees might have to be carried our remotely. The Management's supervision and review helps to deter and detect both errors and fraud.

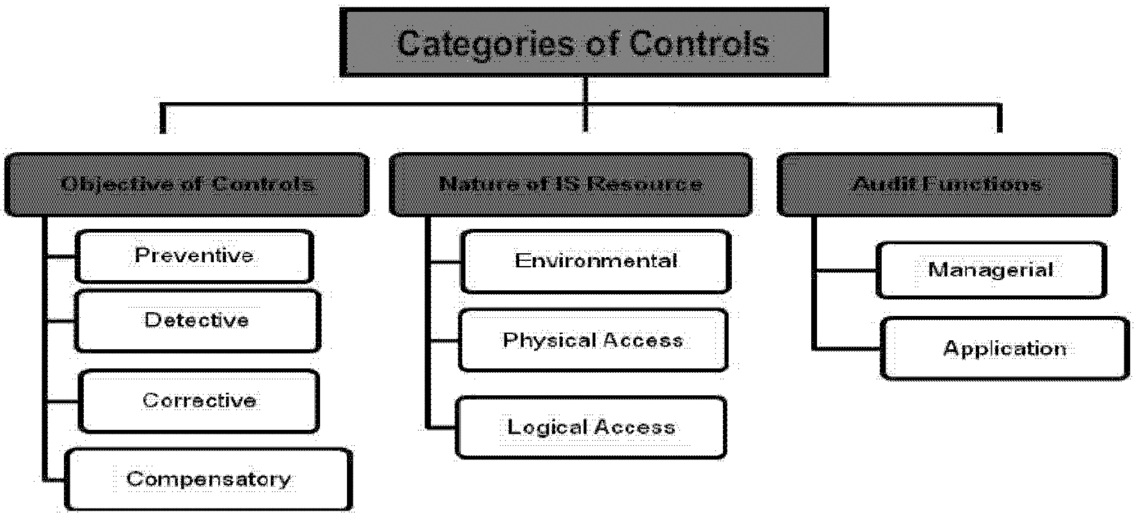
7. **Independent Checks on Performance:** Computer programs are authorized, accurate, and complete, the system will always follow the designated procedures.

8. **Comparing Recorded Accountability with Assets:** Data and the assets that the data purports to represent should periodically be compared to determine whether incompleteness or inaccuracies in the data exist or whether shortages or excesses in the assets have occurred

9. **Delegation of Authority and Responsibility:** A clear line of authority and responsibility is an essential control in both manual and computer systems. In a computer system, however, delegating authority and responsibility in an unambiguous way might be difficult because some resources are shared among multiple users.

Q.No.14. List out the various categories of Controls? (B)

1. Internal controls can be classified into various categories to illustrate the interaction of various groups in the enterprise and their effect on computer controls.
2. These categories are:



Q.No.15. Write short notes on the types of control based on the objectives of controls? (A) (PM)

1. **Preventive controls:** These are controls which are designed to prevent an error, omission or malicious act occurring.
2. An example of a preventive control is the use of passwords to gain access to a financial system.
3. These can be implemented in both manual and computerized environment for the same purpose.

   a) **Characteristics:**

   i) Understanding vulnerabilities of the asset is required

   ii) Understanding of probable threats is required

   iii) Provision of necessary controls for preventing probable threats from materializing and exploiting the vulnerabilities

   b) **Examples of preventive controls:**

   i) Employ qualified personnel

   ii) Segregation of duties

   iii) Access control

   iv) Documentation

   v) Validation, edit checks in the application

   vi) Anti-virus software (sometimes this acts like a corrective control also), etc

   vii) User instruction manuals.

   viii) Prescribing appropriate books for a course,

   ix) Training and retraining of staff,

   x) Authorization of transaction,

   xi) Firewalls,

   xii) Passwords.

(What do you mean by Preventive controls? Explain it with the help of examples, also indicate their broad characteristics in brief?)

4. **Detective Controls:** These are designed to detect errors, omissions or malicious acts that occur and report the occurrence. **(N16 - 4M, M16 RTP,M17 RTP, M16 MTP1, N16 MTP2)**

   a) **Characteristics:**

   i) Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc.

   ii) An established mechanism to refer the reported unlawful activities to the appropriate person or group

   iii) Interaction with the preventive control to prevent such acts from occurring

   iv) Surprise checks by supervisor.

   b) **Examples of detective controls:**

   i) Hash totals

   ii) Duplicate checking of calculations

   iii) The internal audit functions

   iv) Bank reconciliation

   v) Monitoring expenditures against budgeted amount.

5. **Corrective Controls:** These are designed to reduce the impact or correct an error once it has been detected. **(Refer Q - 16)**

6. **Compensatory Controls:** **(N16 RTP, M16 MTP2)**

   i) Controls are basically designed to reduce the probability of threats, which can exploit the vulnerabilities of an asset and cause a loss to that asset.

   ii) While designing the appropriate control one thing should be kept in mind - "The cost of the lock should not be more than the cost of the assets it protects."

   iii) Sometimes, while designing and implementing controls, organizations because of different constraints like financial, administrative or operational, may not be able to implement appropriate controls.

   iv) In such a scenario, there should be adequate compensatory measures, which may although not be as efficient as the appropriate control, but reduce the probability of loss to the assets. Such measures are called compensatory controls.

Q.No.16. Do you consider Corrective Controls are a part of Internal Controls/ Describe the characteristics of Corrective Controls. (M15 - 6M, N16 RTP, M16 RTP, M15 RTP)

(OR)

What do you mean by Corrective controls? Explain it with the help of examples. Also indicate their broad characteristics in brief? (A) (PM)

a) Yes, we consider Corrective Controls to be a part of Internal Controls.

b) Corrective controls are designed to reduce the impact or correct an error once it has been detected.

c) Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date.

d) **Characteristics**:

   i) Minimizing the impact of the threat;

   ii) Identifying the cause of the problem;

   iii) Providing remedy to the problems discovered by detective controls;

   iv) Getting feedback from preventive and detective controls;

   v) Correcting error arising from a problem

   vi) Modifying the processing systems to minimize future occurrences of the incidents.

e) **Examples of Corrective Controls:**

   i) Contingency planning

   ii) Backup procedure

   iii) Rerun procedures

   iv) Treatment procedures for a disease

   v) Change input value to an application system

   vi) Investigate budget variance and report violations.

Q.No.17. Write short notes on the types of controls based on the nature of IS resources? (B)

Types of controls based on the "Nature of Information System Resources" are as follows:

a) **Environmental controls:** Controls relating for housing IT resources such as power, air-conditioning, UPS, smoke detection, fire-extinguishers, dehumidifiers etc.

b) **Physical Access Controls:**

i) Controls relating to physical security of the tangible IS resources and intangible resources stored on tangible media etc.

ii) Such controls include Access control doors, Security guards, door alarms, restricted entry to secure areas, visitor logged access, video monitoring etc.

c) **Logical Access Controls:** Controls relating to logical access to information resources such as operating systems controls, Application software boundary controls, networking controls, access to database objects, encryption controls etc.

Q.No.18. What are the Environmental issues and exposures with respect to Environmental controls. (B)

Environmental issues and Exposures;

- Environmental exposures are primarily due to elements of nature. However, with proper controls, exposures can be reduced.
- Common occurrences are Fire, Natural disasters-earthquake, volcano, hurricane, tornado, Power spike, Air conditioning failure, Electrical shock, Equipment failure, Water damage/flooding-even with facilities located on upper floors of high buildings.
- Water damage is a risk, usually from broken water pipes, and Bomb threat/attack.

Other environmental issues and revelations include the following:

- *Is the power supply to the compiler equipment properly controlled so as to ensure that it remains within the manufacturer's specification?*
- *Are the air conditioning, humidity and ventilation control systems protected against the effects of electricity using static rug or anti -static spray?*
- *Is consumption of food, beverage and tobacco products prohibited, by policy around computer equipment?*
- *Are backup media protected from damage due to variation in temperatures or are they guarded against strong magnetic fields and water damage?*
- *Is the computer equipment kept free from dust, smoke and other particulate matter?*

Q.No.19. What are the categories of Information Systems resources from the perspective of environmental exposures and controls. (B)

From the perspective of environmental exposures and controls, information systems resources may be categorized as follows, with the focus primarily on facilities which house:

1. **Hardware and Media:** Includes Computing Equipment, Communication equipment, and Storage Media.
2. **Information Systems Supporting Infrastructure or Facilities:**

a) Environmental Issues and exposures includes Audit and Evaluation Techniques for Environmental Controls

b) This typically includes the following:

i) Physical Premises, like Computer Rooms, Cabins, Server Rooms/Farms, Data Centre premises, Printer Rooms, Remote facilities and Storage Areas

ii) Communication Closets

iii) Cabling ducts

iv) Power Source

v) Heating, Ventilation and Air Conditioning (HVAC)

3. **Documentation:** Physical and geographical documentation of computing facilities with emergency excavation plans and incident planning procedures.
4. **Supplies:** The third party maintenance procedures for say air-conditioning, fire safety, and civil contractors whose entry and assess with respect to their scope of work assigned are to be monitored and logged.
5. **People:** The employees, contract employees, visitors, supervisors and third party maintenance personnel are to be made responsible and accountable for environmental controls in their respective information processing facility (IPF). Training of employees and other stake holders on control procedures is a critical component.

Q.No.20. Explain the different controls for environment exposures/risks? (B)

Environmental Exposures	Meaning	Controls for Environmental Exposures
Fire Damage	It is a major threat to the physical security of a computer installation.	Ref. Q. No : 21
Power Spikes	This is caused due to a very short pulse of energy in a power line.	Ref. Q. No : 22
Water Damage	Water damage to a computer installation can be the outcome of water pipes burst. Water damage may also result from other resources such as cyclones, tornadoes, floods etc	Ref. Q. No : 21
Pollution Damage & others	Major pollutant in a computer installation is dust.	Ref. Q. No : 23

Q.No.21. Discuss the arrangements a company XYZ should emphasize in order to tighten its Physical Security for protecting its IT assets. (B) (N15 RTP)

Physical Security: The security required for computer system can be categorized as security from Accidental Breach and Incidental Breach.

- Accidental breach of security due to such natural calamities as fire, flood and earthquake etc. may cause total destruction of important data and information.
- Incidental or fraudulent modification or tampering of financial records maintained by the organization can cause considerable amount of money to be disbursed to fraudulent personnel.
- Physical security includes the following arrangements:

1. **Fire Damage:**

[Explain various environmental exposures and controls with respect to fire damage] (M17 RTP)

It is a major threat to the physical security of a computer installation. Some of the major features of a well-designed fire protection system are:

a) Both automatic, manual fire alarms and fire extinguishers are placed at strategic locations;

b) A control panel may be installed which shows where in the location an automatic or manual alarm has been triggered;

c) Fire exits should be clearly marked. *When a fire alarm is activated, a signal may be sent automatically to permanently manned station*;

d) All staff should know how to use the systems such as Fire Alarms, Extinguishers, and Sprinklers etc.

e) Less Wood and plastic should be in computer rooms.

f) Regular Inspection by Fire Department should be conducted.

g) Fire repression systems should be supplemented and not replaced by smoke detectors.

2. **Water Damage:**

[During the equipment installation in ABC shopping mall, its construction contractor wishes to ensure that the installation is protected against any kind of water damage. Discuss some of the major ways with which the same can be achieved. (OR) Explain various environmental exposures and controls with respect to water damage]

a) Water damage to a computer installation can be the outcome of water pipes burst. Water damage may also result from other resources such as cyclones, tornadoes, floods etc.

b) Some of the major ways of protecting the installation against water damage are:

i) Use of waterproof ceilings, walls and floors;

ii) Ensure an adequate positive drainage system exists;

iii) Install alarms at strategic points.

iv) Installation at the upper floors or top floors of a building;

v) Use a gas based fire suppression system;

3. **Power Supply Variation:**

a) Voltage regulators and circuit breakers used to protect the hardware from temporary increase or decrease of power.

b) UPS Battery back-up can be provided in case a temporary loss of power occurs. A generator is needed for sustained losses in power for extended period.

4. **Pollution Damage**: The major impurity in a computer installation is dust. Due consideration should be given for dust free environment in the computer room. Regular cleaning of walls, floors and equipment etc. is esential.

5. **Unauthorized Intrusion:**

a) Physical entry may be restricted to the computer room by various means so that unauthorized intrusion does not take place.

b) A badge system may be used to identify the status of personnel inside the computer room.

Q.No.22. Explain various environmental exposures and controls with respect to power spikes. (B)

Power Spikes: This is caused due to a very short pulse of energy in a power line.

Some of the major ways of protecting the installation against power spikes as follows:

a) **Uninterruptible Power System (UPS)/Generator:** In case of a power failure, the UPS provides the back up by providing electrical power from the battery to the computer for a certain span of time.

b) **Power Supply Variation:** Voltage regulators and circuit breakers protect the hardware from temporary increase or decrease of power.

c) **Emergency Power - Off Switch:** When the need arises for an immediate power shut down during situations like a computer room fire or an emergency evacuation, an emergency power-off switch at the strategic locations would serve the purpose. *They should be easily accessible and yet secured from unauthorized people.*

Q.No.23. Explain various environmental exposures and controls with respect to pollution damage and others? (B)

The major pollutant in a computer installation is dust. Dust caught between the surfaces of magnetic tape / disk and the reading and writing heads may cause either permanent damage to data or read/ write errors.

a) **Documented and Tested Emergency Evacuation Plans:** Relocation plans should emphasize human safety, but should not leave information processing facilities physically unsecured. Procedures should exist for a controlled shutdown of the computer in an emergency situation. In all circumstances saving human life should be given paramount importance.

b) **Power Leads from Two Substations:** Electrical power lines that are exposed to many environmental dangers such as water, fire, lightning, cutting due to careless digging etc. To avoid these types of events, redundant power links should feed into the facility. Interruption of one power supply does not adversely affect electrical supply.

c) **Prohibitions against Eating, Drinking and Smoking within the Information Processing Facility:** These activities should be prohibited from the information processing facility. This prohibition should be clear, e.g. a sign on the entry door.

Q.No.24. What are Physical access controls? (B)

1. Physical access controls are the controls which are designed to protect information system resources from physical access issues and exposures.
2. Issues convered under these controls are:
   a) Physical Access Issues and Exposures
   b) Physical Access Exposure Controls

Q.No.25. What are the effects of violation of Physical Access Paths? (B)

1. Abuse of data processing resources
2. Blackmail
3. Embezzlement
4. Abuse of data processing resources.
5. Damage, vandalism or theft to equipments or documents.
6. Modification of equipment and information.
7. Public disclosure of sensitive information.
8. Unauthenticated entry.

Q.No.26. List out the possible Perpetrators who may violate Physical access? (B)

Possible perpetrators: Perpetrations may be because of employees who are:

a) Accidental ignorant-someone who outrageously violates rules

b) Addicted to a substance or gambling

c) Former employee

d) Discontented

e) Interested or informed outsiders, such as competitors, thieves, organized crime and hackers

f) Experiencing financial or emotional problems

g) Notified their termination

h) On strike

i) Threatened by disciplinary action or dismissal.

Q.No.27. List out the other areas of exposures to confidential matters with respect to physical access issues and exposures. (B)

Exposures to confidential matters may be in form the unaware, accidental or anonymous persons, although the greatest impact may be from those with malicious intent. Other areas of concern include the following:

i) How far the hardware facilities are controlled to reduce the risk of unauthorized access?

ii) Are the hardware facilities protected against forced entry?

iii) Are intelligent computer terminals locked or otherwise secured to prevent illegal removal of physical components like boards, chips and the computer itself?

iv) When there is a need for the removal of computer equipment from its normal secure surroundings, are authorized equipment passes required for the removal?

Q.No.28. List out the IS facilities that need to be protected from Physical access control violations from auditor's perspective? (B)

The facilities that need to be protected from the auditor's perspective are:

a) Computer room

b) Micro computers /personal computers

c) Local area networks

d) Portable equipment

e) Power sources

f) Programming area

g) Storage rooms and supplies

h) Tape library, tapes, disks and all magnetic media

i) Telecommunications equipment

j) Telephone lines

k) Off-site backup file storage facility

l) On-site and remote printers

m) Operator consoles and terminals.

Q.NO.29. Discuss locks on doors with respect to controls for physical access exposures in brief? (A) (PM)

1. **Cipher locks (Combination Door Locks):** The cipher lock consists of a pushbutton panel that is mounted near the door outside of a secured area. There are ten numbered buttons on the panel. To enter, a person presses a four digit number sequence, and the door will unlock for a predetermined period of time, usually ten to thirty seconds.

2. **Bolting Door Locks:** A special metal key is used to gain entry when the lock is a bolting door lock. To avoid illegal entry the keys should be not be duplicated.

3. **Electronic Door Locks:** A magnetic or embedded chip-based plastics card key or token may be entered into a sensor reader to gain access in these systems. The sensor device upon reading the special code that is internally stored within the card activates the door locking mechanism.

   Advantages electronic door locks over bolt and combinational locks: [M16 - 4M]

   a) Through the special internal code, cards can be made to identity the correct individual.

   b) Individuals access needs can be restricted through the special internal code and sensor devices.

c) Degree of duplication is reduced.

d) Card entry can be easily deactivated in the event an employee is terminated or a card is lost or stolen.

e) *If unauthorized entry is attempted silent or audible alarms can be automatically activated.*

f) An administrative process, which may deal with Issuing, accounting for and retrieving the card keys, are also, parts of security. The card key becomes an important item to retrieve when an employee leaves the firm.

4. **Biometric Door Locks:** These locks are extremely secure where an individual's unique body features, such as voice, retina, fingerprint or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected, such as in the military.

Q.No.30. Explain the various types of Physical identification media as a part of Controls for Physical access exposures? (B)

Physical identification medium:

1. **Personal Identification numbers (PIN):** A secret number will be assigned to the individual, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual. The visitor will be asked to log on by inserting a card in some device and then enter their PIN via a PIN keypad for authentication. His entry will be matched with the PIN number available in the security database.
2. **Plastic Cards:** These cards are used for identification purposes. Controls over card seek to ensure that customers need to safeguard their card if does not fall into unauthorized hands.
3. **Identification Badges:** Special identification badges can be issued to personnel as well as visitors.

   a) Sophisticated photo of IDs can also be utilized as electronic card keys.

   b) Issuing accounting for and retrieving the badges administrative prices that must carefully controlled.

Q.No.31. Explain various types of Logging on utilities in the context of Physical access control? (C)

1. **Manual Logging:** All visitors should be prompted to sign a visitor's log indicating their name, company represented, their purpose of visit, and person to see.

   a) Logging may happen at both the front reception and entrance to the computer room.

   b) A valid and acceptable identification such as a driver's license, business card or vendor identification tag may also be asked for before gaining entry inside the company.

2. **Electronic Logging:** This feature is a combination of electronic and biometric security systems. The users logging in can be monitored and the unsuccessful attempts being highlighted.

Q.No.32. Besides locks on door, Physical identification medium and logging on facilities explain other methods of controlling Physical access? (B)

1. **Video Cameras:** Cameras should be placed at specific locations and monitored by security guards. Refined video cameras can be activated by motion. The video supervision recording must be retained for possible future play back.
2. **Security Guards:** Extra security can be provided by appointing guards aided with video cameras and locked doors. Guards supplied by an external agency should be made to sign a bond to protect the organization from loss.

3. **Controlled Visitor Access:** A responsible employee should escort all visitors. Visitors may be friends, maintenance personnel, computer vendors, consultants and external auditors.

4. **Bonded Personnel:** All service contract personnel, such as cleaning people and off-site storage services, should be asked to sign a bond. This may not be a measure to improve physical security but to a certain extent can limit the financial exposure of the organization.

5. **Dead man Doors:** These systems encompasses are a pair of doors that are typically found in entries to facilities such as computer rooms and document stations. The first entry door must close and lock, for the second door to operate, with the only person permitted in the holding area. Only a single person is permitted at a given point of time and this will surely reduce the risk of piggybacking, when an unauthorized person follows an authorized person through a secured entry.

6. **Non-exposure of Sensitive Facilities:** There should be no explicit indication such as presence of windows of directional signs hinting the presence of facilities such as computer rooms. Only the general location of the information processing facility should be identifiable.

7. **Computer Terminal Locks:** These locks ensure that the device to the desk is not turned on or disengaged by unauthorized persons.

8. **Controlled Single Entry Point:** All incoming personnel can use controlled Single Entry Point. A controlled entry point is monitored by a receptionist. Multiple entry points increase the chances of unauthorized entry. Unnecessary or unused entry points should be eliminated or deadlocked.

9. **Alarm System:** Illegal entry can be avoided by linking alarm system to inactive entry point motion detectors and the reverse flows of enter or exit only doors, so as to avoid illegal entry. Security personnel should be able to hear the alarm when activated.

10. **Perimeter Fencing:** Fencing at boundary of the facility may also enhance the security mechanism.

11. **Control of out of hours of employee-employees:** Employees who are out of office for a longer duration during the office hours should be monitored carefully. Their movements must be noted and reported to the concerned officials frequently.

12. **Secured Report/ Document Distribution cart:**- Secured carts such as mail carts, must be covered and locked and should always be attended.

Q.No.33. What are Logical access controls? (B)

1. Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted.

2. Assessing logical access controls involves evaluating the following critical procedures :

   a) Logical access controls restrict users to authorized transactions and functions.

   b) There are logical controls over network access.

   c) There are controls implemented to protect the integrity of the application and the confidence of the public when the public accesses the system.

Q.No.34. Explain the control aspects retaining to Logical access paths? (A)

1. **Online Terminals:** To access an online terminal a user has to provide a valid logon-ID and password. If additional authentication mechanisms are added along with the password, it will strengthen the security.

2. **Operator Console:**

   a) The operator console is one of the crucial places where any intruders can play havoc.

b) Hence, access to operator console must be restricted. This can be done by

i) Keeping the operator console at a place, which is visible, to all?

ii) By keeping the operator console in a protected room accessible to selected personnel.

3. **Dial-up Ports:**

a) Using a dial up port user at one location can connect remotely to another computer present at an unknown location via a telecommunication media.

b) A modem is a device, which can convert the digital data transmitted to analog data (the one that the telecommunication device uses). Thus the modem can act as an interface between remote terminal and the telephone line.

c) Security is achieved by providing a means of identifying the remote user to determine authorization to access. A dial back line ensures security by confirming the presence and exactness of the data sent.

4. **Telecommunication Network:** In a Telecommunication network a number of computer terminals, Personal Computers etc. are linked to the host computer through network or telecommunication lines. Whether the telecommunication lines could be private (i.e., dedicated to one user) or public, security is provided in the same manner as it is applied to online terminals.

Q.No.35. Logical access Issues and Exposures? (B)

1. Controls that reduce the risk of misuse (intentional or unintentional), theft, alteration or destruction should be used to protect unauthorized and unnecessary access to computer files.
2. Restricting and monitoring computer operator activities in a batch -processing environment provide this control.
3. The opportunities of access in an online system, is more; hence, the level of control for this system must be more complex.
4. Access control mechanisms should be applied not only to computer operators but also to end users programmers, security administrators, management or any other authorized users.
5. Access control mechanisms should provide security to the following applications:

a) Access control software,

b) Application software,

c) Data

d) Data dictionary/directory,

e) Dial-up lines

f) Libraries

g) Logging files

h) Operating systems Password library

i) Procedure libraries

j) Spool queues

k) System software

l) Tape files,

m) Telecommunication lines,

n) Temporary disk files

o) Utilities.

Q.No.36. Explain the different types of Technical exposures/ Threats in relation to logical access? (A) (RTP – N14) (PM)

Technical exposure: Technical exposures include unauthorized implementation or modification of data and software. Technical exposures include the following:

a) **Data Diddling:** Data diddling involves the change of data before or as they are entered into the system. A limited technical knowledge is required to data diddle and the worst part with this is that it occurs before computer security can protect data.

b) Bomb: Bomb is a piece of bad code deliberately planted by an insider or supplier of a program. An event, which is logical, triggers a bomb or time based. The bombs explode when the conditions of explosion get fulfilled causing the damage immediately. However, these programs cannot infect other programs. **(M17- 4M)**

c) Time Bomb: The computer time bomb causes a perverse activity, such as, disruption of computer system, modifications, or destructions of stored information etc. on a particular date and time for which it has been developed. The computer clock initiates it.

d) Logic Bomb: They resemble time bombs in their destruction activity. Logic bombs are activated by combination of events. For example, a code like; "If a file named DELETENOT is deleted then destroy the memory contents by writing ones." This code segment, on execution,may cause destruction of the contents of the memory on deleting a file named DELETENOT. These bombs can be set to go off at a future event.

e) Trojan Horse: **(N14 RTP)**

i) These are malicious programs that are hidden under any authorized program.

ii) A Trojan horse is an illicit coding contained in a legitimate program, and causes an illegitimate action.

iii) A Trojan may:

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

iv) A Trojan Horse program is an apparently useful program, or command procedure, containing hidden code which performs unwarranted function when it is invoked.

v) *An author of a Trojan horse might first create or gain access to the source code of a useful program that is attractive to other users and then add a harmful code so that the program performs some harmful function in addition to its useful function.*

f) Worms:

i) A Worm is a program that burrows into the computer's memory and replicates into areas of idle memory.

ii) Worm systematically occupies idle memory until the MEMORY IS EXHAUSTED and the system fails.

iii) Limited in damage, as the network traffic they generate grows so exponentially that they can are quickly identified and blocked.

iv) Worms can also be used to perform some useful tasks. For example, worms can be used in the installation of a network. A worm can be inserted in a network and we can check for its presence at each node. A node, which does not indicate the presence of the worm for quite some time, can be assumed as not connected to the network.

v) Examples of worms are Alarm clock Worm, which places wake-up calls on a list of users. It passes through the network to an outgoing terminal.

g) Rounding Down: This refers to rounding down of small fractions of a denomination and transferring these small fractions into an authorized account. As the amount is small, it gets rarely noticed.

h) Salami Techniques:

i) Slicing of small amounts of money from a computerized transaction or account.

ii) Difference from Rounding Down: A Salami technique is slightly different from a rounding technique in the sense only last few digits are rounded off here. For example, in the rounding down technique, Rs. 21,23,456.39 becomes Rs. 21,23,456.35, while in the Salami technique the transaction amount Rs. 21,23,456.39 is truncated to either Rs. 21,23,456.30 or Rs. 21,23,456.00, depending on the calculation.

i) **Trap Doors:** System programmers sometimes insert Code (Program) which compromises the usual controls, but only with a positive objective e.g. for debugging during system development/ system maintenance. These codes are generally removed after the activity. But, when they are not removed – they may become methods of system compromise.

Q.No.37. Explain the effect of computer crime exposures? (A) (N16 MTP2) (OR) 'Crimes are committed by using computers and can damage the reputation, morale and even the existence of an organization.' What are the problems do you think that any organization can face with the result of computer crimes? (PM, N15 - 6M)

1. Crimes that are committed using computers and the information they contain can damage the reputation, morale and existence of an organization.
2. Computer crimes generally result in Loss of customers, embarrassment to management and legal actions against the organizations.

   a) **Financial Loss:** Financial losses may be direct like loss of electronic funds or indirect like expenditure towards repair of damaged electronic components.

   b) **Legal Repercussions:** An organization has to adhere to many human rights laws while developing security policies and procedures. These laws protect both the perpetrator and organization from trial. The organizations will be exposed to lawsuits from investors and insurers if there are no proper security measures. The IS auditor should take legal counsel while reviewing the issues associated with computer security.

   c) **Loss of Credibility or Competitive Edge:** In order to maintain competitive edge, many companies, especially service firms such as banks and investment firms, needs credibility and public trust. This credibility will be shattered resulting in loss of business and prestige if security violation occurs.

   d) **Blackmail/industrial Espionage:** By knowing the confidential information, the perpetrator can obtain money from the organization by threatening and exploiting the security violation.

   e) **Disclosure of Confidential, Sensitive or Embarrassing Information:** These events can spoil the reputation of the organization. Legal or regulatory actions against the company are also a result of disclosure.

   f) **Sabotage:** People who may not be interested in financial gain but who want to spoil the credibility of the company or to will involve in such activities. They do it because of their dislike towards the organization.

   g) **Spoofing:**

      i) A spoofing attack involves forging one's source address. One machine is used to impersonate the other in spoofing technique.

      ii) Spoofing occurs only after a particular machine has been identified as vulnerable; A penetrator makes the user think that he is interacting with the operating system. For example, a penetrator duplicates the logon procedure, captures the user's password, attempts for a system crash and makes the user login again. It is only the second time the user actually logs into the system.

Q.No.38. What are Asynchronous attacks? Explain the various forms of asynchronous attacks? (A) (PM, N16 RTP, N14 RTP, M16 MTP2, M17 MTP)

Asynchronous Attacks

a) They occur in many environments where data can be moved asynchronously across telecommunication lines.

b) Numerous transmissions must wait for the clearance of the line before data being transmitted.

c) Data that are waiting to be transmitted are liable to unauthorized access called asynchronous attack. These attacks are hard to detect because they are usually very small pin like insertions.

d) There are many forms of **asynchronous attacks.**

i) **Data Leakage:** Data is critical resource for an organization to function effectively. Data leakage involves leaking information out of the computer by means of dumping files to paper or stealing computer reports and tape.

ii) **Wire-tapping:** This involves spying on information being transmitted over telecommunication network.

iii) **Piggybacking:**

- This is the act of electronically attaching to an authorized telecommunication link that intercepts and alters transmissions.
- This involves intercepting communication between the operating system and the user and modifying them or substituting new messages.
- A special terminal is tapped into the communication for this purpose.
- Computer users either who do not have their own connections or who are outside the range of their own might find someone else's and use that one.

iv) **Shut Down of the Computer/Denial of Service:**

- This is initiated through terminals or microcomputers that are directly or indirectly connected to the computer.
- Individuals who know the high-level systems log on-ID initiate shutting down process. When overloading happens some systems have been proved to be vulnerable to shutting themselves.
- Hackers use this technique to shut down computer systems over the Internet.

Q.No.39. Explain some of the key ways to control remote and distributed data processing applications with respect to issues and revelations related to Logical Access in brief? (B) (PM)

a) Remote access to computer and data files through the network should be implemented.

b) Having a terminal lock can assure physical security to some extent.

c) Applications that can be remotely accessed via modems and other devices should be controlled appropriately.

d) Terminal and computer operations at remote locations should be monitored carefully and verify frequently for violations.

e) In order to prevent unauthorized users from accessing the system, there should be proper control mechanisms over system documentation and manuals.

f) Data transmission over remote locations should be controlled.

g) When replicated copies of files exist at multiple locations it must be ensured that all identical copies contain the same information and checks are also implemented to ensure that duplicate data does not exist.

Q.No.40. Explain about Logical Access Violators. (B) (M17MTP)

Logical Access Violators are often the same people who exploit physical exposures, although the skills needed to exploit logical exposures are more technical and complex. They are mainly:

a) **Hackers:** Hackers try their best to overcome restrictions to prove their ability. Ethical hackers most likely never try to misuse the computer intentionally

b) **Employees** (authorized or unauthorized)

c) **IS Personnel:** They have easiest to access to computerized information since they come across to information during discharging their duties. Segregation of duties and supervision help to reduce the logical access violations

d) **Former Employees**: should be cautious of former employees who have left the organization on unfavorable terms

e) **End Users;** Interested or Educated Outsiders; Competitors; Foreigners; Organized Criminals; Crackers; Part-time and Temporary Personnel; Vendors and consultants; and Accidental Ignorant – Violation done unknowingly.

Q.No.41. Discuss Logical Access Controls across the system in brief. (B)

Logical Access Controls: The purpose of Logical Access Controls is to restrict access to information assets/resources. They are expected to provide access to information resources on a need to know and need to do basis using principle of least privileges. *It means that the access should not be so restrictive that it makes the performance of business functions difficult or it should not be so liberal that it can be misused i.e. it should be just sufficient for one to perform one□ s duty without any problem or restraint.*

The data, an information asset, can be:

a) Used by an application (Data at Process);

b) Stored in some medium (Back up) (Data at Rest); or

c) It may be in transit (being transferred from one location to another).

Q.No.42. Write about User Access Management and User Responsibilities with respect to logical access controls. (B)

User Access Management:

a) **User registration:** Information about every user is documented. For example: Why is the user granted the access?; Has the data owner approved the access? etc.

b) **Privilege management:** Access privileges are to be aligned with job requirements and responsibilities. For example, an operator at the order counter shall have direct access to order processing activity of the application system.

c) **User password management:** Passwords are usually the default screening point for access to **systems**. Allocations, storage, revocation, and reissue of password are password management functions.

d) **Review of user access rights:** A user's need for accessing information changes with time and requires a periodic review of access rights to check anomalies in the user's current job profile, and the privileges granted earlier.

User Responsibilities: User awareness and responsibility is also an important factor:

a) **Password use:** Mandatory use of strong passwords to maintain confidentiality.

b) **Unattended user equipment:** Users should ensure that none of the equipment under their responsibility is ever left unprotected. They should also secure their PCs with a password, and should not leave it accessible to others.

Q.No.43. Write about Network Access Controls with respect to logical access controls. (A)

Network Access Control: An Internet connection exposes an organization to the entire world this brings up the issue of benefits the organization should derive along with the precaution against harmful elements. This can be achieved through the following means:

a) **Policy on use of network services:** Selection of appropriate services and approval to access them aligned with the business need for using the Internet services is the first step.

b) **Enforced path:** Based on risk assessment, it is necessary to specify the exact path or route connecting the networks; e.g., internet access by employees will be routed through a firewall and proxy.

c) **Segregation of networks:** Based on the sensitive information handling function; say a VPN connection between a branch office and the head-office, this network is to be isolated from the internet usage service

d) **Network connection and routing control:** The traffic between networks should be restricted, based on identification of source and authentication access policies implemented across the enterprise network facility.

e) **Security of network services:** The techniques of authentication and authorization policy should be implemented across the organization's network.

f) **Firewall:**

i) A Firewall is a system that enforces access control between two networks. To accomplish this, all traffic between the external network and the organization's Intranet must pass through the firewall.

ii) Only authorized traffic between the organization and the outside is allowed to pass through the firewall. The firewall must be immune to penetrate from both outside and inside the organization.

iii) *In addition to insulating the organization's network from external networks, firewalls can be used to insulate portions of the organization's Intranet from internal access also.*

g) **Encryption:**

i) Encryption is the conversion of data into a secret code for storage in databases and transmission over networks.

ii) The sender uses an encryption algorithm and the original message called the clear text is converted into cipher text. This is decrypted at the receiving end. The encryption algorithm uses a key.

iii) The more bits in the key, the stronger are the encryption algorithms.

iv) Two general approaches are used for encryption viz. private key and public key encryption.

h) **Call Back Devices:**

i) It is based on the principle that the key to network security is to keep the intruder off the Intranet rather than imposing security measure after the criminal has connected to the intranet.

ii) The call- back device requires the user to enter a password and then the system breaks the connection. If the caller is authorized, the call back device dials the caller's number to establish a new connection.

iii) *This limits access only from authorized terminals or telephone numbers and prevents an intruder masquerading as a legitimate user. This also helps to avoid the call forwarding and man-in-the middle attack.*

i) **Recording of Transaction Log:** An intruder may penetrate the system by trying different passwords and user ID combinations. All incoming and outgoing requests along with attempted access should be recorded in a transaction log. The log should record the user ID, the time of the access and the terminal location from where the request has been originated.

Q.No.44. Write about Operating System Access Controls with respect to logical access controls. (A)

Operating System Access Control: Operating System is the computer control program. It allows users and their applications to share and access common computer resources, such as processor, main memory, database and printers.

Major tasks of O/S:

a) Scheduling Jobs;

b) Managing Hardware and Software Resources;

c) Maintaining System Security;

d) Enabling Multiple User Resource Sharing;

e) Handling Interrupts and Maintaining Usage Records.

f) Operating system security involves policy, procedure and controls that determine, 'who can access the operating system,' 'which resources they can access', and 'what action they can take'.

g) Operating System provides the platform for an application to use various Information System resources and perform the specific business function.

h) *If an intruder is able to bypass the network perimeter security controls, the operating system is the last barrier to be conquered for unlimited access to all the resources. Hence, protecting operating system access is extremely crucial.*

1. **Automated terminal identification:** This will help to ensure that a particular session could only be initiated from a particular location or computer terminal.

2. **Terminal log-on procedures:** A log-in procedure is the first line of defense against unauthorized access. The log-in procedure does not provide unnecessary help or information, which could be misused by an intruder. When the user initiates the log-on process by entering user-id and password, the system compares the ID and password to a database of valid users. If the system finds a match, then log-on attempt is authorized.

3. **Access Token:** If the log on attempt is successful, the Operating System creates an access token that contains key information about the user including user-id, password, user group and privileges granted to the user. The information in the access token is used to approve all actions attempted by the user during the session.

4. **Access Control List:** This list contains information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compasses his or her user-id and privileges contained in the access token with those contained in the access control list. If there is a match, the user is granted access.

5. **Discretionary Access Control:** The system administrator usually determines; who is granted access to specific resources and maintains the access control list. However, in distributed systems, resources may be controlled by the end-user. Resource owners in this setting may be granted discretionary access control, which allows them to grant access privileges to other users. *For example, the controller who is owner of the general ledger grants read only privilege to the budgeting department while accounts payable manager is granted both read and write permission to the ledger.*

6. **User identification and authentication:** The users must be identified and authenticated in a foolproof manner. Depending on risk assessment, more stringent methods like Biometric Authentication or Cryptographic means like Digital Certificates should be employed.

7. Password management system: An operating system could enforce selection of good passwords. Internal storage of password should use one-way hashing algorithms and the password file should not be accessible to users.
8. Use of system utilities: System utilities are the programs that help to manage critical functions of the operating system e.g. addition or deletion of users.
9. Duress alarm to safeguard users: If users are forced to execute some instruction under threat, the system should provide a means to alert the authorities.
10. Terminal time out: Log out the user if the terminal is inactive for a defined period. This will prevent misuse in absence of the legitimate user.
11. Limitation of connection time: Define the available time slot. Do not allow any transaction beyond this time period. For example, no computer access after 8.00 p.m. and before 8.00 a.m. - or on a Saturday or Sunday.

SIMILAR QUESTION:

1. Operating System not only provides the platform for an application to use various Information System resources but is also the last barrier to be conquered for unlimited access to all the resources, Explain the statement by describing operating system access controls to protect IT resources from unauthorized access.

Q.No.45. Write about Application and Monitoring System Access Controls with respect to logical access controls. (B)

Application and Monitoring System Access Control:

a) **Information access restriction:** The access to information is prevented by application specific menu interfaces, which limit access to system function. A user is allowed to access only to those items, s/he is authorized to access.

b) **Sensitive system isolation:** Based on the critical constitution of a system in an enterprise, it may even be necessary to run the system in an isolated environment.

c) **Event logging:** In Computer systems, it is easy and viable to maintain extensive logs for all types of events. It is necessary to review if logging is enabled and the logs are archived properly.

d) **Monitor system use:** Based on the risk assessment, a constant monitoring of some critical systems is essential. This defines the details of types of accesses, operations, events and alerts that will be monitored.

e) **Clock synchronization:** Event logs maintained across an enterprise network plays a significant role in correlating an event and generating report on it. Hence, the need for synchronizing clock time across the network as per a standard time is mandatory.

Q.No.46. Write about Mobile Computing with respect to logical access controls. (C)

- In today's organizations, computing facility is not restricted to a particular data centre alone. Ease of access on the move provides efficiency and results in additional responsibility on the management to maintain information security.
- Theft of data carried on the disk drives of portable computers is a high risk factor. Both physical and logical access to these systems is critical. Information is to be encrypted and access identifications like fingerprint, eye-iris, and smart cards are necessary security features.

Q.No.47. Explain various Managerial Controls in detail with respect to audit objectives in IS controls? (A) (N15 MTP2)

Managerial Controls: The managerial controls must be performed to ensure the development, implementation, operation and maintenance of information systems in a planned and controlled manner in an organization. The controls at this level provide a stable infrastructure in which information systems can be built, operated, and maintained on a day-to-day basis.

Management Subsystem	Description of Subsystem
Top Management	Top management must ensure that information systems function is well managed. It is responsible primarily for long - run policy decisions on how Information Systems will be used in the organization.
Information Systems Management	IS management has overall responsibility for the planning and control of all information system activities. It also provides advice to top management in relation to long-run policy decision making and translates long-run policies into short run goals and objectives.
Systems Development Management	Systems Development Management is responsible for the design, implementation, and maintenance of application systems.
Programming Management	It is responsible for programming new system; maintain old systems and providing general systems support software.
Data Administration	Data administration is responsible for addressing planning and control issues in relation to use of an organization's data.
Quality Assurance Management	It is responsible for ensuring information systems development; implementation, operation, and maintenance conform to established quality standards.
Security Administration	It is responsible for access controls and physical security over the information systems function.
Operations Management	It is responsible for planning and control of the day-to-day operations of information systems.

Q.No.48. Explain Top Management and Information Systems Management Controls with respect to managerial controls? (A)

Managerial controls over the managerial functions that must be performed to ensure the development, implementation, operation and maintenance of information systems in a planned and controlled manner in an organization.

Top Management and Information Systems Management Controls: The senior managers who take responsibility for IS function in an organization face many challenges.

The major functions that a senior manager must perform are as follows:

a) **Planning:** Determining the goals of the information systems function and the means of achieving these goals;

i) **Preparing the plan:** This involves the following tasks:

- Recognizing opportunities and problems that confront the organization in which Information technology and Information systems can be applied cost effectively;
- Identifying the resources needed to provide the required information technology and information systems.
- Formulating strategies and tactics for acquiring the needed resources.

ii) **Types of Plans:**

- Top management must prepare two types of information systems plans for the information systems function: a Strategic plan and an Operational plan.
- Both the plans need to be reviewed regularly and updated as the need arises.
- **Strategic Plan:** The Strategic Plan is the long-run plan covering, say, the next three to five years of operations;
- **Operation Plan:** It is the short-plan covering, say, next one to three years of operations.

iii) **Role of a Steering Committee:**

- The steering committee shall comprise of representatives from all areas of the business, and IT personnel. The committee would be responsible for the overall direction of IT.
- The ultimate responsibility for information systems planning should be vested in an information systems steering committee.
- The steering committee should assume overall responsibility for the activities of information systems function.

b) **Organizing:** There should be a prescribed IT organizational structure with documented roles and responsibilities and agreed job descriptions. This includes gathering, allocating, and coordinating the resources needed to accomplish the goals that are established during planning function.

i) **Resourcing the Information Systems Function:** A major responsibility of top management is to acquire the resources needed to accomplish the goals and objectives set out in the information systems plan. These resources include hardware, software, personnel, finances and facilities.

ii) **Staffing the Information systems Function:** Staffing the Information systems function involves three major activities - Acquisition of information systems personnel, Development of information systems personnel, and Termination of information systems personnel.

c) **Leading:** This includes motivating, guiding, and communicating with personnel. The purpose of leading is to achieve the harmony of objectives; *i.e. a person's or group's objectives must not conflict with the organization's objectives..*

i) **Motivating and Leading Information Systems Personnel:** Though many theories exist, however there is no one best way of motivating and guiding all people and thus the strategies for motivating/leading people need to change depending upon particular characteristics of an individual person and his/her environment.

ii) **Communicating with IS Personnel: Effective** communications are also essential to promoting good relationships and a sense of trust among work colleagues.

d) **Controlling:** This includes comparing actual performance with planned performance as a basis for taking any corrective actions that are needed. *This involves determining when the actual activities of the information system's functions deviate from the planned activities.*

i) **Overall Control of IS function:** When top managers seek to exercise overall control of the information systems function, two questions arise:

- How much the organization should be spending on the information systems function?
- Is the organization getting value for the money from its information systems function?

ii) **Control of Information System Activities:** Top managers should seek to control the activities on the basis of Policies and Procedure.

iii) **Control over Information System Services:** For each service level, estimates must be made of the expected benefits and resource consumption and finally the review committee must establish priorities.

Q.No.49. Explain Systems Development Management Controls? (A) (N15 RTP)

1. Systems Development Management has responsibility for the functions concerned with analyzing, designing, building, implementing, and maintaining information systems.
2. There are different types of audits may be conducted during system development process.
   a) **System Authorization Activities:** All systems must be properly authorized to ensure their economic justification and feasibility.
   b) **User Specification Activities:** Users must be actively involved in the systems development process. Regardless of the technology involved, the user can create a detailed written description of the logical needs that must be satisfied by the system.
   c) **Technical Design Activities:** The technical design activities in the SDLC translate the user specifications into a set of detailed technical specifications of a system that meets the user's needs.
   d) **Internal Auditor's Participation:** The internal auditor plays an important role in the control of systems development activities. Auditor's involvement should be continued throughout all phases of the development process and into the maintenance phase.
   e) **Program Testing:** All program modules must be thoroughly tested before they are implemented. The results of the tests are then compared against predetermined results to identify programming and logic errors.
   f) **User Test and Acceptance Procedures:** Just before implementation, the individual modules of the system must be tested as a unified whole. A test team comprising user personnel, systems professionals, and internal audit personnel subjects the system to rigorous testing. Once the test team is satisfied that the system meets its stated requirements, the system is formally accepted by the user department(s).

Q.No.50. Explain Programming Management Controls? (OR) Explain phases of Program development life cycle. (A) (N16 MTP1, M17- 6M)

The primary objectives of Program development and implementation phase are to produce or acquire and to implement high - quality programs.

1. The program development life cycle comprises six major phases – Planning; Design; Control; Coding; Testing; and Operation and Maintenance with Control phase running in parallel for all other phases.
2. The purpose of the control phase during software development or acquisition is to monitor progress against plan and to ensure software released for production use is authentic, accurate, and complete.

Phases of Program Development Life Cycle

Phase	Controls
Planning	Techniques like Work Breakdown Structures (WBS), Gantt Charts and PERT (Program Evaluation and Review Technique) Charts can be used to monitor progress against plan.
Control	• Task progress in various software life-cycle phases should be monitored against plan and corrective action should be taken in case of any deviation. • Control over software development, acquisition, and implementation tasks should be exercised to ensure software released for production use is authentic, accurate, and complete
Design	A systematic approach to program design, such as any of the structured design approaches or object-oriented design is adopted.

Coding	Programmers must choose a module implementation and integration strategy (like Top-down, bottom-up and Threads approach), a coding strategy (that follows the percepts of structured programming), and a documentation strategy (to ensure program code is easily readable and understandable).
Testing	Three types of testing can be undertaken: • Unit Testing – which focuses on individual program modules; • Integration Testing – Which focuses in groups of program modules; and • Whole – of – Program Testing – which focuses on whole program. • These tests are to ensure that a developed or acquired program achieves its specified requirements.
Operations & Maintenance	Management establishes formal mechanisms to monitor the status of operational programs so maintenance needs can be identified on a timely basis. Three types of maintenance can be used – **1.** Repair maintenance – in which program errors are corrected; **2.** Adaptive Maintenance – in which the program is modified to meet changing user requirements; and **3.** Perfective Maintenance - in which the program is tuned to decrease the resource consumption.

Q.No.51. Explain Data Resource Management Controls? (B) (N16 RTP, N15 RTP)

1. Data is a critical resource that must be managed properly. Accordingly, centralized planning and control must be implemented.
2. For data to be managed better users must be able to share data, data must be available to users when it is needed, in the location where it is needed, and in the form in which it is needed.
3. It allows easy modification of data and the integrity of the data must be preserved.
4. If data repository system is used properly, it can enhance data and application system reliability.
5. Careful control should be exercised over the roles by appointing senior, trustworthy persons, separating duties to the extent possible and maintaining and monitoring logs of the data administrator's and database administrator's activities.
6. **The control activities involved in maintaining the integrity of the database is as under:**

   a) **Definition Controls:** These controls are placed to ensure that the database always corresponds and comply with its definition standards.

   b) **Existence/Backup Controls**: These ensure the existence of the database by establishing backup and recovery procedures. Backup refers to making copies of the data so that these additional copies may be used to restore the original data after a data loss.

   Various backup strategies are given as follows:

   i) **Dual recording of data**: Under this strategy, two complete copies of the database are maintained. The databases are concurrently updated.

   ii) **Periodic dumping of data**: This strategy involves taking a periodic dump of all or part of the database onto some backup storage medium – magnetic tape, removable disk, Optical disk etc. The dump may be scheduled

   iii) **Logging input transactions**: This involves logging the input data transactions which cause changes to the database. Normally, this works in conjunction with a periodic dump.

   iv) **Logging changes to the data**: This involves copying a record each time it is changed by an update action.

   c) **Access Controls:** Access controls are designed to prevent unauthorized individual from viewing, retrieving, computing or destroying the entity's data.

Controls are established in the following manner:

i) **User Access Controls** through passwords, tokens and biometric Controls; and

ii) **Data Encryption:** Keeping the data in database in encrypted form.

d) **Update Controls:** These controls restrict update of the database to authorized users in two ways:

i) By permitting only addition of data to the database; and

ii) Allowing users to change or delete existing data.

e) **Concurrency Controls:** These controls provide solutions, agreed-upon schedules and strategies to overcome the data integrity problems that may arise when two update processes access the same data item at the same time.

f) **Quality Controls:** These controls ensure the accuracy, completeness, and consistency of data maintained in the database. This may include traditional measures such as program validation of input data and batch controls over data in transit through the organization

Q.No.52. Explain Quality Assurance Management Controls? (B) (M17 RTP)

1. Quality Assurance management is concerned with ensuring that the –

a) Information produced by the information systems function is to achieve certain quality goals; and

b) Development, implementation, operation and maintenance of Information systems comply with a set of quality standards.

2. The reasons for the emergence of Quality assurance in many organizations are as follows:

a) Organizations are increasingly producing safety-critical systems and users are becoming more demanding in terms of the quality of the software they employ to undertake their work.

b) Organizations are undertaking more ambitious projects when they build software.

c) Users are becoming more demanding in terms of their expectations about the quality of software they employ to undertake their work, Organizations are becoming more concerned about their liabilities if they produce and sell defective software.

d) Poor quality control over the production, implementation, operation, and maintenance of software can be costly in terms of missed deadlines, dissatisfied users and customer, lower morale among IS staff, higher maintenance and strategic projects that must be abandoned.

e) Improving the quality of Information Systems is a part of a worldwide trend among organizations to improve the quality of the goods and services they sell.

3. Quality Assurance (QA) personnel should work to improve the quality of information systems produced, implemented, operated, and maintained in an organization. They perform a monitoring role for management to ensure that –

a) Quality goals are established and understood clearly by all stakeholders; and

b) Compliance occurs with the standards that are in place to attain quality information systems.

Q.No.53. Explain Security Management Controls? (B)

1. Information security administrators are responsible for ensuring that information systems assets are categorized under Personnel, Hardware, Facilities, Documentation, Supplies Data, Application Software and System Software etc.

2. Assets are secure when the expected losses that will occur over some time are at an acceptable level.

3. The control's classification on the basis of "Nature of Information System Resources – Environmental Controls, Physical Controls and Logical Access Controls are all security measures against the possible threats.

4. **Threat Identification**: A threat is some action or event that can lead to a loss. During the threat-identification phase, security administrators attempt to flesh out all material threats that can eventuate and result in information systems assets being exposed, removed either temporarily or permanently lost, damaged, destroyed or used for unauthorized purposes.

   Some of the major threats and to the security of information systems and their controls are:

Major threats and their control measures

Threat	Control
Fire	Well-designed, reliable fire-protection systems must be implemented.
Water	Facilities must be designed and sited to mitigate losses from water damage
Energy Variations	Voltage regulators, circuit breakers, and uninterruptible power supplies can be used.
Structural Damage	Facilities must be designed to withstand structural damage.
Pollution	Regular cleaning of facilities and equipment should occur.
Unauthorized Intrusion	Physical access controls can be used.
Viruses and Worms	Controls to prevent use of virus-infected programs and to close security loopholes that allow worms to propagate.
Misuse of software, data and services	Code of conduct to govern the actions of information systems employees.
Hackers	Strong, logical access controls to mitigate losses from the activities of hackers.

Q.No.54. Inspite of the controls on place, there could be a possibility that a control might fail what are the last resort controls to recover operations and mitigate losses, when disaster strikes. (C)

DRP:

- A comprehensive DRP comprise four parts – an Emergency Plan, a Backup Plan, a Recovery Plan and a Test Plan. The plan lays down the policies, guidelines, and procedures for all Information System personnel.
- BCP (Business Continuity Planning) Controls are related to having an operational and tested IT continuity plan, which is in line with the overall business continuity plan, and its related business requirements so as to make sure IT services are available as required and to ensure a minimum impact on business in the event of a major disruption.
- The controls include Critical Classification, alternative procedures, Back-up and Recovery, Systematic and Regular Testing and Training, Monitoring and Escalation Processes, Internal and External Organizational Responsibilities, Business Continuity Activation, Fallback and Resumption plans, Risk Management Activities, Assessment of Single Points of Failure and Problem Management.

Insurance:

- Adequate insurance must be able to replace Information Systems assets and to cover the extra costs associated with restoring normal operations.
- Policies usually can be obtained to cover the resources like – Equipment, Facilities, Storage Media, Valuable Papers and Records etc.

Q.No.55. Explain Operations Management Controls? (B)

Operations management is responsible for the daily running of hardware and software facilities. Operations management typically performs controls over the functions as below:

a) Computer Operations:

i) The controls over computer operations govern the activities that directly support the day-to-day execution of either test or production systems on the hardware/software platform available.

ii) Three types of controls fall under this category:

- **Operation controls:** These controls prescribe the functions that either human operators or automated operations facilities must perform.
- **Scheduling controls:** These controls prescribe how jobs are to be scheduled on a hardware/software platform.
- **Maintenance controls**: These controls prescribe how hardware is to be maintained in good operating order.

b) Network Operations:

i) This includes the proper functioning of network operations and monitoring the performance of network communication channels, network devices, and network programs and files.

ii) Data may be lost or corrupted through component failure.

iii) The primary components in the communication sub-systems are given as follows:

- Communication lines viz. twisted pair, coaxial cables, fiber optics, microwave and satellite etc.
- Hardware – ports, modems, multiplexers, switches and concentrators etc.
- Software – Packet switching software, polling software, data compression software etc.
- Due to component failure, transmission between sender and receiver may be disrupted, destroyed or corrupted in the communication system.

c) Data Preparation and Entry: Irrespective of whether the data is obtained indirectly from source documents or directly from, say, customers, keyboard environments and facilities should be designed to promote speed and accuracy and to maintain the well being of keyboard operators.

d) Production Control: This includes the major functions like- receipt and dispatch of input and output; job scheduling; management of service-level agreements with users; transfer pricing/charge-out control; and acquisition of computer consumables.

e) File Library: This includes the management of an organization's machine-readable storage media like magnetic tapes, cartridges, and optical disks.

f) Documentation and Program Library: This involves that documentation librarians ensure that documentation is stored securely; that only authorized personnel gain access to documentation; that documentation is kept up-to-date and that adequate backup exists for documentation. The documentation may include reporting of responsibility and authority of each function; Definition of responsibilities and objectives of each functions; Reporting responsibility and authority of each function; Policies and procedures; Job descriptions and Segregation of duties.

g) Help Desk/Technical support: This assists end-users to employ end-user hardware and software such as micro-computers, spreadsheet packages, database management packages etc. and also provides the technical support for production systems by assisting with problem resolution.

h) Capacity Planning and Performance Monitoring: Regular performance monitoring facilitates the capacity planning wherein the resource deficiencies must be identified well in time so that they can be made available when they are needed.

i) Management of Outsourced Operations: This has the responsibility for carrying out day-to-day monitoring of the outsourcing contract.

Q.No.56. Explain various user Controls? (Or) Software applications require interface between the user and the business functions. Discuss user controls describing various types of controls to be exercised to achieve system effectiveness and efficiency. (A) (PM, M15 - 6M)

Application system controls are undertaken to accomplish reliable information processing cycles that perform the processes across the enterprise. Applications represent the interface between the user and the business functions. For example, a counter clerk at a bank is required to perform various business activities as part of his/her job description and assigned responsibilities.

User Controls: Application system represents the interface between the user and the business functions. From the users' perspective, it is the applications that drive the business logic and thus User Controls are required. The user controls that are to be exercised for system effectiveness and efficiency are as follows:

a) **Boundary Controls:** These establish interface between the user of the system and the system itself. The system must ensure that it has an authentic user. Further users are allowed using resources in restricted ways.

b) **Input Controls:** Responsible for ensuring the accuracy and completeness of data and instruction input into an application system. Input Controls are validation and error detection of data input into the system.

c) **Processing Controls:** These controls are responsible for computing, sorting, classifying and summarizing data. These maintain the chronology of events from the time data is received from input or communication systems to the time data is stored into the database or output as results.

d) **Output Controls:** These controls provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared and routed to users.

e) **Database Controls:** These are responsible to provide functions to define, create, modify, delete and read data in an information system. These maintain procedural data-set of rules to perform operations on the data to help a manager to take decisions.

Q.No.57. What do you understand by Boundary controls? Explain major boundary control techniques in brief. (PM, M15 - 6M, N14 RTP, M17 - 4M) (OR) You are selected by UVW Limited to review and strengthen Software Access Control mechanism for their Company. Prepare a report on the need of boundary controls enlisting major boundary control techniques to be implemented by them. (A) (PM)

1. Boundary Controls establish interface between the user and the system itself.
2. The major controls of the boundary system are the physical access controls.
3. Physical access controls are implemented with an access control mechanism and links the authentic users to the authorized resources they are permitted to access.
4. The access control mechanism consists of the three steps - "identification", "authentication" and "authorization" with respect to the access control policy.

Major Boundary Control techniques are:

a) **Cryptography:**

i) Deals with programs for transforming data into codes that are meaningless to anyone who does not possess the authentication to access the respective system resource or file.

ii) A cryptographic technique encrypts data (clear text) into cryptograms (cipher text) and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst.

iii) *The three techniques of cryptography are transposition (permute the order of characters within a set of data), substitution (replace text with a key-text) and product cipher (combination of transposition and substitution).*

b) **Passwords:**

i) User identification by an authentication mechanism with personal characteristics like name, birth date, employee code, function, designation or a combination of two or more of these can be used as a password boundary access control.

ii) A few best practices followed to avoid failures in this control system are; minimum password length, avoid usage of common dictionary words, periodic change of passwords, encryption *of passwords and number of entry attempts.*

c) **Personal Identification Numbers (PIN):** The personal identification number is assigned to a user by an institution based on the user characteristics and encrypted using a cryptographic algorithm or the institute generates a random number stored in its database independent to a user identification details, or a customer selected number.

d) **Identification Cards:**

i) Identification cards are used to store information required in an authentication process.

ii) These cards are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.

e) **Biometric Devices:** Biometric identification e.g. thumb and/or finger impression, eye retina etc. are also used as boundary control techniques.

Q.No.58. Write about the importance of input controls, in the context of user controls? (B)

1. Input Controls are responsible for ensuring the accuracy and completeness of data and instruction input into an application system.
2. Input controls are important since substantial time is spent on input of data, involve human intervention and are therefore error and fraud prone.
3. Data codes are used to uniquely identify an entity or identify an entity as a member of a group or set.
4. Poorly designed data codes cause recording and keying errors.
5. Auditors should evaluate the quality of coding systems to analyze their impact on the integrity and accurateness of data keyed into the system.

Q.No.59. what are various input controls? (B)

Input controls are divided into the following broad classes:

1. Source Document Control, **(Refer Q.No: 61)**
2. Data Coding Controls, **(Refer Q.No: 62)**
3. Batch Controls and **(Refer Q.No: 63)**
4. Validation Controls. **(Refer Q.No: 64)**

Q.No.60. Explain Source Document Controls? (B)

1. In systems that use physical source documents to initiate transactions, careful control must be exercised over these instruments.
2. Source document fraud can be used to remove assets from the organization.
3. To control against this type of exposure, the organization must implement control procedures over source documents to account for each document, as described below:

a) **Use pre-numbered source documents:** Source documents should come pre-numbered from the printer with a unique sequential number on each document.

b) **Use source documents in sequence:** Source documents should be distributed to the users and used in sequence. This requires the adequate physical security be maintained over the source document inventory at the user site. .

c) **Periodically audit source documents:** Missing source documents should be identified by reconciling document sequence numbers. Periodically, the auditor should compare the numbers of documents used for updatation, and identify the remaining inventory.

Q.No.61. Explain Data Coding Controls? (OR) For data core entry user may do different types of errors. Name the different types of error for data code entry. (B)

Two types of errors can corrupt a data code and cause processing errors. These are transcription and transposition errors. They are:

a) **Transcription Errors:** These fall into three classes:

i) Addition errors occur when an extra digit or character is added to the code. For example, inventory item number 83276 is recorded as 832766.

ii) Truncation errors occur when a digit or character is removed from the end of a code. In this type of error, the inventory item above would be recorded as 8327.

iii) Substitution errors are the replacement of one digit in a code with another. For example, code number 83276 is recorded as 83266.

b) **Transposition Errors:** There are two types of transposition errors.

i) Single transposition errors occur when two adjacent digits are reversed. For instance, 12345 are recorded as 21345.

ii) Multiple transposition errors occur when nonadjacent digits are transposed. For example, 12345 are recorded as 32154.

Q.No.62. Explain Batch Controls? (B)

1. Batching is the process of grouping together similar types of transactions that bear some type of relationship to each other.

2. Various controls can be exercises over the batch to prevent or detect errors or irregularities. Two types of batches occur: **(N16 RTP)**

   a) **Physical Controls:** These controls are groups of transactions that constitute a physical unit.

   b) **Logical Controls:** These are group of transactions bound together on some logical basis, rather than being physically contiguous.

3. To identify errors or irregularities in either a physical or logical batch, three types of control totals can be calculated as shown as

Control Totals on Logical / Physical Batch

Control Total Type	**Explanation**
Financial totals	Grand totals calculated for each field containing money amounts.
Hash totals	Grand totals calculated for any code on a document in the batch, eg., the source document serial numbers can be totaled.
Document / Record Counts	Grand totals for the number of documents in record in the batch.

Q.No.63. Explain Validation controls? (B)

These controls validate the accuracy/correctness of input data. Input Validation Controls are intended to detect errors in transaction data before the data are processed.

There are following levels of input validation controls, which are:

a) Field Interrogation

- i) **Limit Check:** It may be applied to both the input data and the output data. The field is checked by the program to ensure that its value lies within certain predefined limits.
- ii) **Picture Checks:** Picture check against incorrect input format. For example, all rooms are numbered by numeric. An incorrect room number 9X5 would be filtered.
- iii) **Valid Code Checks:** These checks are made against predetermined transactions codes, tables or order data to ensure that input data are valid.
- iv) **Check Digits:** A customers' account number or any other numeric digits are checked for transcription and transposition errors.
- v) **Arithmetic Check:** Arithmetic check is performed in different ways to validate the results of other computations of the values of selected data fields.
- vi) **Cross Checks:** These may be employed to verify fields appearing in different files to see that the results tally.

b) Record Interrogation:

- i) **Reasonableness Check:** Whether the value specified in a field is reasonable for that particular field?
- ii) **Valid Sign:** The contents of one field may determine which sign is valid for a numeric field.
- iii) **Sequence Check:** If physical records follow a required order matching with logical records.

c) File Interrogation: **(N16 - 6M)**

- i) **Version Usage:** Proper version of a file should be used for processing the data correctly. In this regard it should be ensured that only the most current file be processed.
- ii) **Internal and External Labeling:** Labeling of storage media is important to ensure that the proper files are loaded for process. Where there is a manual process for loading files, external labeling is important to ensure that the correct file is being processed.
- iii) **Data File Security:** Unauthorized access to data file should be prevented, to ensure it achieves objectives such as confidentiality, integrity and availability.
- iv) **Before and after Image and Logging:** The application may provide for reporting of before and after images of transactions.
- v) **File Updating and Maintenance Authorization:** Sufficient controls should exist for file updating and maintenance to ensure that stored data are protected
- vi) **Parity Check:** When programs or data are transmitted, additional controls are needed. Transmission errors are controlled primarily by detecting errors or correcting errors using error detecting and correcting codes.

Q.No.64. Explain communication controls? (A)

1. Three major types of exposure arise in the communication subsystem:

- **a)** Transmission impairments can cause difference between the data sent and the data received;
- **b)** Data can be lost or corrupted through component failure; and
- **c)** A hostile party could seek to subvert data that is transmitted through the subsystem.

2. The common controls in communication subsystem are

a) Physical Component Controls: These controls incorporate features that mitigate the possible effects of exposures. Some of them are :

Transmission Media	It is a physical path along which a signal can be transmitted between a sender and a receiver. It is of two types : • **Guided/Bound Media** in which the signals are transported along an enclosed physical path like – Twisted pair, coaxial cable, and optical fiber. • **Unguided Media**, the signals propagate via free-space emission like – satellite microwave, radio frequency and infrared
Communication Lines	The reliability of data transmission can be improved by choosing a private (leased) communication line rather than a public communication line.
MODEM	**1.** Increases the speed **2.** Reduces the number of line errors
Port Protection Devices	These device performs various security functions to authenticate users
Multiplexers and Concentrators	These devices allow the bandwidth or capacity of a communication line to be used more effectively.

b) Line Error Control: Whenever data is transmitted over a communication line, recall that it can be received in error because of attenuation distortion, or noise that occurs on the line. These errors must be detected and corrected.

i) Error Detection: The errors can be detected by either using a loop (echo) check or building some form of redundancy into the message transmitted.

ii) Error Correction: When line errors have been detected, they must be corrected using either forward error correcting codes or backward error correcting codes.

c) Flow Controls: Flow controls are needed because two nodes in a network can differ in terms of the rate at which they can send, received, and process data.

d) Link Controls: In WANs, line error control and flow control are important functions in the component that manages the link between two nodes in a network. The link management components mainly use two common protocols HDLC (Higher Level Data Link control) and SDLC (Synchronous Data Link Control).

e) Topological Controls: A communication network topology specifies the location of nodes within a network, the ways in which these nodes will be linked, and the data transmission capabilities of the links between the nodes

i) Local Area Network Topologies: Local Area Networks tend to have three characteristics:

- they are privately owned networks and provide high -speed communication among nodes;
- Exists within a limited geographic areas.

They are implemented using four basic types of topologies:

- Bus topology
- Tree topology
- Ring topology
- Star topology.
- Hybrid topologies

ii) Wide Area Network Topologies: Wide Area Networks have the following characteristics:

i) they often encompass components that are owned by other parties (e.g. a telephone company);

ii) They provide relatively low-speed communication among nodes

iii) They span large geographic areas

f) Channel Access Controls: Two different nodes in a network can compete to use a communication channel. Whenever the possibility of contention for the channel exists, some type of channel access control technique must be used. These techniques fall into two classes: Polling methods and Contention methods.

i) Polling: Polling (non contention) techniques establish an order in which a node can gain access to channel capacity.

ii) Contention Methods: Using contention methods, nodes in a network must compete with each other to gain access to a channel. *Each node is given immediate right of access to the channel. Whether the node can use the channel successfully, however, depends on the actions of other nodes connected to the channel.*

g) Internetworking Controls: Internetworking is the process of connecting two or more communication net-works together to allow the users of one network to communicate with the users of other networks.

h) Three types of devices are used to connect sub-networks in an internet are:

Device	Functions
Bridge	A bridge connects similar local area networks (e.g. one token ring network to another token ring network).
Router	A router performs all the functions of a bridge. In addition, it can connect heterogeneous Local Area Networks and direct network traffic over the fastest channel between two nodes that reside in different sub - networks .
Gateway	The primary function is to perform protocol conversion to allow different types of communication architectures to communicate with one another.

<u>**SIMILAR QUESTION:**</u>

1. Discuss any three internetworking devices **(PM, N15 MTP2)**

Q.No.65. Explain Processing Controls? (B)

1. The processing subsystem is responsible for <u>computing, sorting, classifying, and summarizing data.</u>

2. Processor Controls: The processor has three components

a) A Control unit, which fetches programs from memory and determines their type

b) An Arithmetic and Logical Unit, which performs operations;

c) Registers that are used to store temporary results and control information.

Four types of controls that can be used to reduce expected losses from errors and irregularities associated with Central processors are:

Control	Explanation
Error Detection and Correction	Occasionally, processors might malfunction. The causes could be design errors, manufacturing defects, damage, fatigue, electromagnetic interference and ionizing radiation.

Multiple Execution States	It is important to determine the number of and nature of the execution states enforced by the processor. This helps auditors to determine which user processes will be able to carry out unauthorized activities such as gaining access to sensitive data maintained in memory regions assigned to the operating system or other user processes
Timing Controls	An operating system might get stuck in an infinite loop. In the absence of any control, the program will retain use of processor and prevent other programs from undertaking their work.
Component Replication	In some cases, processor failure can result in significant losses Redundant processors allow errors to be detected and corrected.

3. **Real Memory Controls:** This comprises the fixed amount of primary storage in which programs or data must reside for them to be executed or referenced by the central processor. Real memory controls seek to detect and correct errors that occur in memory cells and to protect areas of memory assigned to a program from illegal access by another program.

4. **Virtual Memory Controls:** Virtual Memory exists when the addressable storage space is larger than the available real memory space. To achieve this outcome, a control mechanism must be in place that maps virtual memory addresses into real memory addresses.

5. **Access Control Mechanisms:** An Access Control Mechanism is associated with identified, authorized users the resources they are allowed to access and action privileges.

Q.No.66. Discuss the three processes of Access Control Mechanism, when a user requests for resources. (Or) Write short notes on Access control Mechanism (A) (PM)

An Access Control Mechanism is associated with identified, authorized users the resources they are allowed to access and action privileges. The mechanism processes the users request for Real time Memory and Virtual Memory resources in three steps:

a) **Identification:** Users have to identify themselves.

b) **Authentication:** Users must authenticate themselvel.*The mechanism accesses previously stored information about users, the resources they can access, and the action privileges they have with respect to these resources;* it permits or denies the request. Users may provide four factor of authentication information as described in Table below:

Classes of Authentication

Remembered information	Objects Possessed by the user
Name,	Badge, plastic card, key
Account number,	Finger print, voice print, signature
Passwords	Personal characteristics Dialog Through / around computer

c) **Authorization:** The users request for specific resources, their need for those resources and their areas of usage of these resources. There are two approaches to implementing the authorization module in an access control mechanism:

   i) **Ticket oriented approach:** In a ticket-oriented approach to authorization, the access control mechanism assigns users, a ticket for each resource they are permitted to access. Ticket oriented approach operates via a row in the matrix. Each row along with the user resources holds the action privileges specific to that user.

   ii) **List oriented approach:** In a list-oriented approach, the mechanism associates with each resource a list of users who can access the resource and the action privileges that each user has with respect to the resource. This mechanism operates via a column in the matrix.

Q.No.67. Write short notes on Processing controls and Output controls? (B) (N14 MTP)

a) **Process Controls:**

i) Data processing controls perform validation checks to identify errors during processing of data.

ii) They are required to ensure both the completeness and the accuracy of data being processed.

iii) Normally, the processing controls are enforced through database management system that stores the data.

iv) However, adequate controls should be enforced through the front end application system also to have consistency in the control process.

b) **Output Controls:** **(N14 - 6M)**

i) These controls ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secured manner.

ii) Output can be in any form, it can either be a printed data report or a database file in a removable media such as a CD-ROM or it can be a Word document on the computer's hard disk

iii) Whatever the type of output, it should be ensured that the confidentiality and integrity of the output is maintained and that the output is consistent.

iv) Output controls have to be enforced both in a batch-processing environment as well as in an online environment.

Q.No.68. Explain Data Processing Controls? (B)

These perform validation checks to identify errors during processing of data. They are required to ensure both the completeness and the accuracy of data being processed. Various processing controls are given as follows:

a) **Run – to - run Totals:** These help in verifying data that is subject to process through different stages. *If the current balance of an invoice ledger is Rs. 150,000 and the additional invoices for the period total Rs. 20,000 then the total sales value should be 170,000. A specific record probably the last record can be used to maintain the control total.*

b) **Reasonableness Verification:** Two or more fields can be compared and cross verified to ensure their correctness.

c) **Edit Checks:** Edit checks similar to the data validation controls can also be used at the processing stage to verify accuracy and completeness of data.

d) **Field Initialization:** Data overflow can occur, if records are constantly added to a table or if fields are added to a record without initializing it, i.e. setting all values to zero /blank before inserting the field or record.

e) **Exception Reports:** Exception reports are generated to identify errors in the data processed. Such exception reports give the transaction code and why a particular transaction was not processed or what is the error in processing the transaction.

Q.No.69. Explain the major update controls with respect to Database controls? (A) (PM)

a) **Sequence Check between Transaction and Master Files:** Synchronization and the correct sequence of processing between the master file and transaction file is critical to maintain the integrity of updating, insertion or deletion of records in the master file with respect to the transaction records. If errors in this stage are overlooked it leads to corruption of the critical data.

b) **Ensure All Records on Files are processed:** While processing the transaction file records mapped to the respective master file the end-of-file of the transaction file with respect to the end-of-file of the master file is to be ensured.

c) **Process multiple transactions for a single record in the correct order:** Multiple transactions can occur based on a single master record (eg. dispatch of a product to different distribution centers) here the order in which transactions are processed against the product master record must be done based on a sorted transaction codes.

d) **Maintain a suspense account:** When mapping between the masters record to transaction record results in a mismatch due to failure in the corresponding record entry in the master record then these transactions are maintained in a suspense account. A nonzero balance of the suspense accounts reflect the errors to be corrected.

Q.No.70. Explain the report controls with respect to Database controls? (B) (PM)

1. **Standing Data:**

   a) Application programs use many internal tables to perform various functions like say gross pay calculation, billing calculation based on a price table, bank interest calculation etc,. Maintaining integrity of the pay rate table, price table and interest table is critical within an organization.

   b) Any changes or errors in these tables would have an adverse effect on the organizations basic functions. *Periodic monitoring of these internal tables by means of manual check or by calculating a control total is mandatory.*

2. **Print - Run - to Run control Totals:** Run-to-Run control totals help in identifying errors or irregularities like record dropped erroneously from a transaction file, wrong sequence of updating or the application software processing errors.

3. **Print Suspense Account Entries:** Similar to the update controls in databases the suspense account entries are to be periodically monitors with the respective error file and action taken on time.

4. **Existence/Recovery Controls:**

   a) The back-up and recovery strategies together encompass the controls required to restore failure in a database. Backup strategies are implemented using prior version and log of transactions or changes to the database.

   b) Recovery strategies involve roll-forward (current state database from a previous version) or the rollback (previous state database from the current version) methods.

Q.No.71. As an IS auditor, what are the output controls required to be reviewed with respect to application controls? (B) (PM)

1. **Storage and logging of sensitive, critical forms:** Pre-printed stationery should be stored securely to prevent unauthorized destruction or removal and usage. Only authorized persons should be allowed access to stationery supplies such as security forms, negotiable instruments, etc.

2. **Logging of output program executions:** When programs used for output of data are executed, these should be logged and monitored; otherwise on confidentiality/ integrity of the data may be compromised.

3. **Spooling/queuing:** “Spooling” is an acronym for “Simultaneous Peripherals Operations Online”. This is a process used to ensure that the user is able to continue working, while the print operation is getting completed

4. **Controls over printing:** Outputs should be made on the correct printer and it should be ensured that unauthorized disclosure of information printed does not take place. *Users must be trained to select the correct printer and access restrictions may be placed on the workstations that can be used for printing.*

5. **Report distribution and collection controls:** Distribution of reports should be made in a secure way to prevent unauthorized disclosure of data. *A log should be maintained for reports that were generated and to whom these were distributed. Uncollected reports should be stored securely.*

6. **Retention controls:** Retention controls consider the duration for which outputs should be retained before being destroyed. Consideration should be given to the type of medium on which the output is stored.

Q.No.72. Explain Information Technology General Controls (ITGC)? (A)

1. Information Technology General Controls (ITGC) are the basic policies and procedures that ensure that an organization's information systems are properly safeguarded, that application programs and data are secure, and that computerized operations can be recovered in case of unexpected interruptions.
2. *IT General Controls are provides the assurance that systems operate as intended and that output is reliable.*
3. ITGCs may also be referred to as General Computer Controls (GCC), are defined as Controls applicable to all applications.
4. The objectives of general controls are to ensure the proper development and implementation of applications, the integrity of program and data files and of computer operations.
5. Like application controls, general controls may be either manual or programmed.
6. *Examples of general controls include the development and implementation of an IS strategy and an IS security policy, the organization of IS staff to separate conflicting duties and planning for disaster prevention and recovery.*
7. General Controls are those that control the design, security, and use of computer programs and the security of data files in general throughout an organization.
8. Examples of primary objectives for general controls are to safeguard data, protect application programs, and ensure continued computer operations in case of unexpected interruptions.
9. General controls are applied at the entity-wide, system, and business process application levels, so it is a significant factor in determining the effectiveness of business process controls at the application level.
10. The most common ITGCs are :
    - **a)** Logical access controls over infrastructure, applications, and data.
    - **b)** System development life cycle controls.
    - **c)** Program change management controls.
    - **d)** Data center physical security controls.
    - **e)** System and data backup and recovery controls.
    - **f)** Computer operation controls.

Q.No.73. What is Information classification? Explain the 5-scale or 5-level classification of information? (OR) Explain different classifications of information. (A) (PM, N15-4M) (OR) As a member of IS Steering Committee, how do you classify the information for better integrity and security?

1. Information as it is being created, amended, enhanced, stored, or transmitted. The classification of information and documents is essential if one has to differentiate between that which is of little (if any) value, and that which is highly sensitive and confidential
2. The classification of the information determine the extent to which it needs to be controlled / secured and is also indicative of its value in terms of Business Assets.

3. When data is stored, whether received, created or amended, it should always be classified into an appropriate sensitivity level.

4. For many organizations a simple 5 scale grade will be used.

Information classification	Description	Examples	Controls required
Top secret	Highly sensitive internal information that could cause damage if made public. Must be protected at all times	Information pertaining to mergers or acquisitions, investment strategies, plans or designs	Highest level
Highly confidential	Information that could impede the operations if made public. Must be protected at all times	Business plans, accounting information, bank details	High
Proprietary	Information of proprietary nature defines the way in which organization operates. It can be assessable only to authorized persons.	Standard Operating Procedures, Project plans	High
Internal use only	Information, if lost, could cause some inconvenience, but not Serious Loss	Internal memos, Minutes of meetings,	Normal
Public documents	Information in Public Domain	Annual reports, press statements	Minimal

Q.No.74. What are Data Integrity Controls? (A) (PM)

1. The primary objective of data integrity control techniques is to prevent, detect, and correct errors in transactions as they flow through the various stages of a specific data processing program.

2. Integrity controls ensure that the integrity of a specific application's inputs, stored data, programs, data transmissions, and outputs.

3. Data integrity controls protect data from accidental or malicious alteration or destruction and provide assurance to the user that the information meets expectations about its quality and integrity.

4. Assessing integrity involves evaluating the following critical procedures

   a) Virus detection and elimination software is ins4talled and activated.

   b) Data integrity and validation controls are used to provide assurance that the information has not been altered and the system functions as intended.

Q.No.75. Explain the 6 categories of Data Integrity Controls? (A)

Control category	Definition and purpose	Threats / Risks	Examples of Controls
Source data control	Controls which control data entry at the initial level	Invalid, incomplete, or inaccurate source data input.	• Sequentially prenumbered forms • Segregation of duties • Visual scanning • Check-digit verification
Input controls / Input validation routines	Responsible for ensuring the accuracy and completeness of data and instructions input into an application system.	Invalid or inaccurate data	• Edit programs check key data fields. For instance, sequence, field, sign, validity, limit, range, reasonableness checks.

			• Prompting operators during data entry • Completeness test
Data Processing controls	Data processing controls perform validation checks to identify errors during processing of data. Responsible for computing, sorting, classifying and summarizing data.	Inaccurate or incomplete	• Reconciliation of database totals with externally maintained totals (Batch totals) • Exception reporting
Database controls	Responsible to provide functions to define, create, modify, delete and read data in an information system	Weak database	• Chronological recording of transactions.
Output controls	To provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared and routed to users	Inaccurate or incomplete computer output	• Reconciliation of batch totals. • Proper distribution of output. • Confidential outputs being delivered are protected from unauthorized access, modification, and misrouting.
Data transmission controls	To ensure controls over data transmission	Unauthorized access to data being transmitted or to the system itself; system failures; errors in data transmission	• Monitor network to detect weak points • Multiple communication paths between network components • Preventive maintenance • Data encryption

Q.No.76. Briefly Explain major data integrity policies? (PM, N14 - 5M, N14 RTP, M16 MTP1)

(OR)

Data integrity is a reflection of the accuracy, correctness, validity, and currency of the data'. What can be major Data Integrity Policies to ensure the same. (A) (N16 MTP1)

a) **Virus - Signature Updating:** Virus signatures must be updated immediately when they are made available from the vendor.

b) **Software Testing:** All software must be tested in a suitable test environment before installation on production systems.

c) **Division of Environments:** The division of environments into Development, Test, and Production is required for critical systems.

d) **Version Zero Software:** Version zero software (1.0, 2.0, and so on) must be avoided whenever possible to avoid undiscovered bugs.

e) **Offsite Backup Storage:** Backups older than one month must be sent offsite for permanent storage.

f) **Quarter - End and Year - End Backups:** Quarter-end and year-end backups must be done separately from the normal schedule.

g) **Disaster Recovery:** A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

Q.No.77. Write short notes on Data Security? What should an IS auditor evaluate while reviewing the adequacy of data security controls (B) [M17 - 6M]

1. Data security encompasses the protection of data against accidental or intentional disclosure to unauthorized persons as well as the prevention of unauthorized modification and deletion of the data.

2. Many levels of data security are necessary in an information systems environment; It includes:
   - a) Policies, Database protection
   - b) Data integrity
   - c) Security of the hardware and software controls
   - d) Physical security over the user,
   - e) Organizational

3. An IS auditor is responsible to evaluate the following when reviewing the adequacy of data security controls:
   - a) Who is responsible for the accuracy of the data?
   - b) Who is permitted to read, use and update data?
   - c) Who controls the security of the data?
   - d) If the IS system is outsourced, what security controls and protection mechanism does the vendor have in place to secure and protect data?
   - e) Contractually, what penalties or remedies are in place to protect the tangible and intangible values of the information?
   - f) The disclosure of sensitive information is a serious concern to the organization and is mandatory on the auditor's list of priorities.

Q.No.78. Explain briefly a few financial control techniques? (A) (OR)
What do you understand by Finance Controls? Explain major financial control techniques in brief? (PM, N16 MTP2)

These controls are generally defined as the procedures exercised by the system user personnel over source, or transactions origination, documents before system input.

1. **Authorization:** This entails obtaining the authority to perform some act typically access to such assets as accounting or application entries.
2. **Budgets:** These estimates of the amount of time or money expected to be spent during a particular period of time, project, or event. The budget must be compared with the actual performance, including isolating differences and researching them for a cause and possible resolution.
3. **Cancellation of documents:** This marks a document in such a way to prevent its reuse. This is a typical control over invoices marking them with a "paid" or "processed" stamp or punching a hole in the document.
4. **Dual control:** This entails having two people simultaneously access an asset. Dual access divides the access function between two people: once access is achieved, only one person handles the asset. With teller-machines, for example, two tellers would open the depository vault door together, but only one would retrieve the deposit envelopes.
5. **Input/ output verification:** This entails comparing the information provided by a computer system with the input documents and output reports.
6. **Safekeeping:** This entails physically securing assets, such as computer disks, under lock and key, in a desk drawer, file cabinet storeroom, or vault.
7. **Sequentially numbered documents:** These are working documents with preprinted sequential numbers, which enables the detection of missing documents.
8. **Supervisory review:** This refers to review of specific work by a supervisor but this control requires a sign-off on the documents by the supervisor, in order to provide evidence that the supervisor at least handled them.

Q.No.79. Mr. 'X' has opened a new departmental store and all the activities are computerized. He uses Personal Computers (PCs) for carrying out the business activities. As an IS auditor, list the risks related to the use of PCs in the business of Mr. 'X' and suggest any two security measures to be exercised to overcome them. (OR) Write about risks relating to personal computer controls and the security measures that could be exercised to overcome these risks? (A) (PM, M17 – 6M)

Risks related to the use of PCs in the business are:

1. Personal computers are small in size and easy to connect and disconnect, they are likely to be shifted from one location to another or even taken outside the organization for theft of information.
2. Pen drives can be very conveniently transported from one place to another, as a result of which data theft may occur. Even hard disks can be ported easily these days.
3. PC is basically a single user oriented machine and hence, does not provide inherent data safeguards. Problems can be caused by computer viruses and pirated software, namely, data corruption; slow operations and system break down etc.
4. Segregation of duty is not possible, owing to limited number of staff.
5. Due to vast number of installations, the staff mobility is higher and hence becomes a source of leakage of information.
6. The operating staff may not be adequately trained.
7. Weak access control

The Security Measures that could be exercised to overcome these aforementioned risks are given as follows:

1. Physically locking the system;
2. Proper logging of equipment shifting must be done;
3. Centralized purchase of hardware and software;
4. Standards set for developing, testing and documenting;
5. Uses of antimalware software;
6. Use of disc locks that prevent unauthorized access .

Q.No.80. Write about Cyber frauds? (B)

1. Cyber frauds are increasing day-by-day with advancements in the technology.
2. Major reasons behind the rise of cyber frauds are:
   a) Failure of internal control system,
   b) Failure of organizations to update themselves to new set of risk
   c) **Smart fraudsters:** These are people who are able to target the weaknesses in system, lacunae's in internal controls, even before the organization realizes that such gaps are there.
3. The most common form is online credit card theft. Other common forms may be monetary cyber frauds include non-delivery of paid products purchased through online auction etc.
4. On the basis of the functionality, these are of two types:
   a) **Pure Cyber Frauds:** Frauds, which exists only in cyber world. They are borne out of use of technology. For example: Website hacking.
   b) **Cyber Enabled Frauds:** Frauds, which can be committed in physical world also but with use of technology; the size, scale and location of frauds changes. For example: Withdrawal of money from bank account by stealing PIN numbers.

Q.No.81. What are major Cyber attacks? Explain? (A) (M17 MTP)

1. **Phishing:** It is the act of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. *Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public.*
2. **Network Scanning:** It is a process to identify active hosts of a system, for purpose of getting information about IP addresses etc.
3. **Virus/Malicious Code:** "Computer Virus" means any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource.
4. **Spam:** E-mailing the same message to everyone on one or more Usenet News Group or LISTSERV lists is termed as spam.
5. **Website Compromise/Malware Propagation:** It includes website defacements. Hosting malware on websites in an unauthorized manner.
6. **Others:** These are given as follows:

   a) **Cracking:** Crackers are hackers with malicious intentions.

   b) **Eavesdropping:** It refers to the listening of the private voice or data transmissions, often using a wiretap.

   c) **E-mail Forgery:** Sending e-mail messages that look as if someone else sent it is termed as E-mail forgery.

   d) **E-mail Threats:** Sending a threatening message to try and get recipient to do something that would make it possible to defraud him is termed as E-mail threats.

   e) **Scavenging:** This is gaining access to confidential information by searching corporate records.

Q.No.82. Explain the impact of Cyber frauds on enterprises? (PM, N14 - 4M, N16-5M, M16 MTP1 & 2)
What are the repercussions of cyber frauds on enterprises? (A)
Discuss major dimensions under which impact of cyber frauds on enterprises can be viewed

a) **Financial Loss:** Cyber frauds lead to actual cash loss to target company/organization. For example, wrongfully withdrawal of money from bank accounts.

b) **Legal Repercussions:** Entities hit by cyber frauds are caught in legal liabilities to their customers. Section 43A of the Information Technology Act, 2000, fixes liability for companies/organizations having secured data of customers. Every entity needs to ensure that data is well protected. In case a fraudster breaks into such database, it adds to the liability of entities.

c) **Loss of credibility or Competitive Edge:** News that an organizations database has been hit by fraudsters, leads to loss of competitive advantage. This also leads to lose credibility. *There have been instances where share prices of such companies went down, as the news of such attach percolated to the market.*

d) **Disclosure of Confidential, Sensitive or Embarrassing Information:** Cyber-attack may expose critical information in public domain. For example, the instances of individuals leaking information about governments secret programs.

e) **Sabotage:** The above situation may lead to misuse of such information by enemy country.

Q.No.83.Discuss major techniques to commit Cyber frauds? (A)
(PM, M16, M15 RTP, M16 MTP2)

1. **Hacking:** It refers to unauthorized access and use of computer systems, usually by means of personal computer and a telecommunication network. Normally, hackers do not intend to cause any damage. **(N15 RTP)**
2. **Cracking:** Crackers are hackers with malicious intentions, which means, un-authorized entry. Now across the world hacking is a general term, with two nomenclatures namely: Ethical and Un-ethical hacking. Un-ethical hacking is classified as Cracking. **(N15 RTP)**
3. **Data Diddling:** Changing data before, during, or after it is entered into the system in order to delete, alter, or add key system data is referred as data diddling.
4. **Data Leakage:** It refers to the unauthorized copying of company data such as computer files.
5. **Denial of Service (DoS) Attack:** It refers to an action or series of actions that prevents access to a software system by its intended/authorized users; causes the delay of its time-critical operations; or prevents any part of the system from functioning.
6. **Internet Terrorism:** It refers to the using Internet to disrupt electronic commerce and to destroy company and individual communications.
7. **Logic Time Bombs:** These are the program that lies idle until some specified circumstances or a particular time triggers it. Once triggered, the bomb sabotages the system by destroying programs, data or both.
8. **Masquerading or Impersonation:** In this case, perpetrator gains access to the system by pretending to be an authorized user.
9. **Password Cracking:** Intruder penetrates a system's defense, steals the file containing valid passwords, decrypts them and then uses them to gain access to system resources such as programs, files and data.
10. **Piggybacking:** It refers to the tapping into a telecommunication line and latching on to a legitimate user before s/he logs into the system.
11. **Round Down:** Computer rounds down all interest calculations to 2 decimal places. Remaining fraction is placed in account controlled by perpetrator.
12. **Scavenging or Dumpster Diving:** It refers to the gaining access to confidential information by searching corporate records.
13. **Social Engineering Techniques:** In this case, perpetrator tricks an employee into giving out the information needed to get into the system.
14. **Super Zapping:** It refers to the unauthorized use of special system programs to bypass regular system controls and performs illegal acts.
15. **Trap Door:** In this technique, perpetrator enters in the system using a back door that bypasses normal system controls and perpetrates fraud.

THE END

4. BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

Q.No.1. What is meant by Business Continuity Management (BCM)? Explain need of BCM? (A) (N13-4M)

1. Business Continuity Management (BCM) is a very effective management process to help enterprises to manage the disruption of all kinds, providing countermeasures to safeguard from the incident of disruption.
2. With the BCM Process, enterprises are able to assess the potential threats and manage the consequences of the disruption, which could reduce or eliminate the losses.
3. In order to ensure effective implementation of BCM, the enterprise should conduct regular internal audits at planned intervals to conform to the compliance of Business Continuity Process in line.
4. **Need of Business Continuity Management (BCM):**
   - To meet the enterprise business objectives
   - Ensure continuity of services and operations
5. Business continuity means maintaining the uninterrupted availability of all key business resources required to support essential business activities.
6. Some key terms related to BCM.

   a) **Business Contingency:** A business contingency is an event with the potential to disrupt computer operations, thereby disrupting critical mission and business functions. Such an event could be a power outage, hardware failure, fire, or storm. If the event is very destructive, it is often called a disaster.

   b) **BCP Process:** BCP is a process designed to reduce the risk to an enterprise from an unexpected disruption of its critical functions, both manual and automated ones, and assure continuity of minimum level of services necessary for critical operations. The purpose of BCP is to ensure that vital business functions are recovered and operationalzed within an acceptable timeframe.

   c) **Business Continuity Planning (BCP)**: It refers to the ability of enterprises to recover from a disaster and continue operations with least impact.

Q.No.2. Write short notes on BCP manual and explain the scope of Business Continuity? (B) (S15 MTP)

1. **BCP Manual:**

   a) Successful organizations have a comprehensive BCP Manual, which ensures process readiness, data and system availability to ensure business continuity.

   b) A BCP manual is a documented description of actions to be taken, resources to be used and procedures to be followed before, during and after an event that severely disrupts all or part of the business operations.

   c) The BCP is expected to provide:

      i) Reasonable assurance to senior management of enterprise about the capability to recover from any unexpected disaster affecting business operations and continue to provide services with minimal impact.

      ii) Anticipate various types of incident or disaster scenarios and outline the action plan for recovering from the incident or disaster with minimum impact and ensuring 'Continuous availability of all key services to clients'.

d) The BCP Manual is expected to specify the responsibilities of the BCM team, whose mission is to establish appropriate BCP procedures to ensure the continuity of enterprise's critical business functions.

e) *In the event of an incident or disaster affecting any of the functional areas, the BCM Team serves as liasioning teams between the functional area affected and other departments providing support services.*

2. **Scope of Business Continuity:**

a) Top management of the enterprise needs to define the scope of the BCM program by identifying the key products and services that support the enterprise's objectives, obligations and statutory duties in line with the threat scenario and the business impact analysis.

b) In case of an outsourced service, the risk accountability remains with the enterprise and necessary controls and process should be in place to manage the risk.

Q.No.3. Write are the advantage of Business Continuity? (B) (N15 RTP)

The advantages of BCM are that the enterprise:

a) Is able to proactively assess the threat scenario and potential risks

b) Has planned response to disruptions which can contain the damage and minimize the impact on the enterprise; and

c) Is able to demonstrate a response through a process of regular testing and trainings.

Q.No.4. Explain the BCM policy? Explain its objectives? (B) (PM, N14 – 4M)

1. The main objective of BCP is to minimize or eliminate the loss to enterprise's business in terms of revenue loss, loss of reputation, loss of productivity and customer satisfaction.
2. This policy document is a high level document, which guide to make a systematic approach for disaster recovery,
3. It also provides awareness among the persons in scope about the business continuity aspects and its importance and to test and review the business continuity planning.
4. While developing the BCM policy, the enterprise should consider defining the scope, BCM principles, guidelines and minimum standards for the enterprise.
5. The BCM policy defines the processes of setting up activities for establishing a business continuity capability and the ongoing management and maintenance of the business continuity capability.
6. **BCM policy objectives:** The objective of Business Continuity Management Policy is to provide a structure through which: **(PM)**

a) The loss to enterprise's business in terms of revenue loss, loss of reputation, loss of productivity and customer satisfaction is minimized.

b) Critical services and activities undertaken by the enterprise operation for the customer will be identified.

c) Plans will be developed to ensure continuity of key service delivery following a business

d) Disruption, which may arise from the loss of facilities, personnel, IT and/or communication or failure within the supply and support chains.

e) Invocation of incident management and business continuity plans can be managed.

f) Incident Management Plans & Business Continuity Plans are subject to ongoing testing, revision and updating as required.

g) Planning and management responsibility are assigned to a member of the relevant senior management team

(Explain the objectives of Business Continuity Management Policy briefly?)

Q.No.5. What is meant by Business Continuity Plan (BCP)? (A) (N – 10, RTPM16)

1. Business Continuity Planning (BCP) refers to plans focused on maintaining the operations of an organization, especially the IT infrastructure in face of a threat that has materialized.
2. 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.
3. The logistical plan is called a business continuity plan.
4. Planning is an activity to be performed before the disaster occurs.
5. 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.

Q.No.6. What are the areas covered by Business Continuity Planning? (A)(PM, N–10, RTPM16)

Business continuity covers the following areas:

1. **Business resumption planning:** The operation's piece of business continuity planning.
2. **Disaster recovery planning:** The technological aspect of business continuity planning, the advance planning and preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of disaster.
3. **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.

Q.No.7. Write short notes on Business Continuous life cycle? (B)

1. The business continuity life cycle is broken down into four broad and sequential sections:
   a) Risk assessment,
   b) Determination of recovery alternatives,
   c) Recovery plan implementation, and
   d) Recovery plan validation.
2. Within each of these lifecycle sections, the applicable resource sets are manipulated to provide the organization with the best mix or critical resource quantities at optimum costs with minimum tangible and intangible losses.
3. These resource sets can be broken down into the following components:
   a) Information
   b) Technology
   c) Telecommunication
   d) Process
   e) People
   f) Facilities.

Q.No.8. Explain objectives and goals of Business Continuity Planning? (A)
(PM, N - 08, RTP N14, M15, M16, N16, M17, MTP F16, S16, M17)

1. The primary objective of a business continuity plan is to minimize loss by minimizing the cost associated with disruptions and enable an organization to survive a disaster and to reestablish normal business operations.
2. In order to survive, the organization must assure that critical operations can resume normal processing within a reasonable time frame.
3. The key objectives of the contingency plan should be to:
   - **a)** Provide for the safety and well-being of people on the premises at the time of disaster;
   - **b)** Continue critical business operations
   - **c)** Minimize the duration of a serious disruption to operations and resources
   - **d)** Minimize immediate damage and losses
   - **e)** Establish management succession and emergency powers
   - **f)** Facilitate effective co-ordination of recovery tasks
   - **g)** Reduce the complexity of the recovery effort
   - **h)** Identify critical lines of business and supporting functions
4. The goals of the business continuity plan should be to:
   - **a)** Identify weaknesses and implement a disaster prevention program
   - **b)** Minimize the duration of a serious disruption to business operations
   - **c)** Facilitate effective co-ordination of recovery tasks
   - **d)** Reduce the complexity of the recovery effort.

Q.No.9. Write short notes on methodology of developing a Business Continuity Planning? (or)Mention all the phases that are prescribed under the methodology of developing a BCP? (A)
(PM, M14-4M, N–08, N14 RTP)

The methodology emphasizes on:

- **a)** Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
- **b)** Obtaining commitment from appropriate management to support and participate in the effort;
- **c)** Defining recovery requirements from the perspective of business functions;
- **d)** Documenting the impact of an extended loss to operations and key business functions;
- **e)** Focusing appropriately on disaster prevention and impact minimization, as well as orderly recovery;
- **f)** Selecting business continuity teams that ensure the proper balance required for plan development;
- **g)** Developing a business continuity plan that is understandable, easy to use and maintain.
- **h)** Defining how business continuity considerations must be integrated into ongoing business planning and system development processes.

Q.No.10. List the phased in developing a Business Continuity Planning? (A)
Discuss different phases involved in the development of a BCP? (PM, RTP M15, M16, MTP A16)

1. Pre-Planning Activities (Business continuity plan Initiation)
2. Vulnerability Assessment and General Definition of Requirements
3. Business Impact Analysis
4. Detailed Definition of Requirements
5. Plan Development
6. Testing Program
7. Maintenance Program
8. Initial Plan Testing and Plan Implementation

Q.No.11. Write short notes on Phase1 (or) Pre-Planning activity or Project initiation phase? (B)

1. In phase 1, we obtain an understanding of the existing and projected systems environment of the organization.
2. This enables us to
   a) Refine the scope of business continuity planning and the associated work program
   b) Develop project schedules
   c) Identify and address issues that could have an impact on the delivery and the success of the plan.
3. During this phase a Steering Committee should be established that should undertake an overall responsibility for providing direction and guidance to the business continuity planning team.
4. The committee should also make all decisions related to the recovery planning effort.
5. The Business Continuity Manager should work with the Steering Committee in finalizing the detailed work plan and developing interview schedules for conducting the Security Assessment and the Business Impact Analysis.
6. Two key deliverables of this phase are:
   a) The development of a policy to support the recovery programs
   b) Awareness program to educate management and senior individuals who will be required to participate in the business continuity program.

Q.No.12. Write short notes on Phase 2 (or) Vulnerability assessment and general definition of requirements? (B) (OR) (PM, N14 RTP)
While developing a Business Continuity Plan, the key tasks that should be covered in the second phase 'Vulnerability assessment and general definition of requirement'

1. This phase focuses on identifying the Vulnerability of the assets to any disaster and to reduce the probability of occurrence..
2. Security and control within an organization is a continuing concern.
3. It is to concentrate on activities that have the effect of reducing the possibility of disaster occurrence, rather than concentrating primarily on minimizing the impact of an actual disaster.
4. This phase include the following tasks:

a) A thorough Security Assessment of the system and communications environment including

i) Personnel practices

ii) Physical security

iii) Operating procedures

iv) Backup and contingency planning

v) Systems development and maintenance

vi) Database security

vii) Data and voice communications security

viii) Systems and access control software security

ix) Insurance

x) Security planning and administration

xi) Application controls

xii) Personal computers.

b) Present findings and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.

c) Define the scope of the planning effort.

d) Analyze, recommend and purchase recovery planning and maintenance software required to support the development and maintenance of the plans.

e) Develop a Plan Framework.

f) Assemble business continuity team and conduct awareness sessions.

Q.No.13. What is meant by Business Impact Assessment (BIA) (or) Explain the 3rd Phase of BCP? (A)

1. A Business Impact Assessment (BIA) of all business units that are part of the business environment enables the project team to:

a) Identify critical systems, processes and functions

b) Assess the economic impact of incidents and disasters that result in a denial of access to systems services and other services and facilities

c) Assess the "pain threshold," that is, the length of time business units can survive without access to systems, services and facilities.

2. The BIA Report should be presented to the Steering Committee. This report identifies critical service functions and the timeframes in which they must be recovered after interruption.

3. The BIA Report should then be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities.

Q.No.14. What do you mean by Detailed Definition of requirements in BCP process (or) Phase 4 of BCP? (B)

1. During this phase, a profile of recovery requirements is developed.

2. This profile is to be used as a basis for analyzing alternative recovery strategies.

3. The profile is developed by identifying resources required to support critical functions identified in the Business Impact Analysis.

4. This profile should include

a) Hardware (mainframe, data and voice communication and personal computers)

b) Software (vendor supplied, in-house developed, etc.)

c) Documentation (DP, user, procedures)

d) Outside support (public networks, DP services, etc.)

e) Facilities (office space, office equipments, etc.)

f) Personnel for each business unit.

5. Recovery Strategies will be based on short term, intermediate term and long term outages.
6. Another key deliverable of this phase is the definition of the plan scope, objectives and assumptions.

Q.No.15. Write short notes on Plan Development Phased of BCP or 5 Phase of BCP)? (B)

1. In this phase, recovery plans components are defined and plans are documented.
2. This phase also includes the implementation of changes to user procedures, upgrading of existing data processing operating, vendor contract negotiations andthe definition of recovery teams, their roles and responsibilities.
3. Recovery standards are developed and for the recovery of the core business processes. In the event of a disaster, it is survival and not business as usual.

Q.No.16. Write short notes on the Testing program Phased of BCP or 6 Phase of BCP? (C)

1. The plan Testing/Exercising Program is developed during this phase.
2. Testing/Exercising goals are established and alternative testing strategies are evaluated.
3. Testing strategies tailored to the environment should be selected and an on-going testing program should be established.
4. Unless the plan is tested on a regular basis, there is no assurance that in the event the plan is activated, the organization will survive a disaster.

Q.No.17. List the tasks undertaken in Maintenance program Phase of BCP (7th step of BCP)? (C)

a) Maintenance of the plans is critical to the success of actual recovery.

b) The plans must reflect changes to the environment. **(N16-4M, N14 RTP)**

c) It is critical that existing change management processes are revised to take recovery plan maintenance into account.

d) In areas where change management does not exist, change management procedures will be recommended and implemented.

e) Many recovery software products take this requirement into account.

Q.No.18. Write short notes on Testing and Implementation phases of BCP or 8th phase of BCP? (C) (N14 RTP)

a) Once plans are developed, initial tests of the plans are conducted and any necessary modifications to the plans are made based on an analysis of the test results.

b) Specific activities of this phase include the following:

i) Defining the test purpose/approach;

ii) Identifying test teams;

iii) Structuring the test;

iv) Conducting the test;

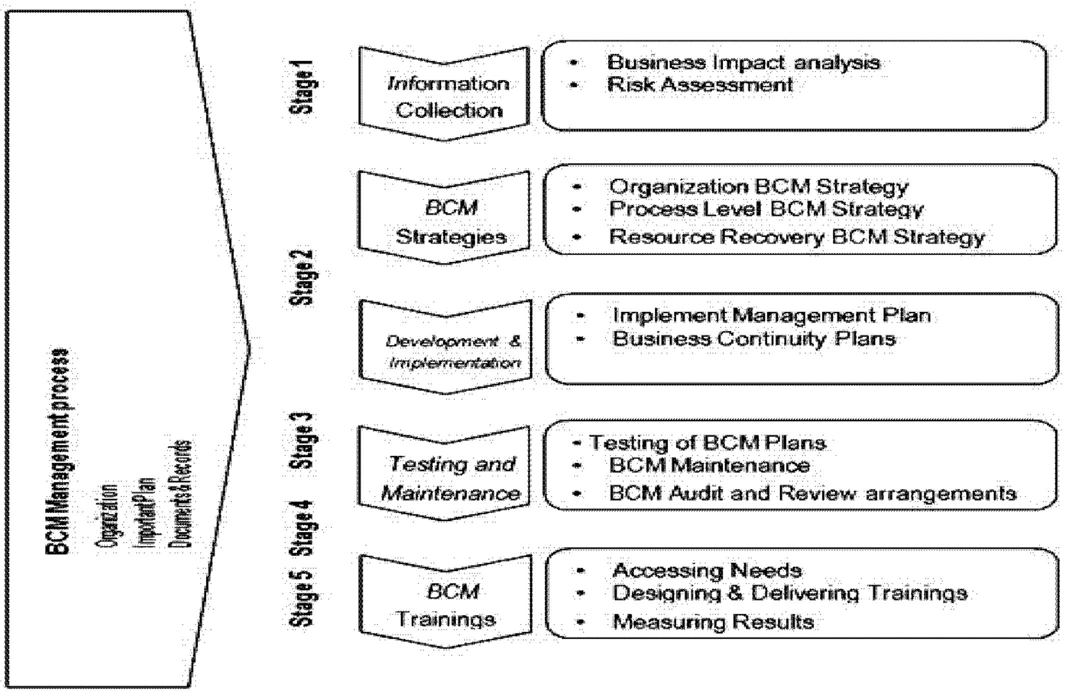
v) Analyzing test results; and

vi) Modifying the plans as appropriate.

c) The approach taken to test the plans depends largely on the recovery strategies selected to meet the recovery requirements of the organization.

d) As the recovery strategies are defined, specific testing procedures should be developed to ensure that the written plans are comprehensive and accurate.

Q.No.19. Explain the components of BCM process? (OR) Explain the Six stages or components of BCM Process. (B) (M17 - 6M, M16 - 5M)



Components of BCM Process

Components of BCM Process are:

a) **BCM - Management Process:** The management process enables the business continuity, capacity and capability to be established and maintained.

b) **BCM – Information Collection Process:** The activities of assessment process do the prioritization of an enterprise's products and services and the urgency of the activities that are required to deliver them. This sets the requirements that will determine the selection of appropriate BCM strategies in the next process.

c) **BCM – Strategy Process:** Finalization of business continuity strategy requires assessment of a range of strategies. This requires an appropriate response to be selected at an acceptable level and during and after a disruption within an acceptable timeframe for each product or service.

d) **BCM – Development and Implementation Process:** Development of a management framework and a structure of incident management, business continuity and business recovery and restoration plans.

e) **BCM Testing and Maintenance Process:** BCM testing, maintenance and audit testify the enterprise BCM to prove the extent to which its strategies and plans are complete, current and accurate; and Identifies opportunities for improvement.

f) **BCM Training Process:** Extensive trainings in BCM framework, incident management, business continuity and business recovery and restoration plans enable it to become part of the enterprise's core values and provide confidence in all stakeholders in the ability of the enterprise to cope with minimum disruptions and loss of service.

Q.No.20. Explain the BCM management process? (C)

1. A BCM process should be in place to address the policy and objectives as defined in the business continuity policy by providing organization structure with responsibilities and authority, implementation and maintenance of business continuity management.

2. The BCM Processes are mapped as follows:

   a) **Organization Structure:**

      i) The organization should nominate a person or a team with appropriate seniority and authority to be accountable for BCM policy implementation and maintenance.

      ii) It should clearly define the person's responsibilities.

   b) **Implementing Business Continuity in the Enterprise and Maintenance:**

      i) In establishing and implementing the BCM system in the organization, managers from each function on site represent their areas of the operation.

      ii) These people are also responsible for the ongoing operation and maintenance of the system within their area of responsibility.

      iii) Where training is required to enable as a colleague to effectively carry out their BCM responsibilities, this will be identified as part of the ongoing staff appraisal and training process.

Q.No.21. What are the major activities in BCM implementation? (B) (M17-4M)

a) Defining the scope & context

b) Defining roles and responsibilities

c) Engaging and involving all stakeholders

d) Testing of program on regular basis

e) Maintaining the currency & appropriateness of business continuity program

f) Reviewing, reworking and updating the business continuity capability, risk assessments (RA) and business impact analysis (BIAs)

g) Managing costs and benefits associated

h) Convert policies and strategies into action.

Q.No.22. What are the major documents that should be the part of a Business Continuity Management System? Explain in brief? (A) (PM, M17-6M, M16 RTP)

1. All documents that form the BCM are subject to the document control and record control processes.

2. The following documents are classified as being part of the business continuity management system:

   a) The business continuity policy

   b) The business continuity management system

   c) The business impact analysis report

   d) The risk assessment report

   e) The aims and objectives of each function

   f) The activities undertaken by each function

   g) The business continuity strategies

   h) The overall and specific incident management plans;

   i) The business continuity plans

   j) Change control, preventative action, corrective action, document control and record control processes

k) Local Authority Risk Register

l) Exercise schedule and results

m) Incident log

n) Training program.

Q.No.23. Write about the BCM information collection process? (C)

To design an effective BCM, it is important to understand the enterprise from all perspectives of interdependencies of its activities, external enterprises and including:

a) Enterprise's objectives, stakeholder obligations, statutory duties and the environment in which the enterprise operates

b) Activities, assets and resources, including those outside the enterprise, that support the delivery of these products and services

c) Impact and consequences over time of the failure of these activities, assets and resources

d) Perceived threats that could disrupt the enterprise's key products and services and the critical activities, assets and resources that support them.

Q.No.24. What analysis should be done for understanding the degree of potential loss (such as reputation damage, regulation effects) of an organization? Enumerate the tasks to be undertaken in this analysis. In what ways the information can be obtained for this analysis? (N09-10M)

(Or)

What is the significance of a Business Impact Analysis (BIA)? Enumerate the tasks to be undertaken in this Analysis. In what ways the information can be obtained for this analysis? (A) (M13-6M, N11-8M, RTP M16)

1. Business Impact Analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents.
2. For each activity supporting the delivery of key products and services within the scope of its BCM program, the enterprise should:
   a) Assess the impacts that would occur if the activity was disrupted over a period of time
   b) Identify the maximum time period after the start of a disruption within which the activity needs to be resumed
   c) Identify critical business processes
   d) Assess the minimum level at which the activity needs to be performed on its resumption
   e) Identify the length of time within which normal levels of operation need to be resumed
   f) Identify any inter-dependent activities, assets, supporting infrastructure or resources that have also to be maintained continuously or recovered over time.
3. The enterprise should have a documented approach to conduct BIA and to assessing the impact of disruption and its findings and conclusions.
4. The BIA Report should be presented to the Steering committee.
5. *This report identifies critical service functions and the time frame in which they must be recovered after interruption.*

Q.No.25. Explain classification of Critical Activities? (B)

1. BCP leader and BCP team leaders in consultation with respective function owner shall carry out Business Impact Analysis for infrastructure and business transactions.
2. BIA will result in categorization (like vital, desirable and essential) of infrastructure and business function following by disaster scenarios (Catastrophic, major, minor trivial) for various disaster causes (fire, flood, system failure etc.)

   a) **Business Categorization (Vital/essential/desirable):**

   i) The parameters considered in deciding whether a function/service is Vital / Essential / Desirable are:

   - Loss of revenue
   - Loss of reputation
   - Decrease in customer satisfaction
   - Loss of productivity

   ii) These parameters shall be graded in a three-point scale 1-3 where, 1= Low(L), 2= Medium (M), 3- High (H)

   b) **Disaster Scenarios (Major/minor/trivial/catastrophic):**

   i) The scenario of disaster shall be decided with the matrix given below:

   ii) The X-axis represents the Business impact of the infrastructure and business transaction as desirable (value=1), essential (value=2) or vital (value=3). The Y-axis represents the likelihood of occurrence of the disaster on a three point scale (1-3).

3 (minor)	6(Major)	9(Catastrophic)
2(Trivial)	4(Major)	6(Major)
1(Trivial)	2(Trivial)	3(Minor)

Business Impact [Desirable (1), Essential (2), Vital (3)]

   c) Identify all the mission critical processes for categorizing into Vital, Essential and Desirable and looking for the probable disasters as per the list attached.

Q.No.26. Explain Risk Assessment? (B)

1. The risk assessment is assessment of the disruption to critical activities, which are supported by resources such as people, process, technology, information, infrastructure supplies and stakeholders.
2. The enterprise should determine the threats and vulnerabilities of each resource, and the impact that would have, in case it becomes a reality.
3. Specific threats may be described as events or actions, which could, at some point, cause an impact to the resources, e.g. threats such as fire, flood, power failure, staff loss, staff absenteeism, computer viruses and hardware failure.
4. Vulnerabilities might occur a weaknesses within the resources and can, at some point be exploited by the threats, e.g. single points of failure, inadequacies in fire protection, electrical resilience, staffing levels, IT security and IT resilience.
5. The Security Assessment will enable the business continuity team to improve any existing emergency plans and to implement required emergency plans where none exist. This is similar to vulnerability assessment phase of developing a BCP.

6. Impacts might result from the exploitation of vulnerabilities by threats.
7. As a result of the BIA and the risk assessment, the enterprise should identify measures that:
   a) Reduce the likelihood of a disruption
   b) Shorten the period of disruption
   c) Limit the impact of a disruption on the enterprise's key products and services.
8. These measures are known as loss mitigation and risk treatment.

Q.No.27. Explain BCM development and Implementation process? (C)

1. The enterprise should have an exclusive organization structure, Incident Management Team / Crisis management team for an effective response and recovery from disruptions.
2. In the event of any incident, there should be a structure to enable the enterprise to:
   a) Confirm Impact of incident (nature and extent),
   b) Control of the situation,
   c) Contain the incident,
   d) Communicate with stakeholders, and
   e) Coordinate appropriate response.
3. **The Incident Management Plan (IMP):**
   a) To manage the initial phase of an incident, the crisis is handled by IMP.
   b) The IMP should have top management support with appropriate budget for development, maintenance and training.
4. **The Business Continuity Plan (BCP):** To recover or maintain its activities in the event of a disruption to a normal business operation, the BCP are invoked to support the critical activities required to deliver the enterprise's objectives.
5. The recovery strategies may be two-tiered:
   a) **Business:** Logistics, accounting, human resources, etc; and
   b) **Technical:** Information Technology (e.g. desktop, client-server, midrange, mainframe computers, data and voice networks).

Q.No.28. Write about BCM testing? (C)

1. A BCP has to be tested periodically because there will undoubtedly be flaws in the plan and in its implementation.
2. The plan will become outdated as time passes and as the resources used to support critical functions change.
3. Responsibility for keeping the plan updated has to be clearly defined in the BCP.
4. A BCM testing should be consistent with the scope of the BCP(s), giving due regard to any relevant legislation and regulation.
5. Testing may be based on a predetermined outcome, e.g. plan and scope in advance; or allow the enterprise to develop innovative solutions.
6. An exercise program should leads to objective assurance that the BCP will work as anticipated when required.
7. The BCP testing program should include testing of the technical, logistical, administrative, procedural and other operational systems, BCM arrangements and infrastructure and technology and telecommunications recovery, including the availability and relocation of staff.

8. In case of Development of BCP, the objectives of performing BCP tests are to ensure that:
   - **a)** The recovery procedures are complete and workable.
   - **b)** The competence of personnel in their performance of recovery procedures can be evaluated.
   - **c)** There sources such as business processes, systems, personnel, facilities and data are obtainable and operational to perform recovery processes.
   - **d)** The manual recovery procedures and IT backup systems are current and can either be operational or restored.
   - **e)** The success or failure of the business continuity training program is monitored.

Implementation:

1. Once plans are developed, initial tests of the plans are conducted and any necessary modifications to the plans are made based on an analysis of the test results.
2. Specific activities of this phase include the following:
   - **a)** Defining the test purpose/approach;
   - **b)** Identifying test teams;
   - **c)** Structuring the test;
   - **d)** Conducting the test;
   - **e)** Analyzing test results; and
   - **f)** Modifying the plans as appropriate.

Q.No.29. Discuss the maintenance undertaken in the development of a BCP in brief. (B)

1. It is important to keep preparations including documentation, up-to-date.
2. Contracts and agreements may also need to reflect the changes.
3. The BCM maintenance process demonstrates the documented evidence of the proactive management and governance of the enterprise's business continuity program.
4. The maintenance tasks undertaken in Development of BCP are to: **(PM, M16 MTP)**
   - **a)** Determine the ownership and responsibility for maintaining the various BCP strategies within the enterprise
   - **b)** Identify the BCP maintenance triggers to ensure that any organizational, operational, and structural changes are communicated to the personnel who are accountable for ensuring that the plan remains up-to-date
   - **c)** Determine the maintenance regime to ensure the plan remains up-to-date
   - **d)** Determine the maintenance processes to update the plan
   - **e)** Implement version control procedures to ensure that the plan is maintained up-to-date.

Q. No. 30. Explain BCM training process? (B)

a) An enterprise with BCM uses training as a tool to initiate a culture of BCM in all the stakeholders by:

- **a)** Developing a BCM program more efficiently.
- **b)** Providing confidence in its stakeholders in its ability to handle business disruptions.
- **c)** Increasing its resilience over time by ensuring BCM implications are considered in decisions at all levels.
- **d)** Minimizing the likelihood and impact of disruptions.

b) Development of a BCM culture is supported by:

- **a)** Leadership from senior personnel in the enterprise
- **b)** Assignment of responsibilities;
- **c)** Awareness raising
- **d)** Skills training
- **e)** Exercising plans.

(What competencies are necessary for personnel assigned to specific management responsibilities within the system while developing BCM N16 - 4M)

c) Training, Awareness and Competency:

- **a)** While developing the BCM, the competencies necessary for personnel assigned specific management responsibilities within the system have been determined.
- **b)** These are consistent with the competencies required by the organization of the relevant role and are given as follows:
  - **i)** Actively listens to others, their ideas, views and opinions
  - **ii)** Provides support in difficult or challenging circumstances
  - **iii)** Responds constructively to difficult circumstances
  - **iv)** Promotes a positive culture of health, safety and the environment
  - **v)** Recognizes and acknowledges the contribution of colleagues
  - **vi)** Encourages the taking of calculated risks
  - **vii)** Encourages and actively responds to new ideas
  - **viii)** Consults and involves team members to resolve problems
  - **ix)** Demonstrates personal integrity

Q.No.31. Disaster Recovery plan? (OR) Explain the various general components of Disaster Recovery Plan? (OR) what do you understand by Disaster Recovery Plan? Discuss its various components? (OR) what is 'Disaster Recovery Plan'? Discuss its various components? (OR) what are the components or types of DRP? (A) (PM, M – 99, 01, 05, N – 08, N15-6M)

1. Disaster recovery plan describes the contingency measures that organizations have adopted to recover from, or to prevent any bad event or disaster.

2. The primary objective of a disaster recovery plan is to assure the management would be restored in a set time after any disaster occurs, thereby minimizing losses to the organization.

3. **Types of plans:**

   a) Emergency plan: **(N15 RTP)**

   - **i)** The emergency plan specifies the actions to be undertaken immediately when a disaster occurs.
   - **ii)** Management must identify those situations that require the plan to be invoked for example, major fire, major structural damage, and terrorist attack.
   - **iii)** The actions to be initiated can vary depending on the nature of the disaster that occurs.
   - **iv)** If an organization undertakes a comprehensive security review program, the threat identification and exposure analysis phases involve identifying those situations that require the emergency plan to be invoked.
   - **v)** There are four aspects of the emergency plan must be expressed.
     - First, the plan must show who is to be notified immediately when the disaster occurs - management, police, fire department, medicos, and so on.
     - Second, the plan must show actions to be undertaken, such as shutdown of equipment, removal of files, and termination of power.

- Third, any evacuation procedures required must be specified.
- Fourth, return procedures must be designated.

b) Backup plan:

i) The backup plan specifies

- The type of backup to be kept
- Frequency with which backup is to be undertaken
- Procedures for making backup
- Location of backup resources
- Site where these resources can be assembled and operations restarted
- Personnel who are responsible for gathering backup resources and restarting operations
- Priorities to be assigned to recovering the various systems
- Time frame for recovery of each system.

ii) The backup plan needs continuous updating as changes occur.

c) Recovery plan: **(N15, M16 RTP)**

i) Recovery plans set out procedures to restore full information system capabilities.

ii) The plan should specify the responsibilities of the committee and provide guidelines on priorities to be followed.

iii) The plan might also indicate which applications are to be recovered first.

iv) Members of a recovery committee must understand their responsibilities.

v) Periodically, they must review and practice executing their responsibilities.

vi) If committee members leave the organization, new members must be appointed immediately and briefed about their responsibilities.

d) Test plan: **(RTP N16)**

i) The final component of a disaster recovery plan is a test plan.

ii) The purpose of the test plan is to identify deficiencies in the emergency, backup, or recovery plans.

iii) It must enable a range of disasters to be simulated and specify the criteria by which the emergency, backup, and recovery plans can be deemed satisfactory.

iv) Periodically, test plans must be invoked.

v) To facilitate testing, a phased approach can be adopted.

- Testing by desk checking and inspection and walkthroughs, much like the validation procedures adopted for programs.
- Simulation at a convenient time-for example, during a slow period in the day
- Simulation without warning at any time. These are the ACID tests of the organization's ability to recover from a catastrophe.

Q.No.32. Explain briefly Data Backup techniques? (or) Briefly explain the various types of systems Backup for the system and data together? (A) (PM)

When the back-ups are taken of the system and data together, they are called Total System's Back-up. Various types of back-ups are given as follows:

1. **Full Backup:** **(N14, M15, M16 RTP)**

   a) This is the simplest form of backup.

   b) A Full Backup captures all files on the disk or within the folder selected for backup.

   c) With a full backup system, every backup generation contains every file in the backup set.

   d) At each backup run, all files designated in the backup job will be backed up again. This includes files and folders that have not changed.

   e) *For example - Suppose a full backup job or task is to be done every night from Monday to Friday. The first backup on Monday will contain the entire list of files and folders in the backup job. On Tuesday, the backup will include copying all the files and folders again, no matter the files have got changed or not. The cycle continues this way.*

   i) Advantages

   - Restores are fast and easy to manage as the entire list of files and folders are in one backup set.
   - Easy to maintain and restore different versions.

   ii) Disadvantages **(N16 RTP)**

   - Backups can take very long as each file is backed up again every time the full backup is run.
   - Consumes the most storage space compared to incremental and differential backups. The exact same files are stored repeatedly resulting in inefficient use of storage.

2. **Incremental Backup:** **(N14, N16 RTP, A16 MTP)**

   a) An Incremental Backup captures files that were created or changed since the last backup, regardless of backup type.

   b) The last backup can be a full backup or simply the last incremental backup.

   c) With incremental backups, one full backup is done first and subsequent backup runs are just the changed files and new files added since the last backup.

   d) *For example - Suppose an Incremental backup job or task is to be done every night from Monday to Friday. This first backup on Monday willbe a full backup since no backups have been taken prior to this. However, on Tuesday, the incremental backup will only backup the files that have changed since Monday and the backup on Wednesday will include only the changes and new files since Tuesday's backup. The cycle continues this way.*

   i) Advantages

   - Much faster backups.
   - Efficient use of storage space as files are not duplicated. Much less storage space used compared to running full backups and even differential backups.

   ii) Disadvantages

   - Restores are slower than with a full backup and differential backups.
   - Restores are a little more complicated. All backup sets (first full backup and all incremental backups) are needed to perform a restore.

3. **Differential Backup:**

   a) Differential backups fall in the middle between full backups and incremental backup.

   b) A Differential Backup stores files that have changed since the last full backup.

   c) With differential backups, one full backup is done first and subsequent backup runs are the changes made since the last full backup.

d) Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up.

e) *For example - Suppose a differential backup job or task is to be done every night from Monday to Friday. On Monday, the first backup will be a full backup since no prior backups have been taken. On Tuesday, the differential backup will only backup the files that have changed since Monday and any new files added to the backup folders. On Wednesday, the files changed and files added since Monday's full backup will be copied again. While Wednesday's backup does not include the files from the first full backup, it still contains the files backed up on Tuesday.*

i) Advantages **(RTP M17)**

- Much faster backups then full backups.
- More efficient use of storage space then full backups since only files changed since the last full backup will be copied on each differential backup run.
- Faster restores than incremental backups.

ii) Disadvantages

- Backups are slower then incremental backups.
- Not as efficient use of storage space as compared to incremental backups. All files added or edited after the initial full backup will be duplicated again with each subsequent differential backup.
- Restores are slower than with full backups.
- Restores are a little more complicated than full backups but simpler than incremental backups. Only the full backup set and the last differential backup are needed to perform a restore.

4. Mirror back-up:

a) Mirror backups are, a mirror of the source being backed up.

b) With mirror backups, when a file in the source is deleted, that file is eventually also deleted in the mirror backup.

c) Because of this, mirror backups should be used with caution as a file that is deleted by accident, sabotage or through a virus may also cause that same file in mirror to be deleted as well. Some do not consider a mirror to be a backup.

d) *For example - Many online backup services offer a mirror backup with a 30 day delete. This means that when you delete a file on your source, that file is kept on the storage server for at least 30 days before it is eventually deleted. This helps strike a balance offering a level of safety while not allowing the backups to keep growing since online storage can be relatively expensive. Many backup software utilities do provide support for mirror backups.*

i) Advantages: The backup is clean and does not contain old and obsolete files.

ii) Disadvantages: There is a chance that files in the source deleted accidentally, by sabotage or through a virus may also be deleted from the backup mirror.

Q.No.33. Write about alternative Processing facility arrangements? (or) Describe the general guidelines / tips to be considered in relation to a Backup? (or) Discuss the various backup options considered be Security administrator when arranging alternative Processing facility? (A) (PM, M11, N14 – 4M, M15 - 4M, N15-4M)

1. Cold site: **(RTP N15)**

a) If an organization can tolerate some downtime, cold-site backup might be appropriate.

b) A cold site has all the facilities needed to install a mainframe system-raised floors, air conditioning, power, communication lines, and so on.

c) The hardware and software are not present, and the same must be provided by the organization wanting to use the cold site.

d) An organization can establish its own cold-site facility or enter into an agreement with another organization to provide a cold-site facility.

2. **Warm site:**

a) A warm site provides an intermediate level of backup.

b) It has all cold-site facilities plus hardware that might be difficult to obtain or install.

c) For example, a warm site might contain selected peripheral equipment plus a small mainframe with sufficient power to handle critical applications in the short run.

3. **Hot site:** **(RTP N15)**

a) If fast recovery is critical, an organization might need hot site backup.

b) All hardware and operations facilities will be available at the hot site.

c) In some cases software, data and supplies might also be stored there.

d) A hot site is expensive to maintain.

e) They are usually shared with other organizations that have hot-site needs.

4. **Reciprocal agreement:**

a) Two or more organizations might agree to provide backup facilities to each other in the event of one suffering a disaster.

b) This backup option is relatively cheap, but each participant must maintain sufficient capacity to operate another's critical system.

c) If a third-party site is to be used for backup and recovery purposes, security administrators must ensure that a contract is written.

Q.No.34. What are the aspects to be considered in the audit of BCP/DRP? (B)
(PM, N14-6M, M15-4M, M16-6M, N15 RTP)

The objective of BCP audit is to assess the ability of the enterprise to continue all critical operations during a contingency and recover from a disaster within the defined critical recover time period. BCP Auditor is expected to identify residual risks, which are not identified and provide recommendations to mitigate them.

Sample list of BCP Audit steps:

1. **sound and Robust Methodology: Refer Q.No.35**
2. Determine if information backup procedures are sufficient to allow for recovery of critical data.
3. Determine if a test plan exists and to what extent the disaster recovery/business resumption plan has been tested.
4. Determine if resources have been made available to maintain the disaster recovery/ business resumption plan and keep it current.
5. Obtain and review the existing disaster recovery/ business resumption plan.
6. Obtain and review plans for disaster recovery/ business resumption testing and/or documentation of actual tests
7. Obtain and review the existing business impact analysis.
8. Determine if copies of the plan are safeguarded by off-site storage.
9. Gain an understanding of the methodology used to develop the existing disaster recovery/ business resumption plan. Who participated in the development effort?

10. Gain an understanding of the methodology used to develop the existing business impact analysis.
11. Determine if recommendations made by the external firm who produced the business impact analysis have been implemented or otherwise addressed.
12. Have resources been allocated to prevent the disaster recovery/ business resumption plan from becoming outdated and ineffective?
13. Determine if the plan is updated each time that it is revised so that the most current version will be used if needed.
14. Determine if the plan has been updated within past 12 months.
15. Determine all the locations where the disaster recovery/ business resumption plan is stored. Are there a variety of locations to ensure that the plan will survive disasters and will be available to those that need them?
16. Review information backup procedures in general. The availability of backup data could be critical in minimizing the time needed for recovery.
17. **Interview functional area managers or key employees: Refer Q.No.36**
18. **Building, Utilities and Transportation: Refer Q.No. 37**
19. **Information Technology: Refer Q.No. 38**
20. **Administrative Procedure: Refer Q.No. 39**
21. Does the disaster recovery/ business resumption plan include the names and numbers of suppliers of essential equipment and other material?
22. Does the disaster recovery/ business resumption plan include provisions for the approval to expend funds that were not budgeted for the period? Recovery may be costly.
23. Has executive management assigned the necessary resources for plan development, concurred with the selection of essential activities and priority for recovery, agreed to back-up arrangements and the costs involved, and are prepared to authorize activation of the plan should the need arise.

Q.No.35. How an auditor will determine that the disaster recovery planned was developed using a sound and Robust Methodology? Explain. (A) (N13-6M)

Determine if a disaster recovery/business resumption plan exists and was developed using a sound methodology that includes the following elements:

a) Identification and prioritization of the activities which are essential to continue functioning.

b) The plan is based upon a business impact analysis that considers the impact of the loss of essential functions.

c) Operations managers and key employees participated in the development of the plan.

d) The plan identifies the resources that will likely be needed for recovery and the location of their availability.

e) The plan is simple and easily understood so that it will be effective when it is needed.

f) The plan is realistic in its assumptions.

Q.No.36. While Auditing the Disaster recovery plan how an Auditor determines that Employees have a clear understanding of their role in working towards the resumption of normal operations? (B)

Auditor has to interview functional area managers or key employees to determine their understanding of the disaster recovery/ business resumption plan through interviewing as follows:

a) Does the disaster recovery/ business resumption plan include provisions for Personnel

b) Have key employees seen the plan and are all employees aware that there is such plan?

c) Have employees been told their specific roles and responsibilities if the disaster recovery/ business resumption plan is put into effect?

d) Does the disaster recovery/ business resumption plan include contact information of key employees, especially after working hours?

e) Does the disaster recovery/ business resumption plan include provisions for people with special needs?

f) Does the disaster recovery/ business resumption plan have a provision for replacement staff when necessary?

Q.No.37. How an auditor will determine that the disaster recovery planned was developed using Building, Utilities and Transportation? Explain. (B) (RTP M17)

a) Does the disaster recovery/ business resumption plan have a provision for having a building engineer inspect the building and facilities soon after a disaster so that

b) Damage can be identified and repaired to make the premises safe for the return of employees as soon as possible?

c) *Does the disaster recovery/business resumption plan consider the need for alternative shelter, if needed? Alternatives in the immediate area may be affectedly the same disaster.*

d) Review any agreements for use of backup facilities.

e) Verify that the backup facilities are adequate based on projected needs (telecommunications, utilities, etc.). Will the site be secure?

f) Does the disaster recovery/ business resumption plan consider the failure of electrical power, natural gas, toxic chemical containers, and pipes?

g) Are building safety features regularly inspected and tested?

h) *Does the plan consider the disruption of transportation systems? This could affect the ability of employees to report to work or return home. It could also affect the ability of vendors to provide the goods needed in the recovery effort.*

Q.No.38. While auditing a Disaster Recovery Plan (DRP) for information Technology (IT) Assets, What concerns are required to be addressed? Briefly explain? (A) (M14 - 4M)

a) Determine if the plan reflects the current IT environment.

b) Determine if the plan includes prioritization of critical applications and systems.

c) Determine if the plan includes time requirements for recovery/availability of each critical system, and that they are reasonable.

d) Does the disaster recovery/ business resumption plan include arrangements for emergency telecommunications?

e) *Is there a plan for alternate means of data transmission if the computer network is interrupted? Has the security of alternate methods been considered?*

f) *Determine if a testing schedule exists and is adequate (at least annually). Verify the date of the last test. Determine if weaknesses identified in the last tests were corrected.*

Q.No.39. How an auditor will determine that the disaster recovery planned was developed using Administrative Procedure ? Explain. (B) (RTP N15)

a) Does the disaster recovery/ business resumption plan cover administrative and management aspects in addition to operations? Is there a management plan to maintain operations if the building is severely damaged or if access to the buildings denied or limited for an extended period of time?

b) Is there a designated emergency operations center where incident management teams can coordinate response and recovery?

c) *Determine if the disaster recovery/ business resumption plan covers procedures for disaster declaration, general shutdown and migration of operations to the backup facility.*

d) *Have essential records been identified? Do we have a duplicate set of essential records stored in a secure location?*

To facilitate retrieval, are essential records separated from those that will not be needed immediately

Q.No.40. A company has decided to outsource its recovery process to a third party site. What are the issues that should be considered by the Security administrators while drafting the contract? (A) (PM, M10-5M, RTP N15, MTP M16)

If a third-party site is to be used for recovery purposes, security administrators must ensure that a contract is written to cover the following issues:

1. How soon the site will be made available subsequent to a disaster;
2. The number of organizations that will be allowed to use the site concurrently in the event of a disaster;
3. The priority to be given to concurrent users of the site in the event of a common disaster;
4. The period during which the site can be used;
5. The conditions under which the site can be used;
6. The facilities and services the site provider agrees to make available;
7. Procedures to ensure security of company's data from being accessed/damaged by other users of the facility
8. What controls will be in place for working at the off-site facility.

Q.No.41. Describe Contents of a Disaster recovery and planning document. (A) (PM, M14, N15 RTP, O15 MTP)

The disaster recovery planning document may include the following areas:

1. The conditions for activating the plans, which describe the process to be followed before each plan, are activated.
2. Emergency procedures, which describe the actions to be taken following an incident which jeopardizes business operations and/or human life. This should include arrangements for public relations management and for effective liaisoning with appropriate public authorities e.g. police, fire, services and local government.
3. 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.
4. Resumption procedures, which describe the actions to be taken to return to normal business operations.

5. A maintenance schedule, which specifies 'how and when the plan will be tested', and the process for maintaining the plan.
6. 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.
7. The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
8. Contingency plan document distribution list.
9. Detailed description of the purpose and scope of the plan.
10. Contingency plan testing and recovery procedure.
11. List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
12. Checklist for inventory taking and updating the contingency plan on a regular basis.
13. List of phone numbers of employees in the event of an emergency.
14. Emergency phone list for fire, police, hardware, software, suppliers, customers, back-up location, etc.
15. Medical procedure to be followed in case of injury.
16. Back-up location contractual agreement, correspondences.
17. Insurance papers and claim forms.
18. Primary computer centre hardware, software, peripheral equipment and software configuration.
19. Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
20. Alternate manual procedures to be followed such as preparation of invoices.
21. Names of employees trained for emergency situation, first aid and life saving techniques.
22. Details of airlines, hotels and transport arrangements.

Q.No.42. While doing audit or self assessment of the BCM Program of an enterprise, briefly describe the matters to be verified. (OR) As an IS auditor, what are the key areas you would verify during review of BCM arrangements of an enterprise. (A)
(PM, N14-6M, M15-4M, M15 RTP, S15 MTP)

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

a) All key products and services and their supporting critical activities and resources have been identified and included in the enterprise's BCM strategy;

b) The enterprise's BCM policy, strategies, framework and plans accurately reflect its priorities and requirements;

c) The enterprise' BCM competence and its BCM capability are effective and fit –for purpose and will permit management, command, control and coordination of an incident;

d) The enterprise's BCM solutions are up-to-date and appropriate to the level of risk faced by the enterprise;

e) The enterprise's BCM maintenance and exercising programs have been effectively implemented;

f) BCM strategies and plans incorporate improvements that have been identified during incidents and exercises and in the maintenance program;

g) The enterprise has an ongoing program for BCM training and awareness;

h) BCM procedures have been effectively communicated to relevant staff, and that those staff understand their roles and responsibilities; and

i) Change control processes are in place and operate effectively.

THE END

5. ACQUISITION, DEVELOPMENT AND IMPLEMENTATION OF INFORMATION SYSTEM

Q.NO.1. WHAT IS BUSINESS PROCESS DESIGN? WHAT ARE THE STEPS INVOLVED IN IT? (B)

1. Business process design means structuring or restructuring the tasks, functionalities and activities for improvising a business system.
2. It is a critical step to understand the requirements of the system.
3. Business Process Design involves following sequence of the steps:

a) **Analysis of Present Process Documentation:**

i) The purpose of this phase is to analyze each present business process to determine if the processes is necessary and what problem might exists in that business process .

ii) *It includes the following activities:*

- *Understanding the business and the objectives for which it exists;*
- *Documenting the existing business processes; and*
- *Analysis of the documented processes.*

b) **Designing Proposed Process Documentation:**

i) This step is to design the new process requirements for the system. The design is based on the new system requirements and the changes proposed.

ii) *It includes the following activities:*

- *Understanding of the business processes necessary to achieve the business objectives;*
- *Designing the new processes;*
- *Documentation of the new process, preferably using of CASE tools.*

c) **Implementation of New Process:**

i) This step is to implement new and modified business processes at the entity are authorized, tested and implemented in the organization.

ii) *The critical activities may include the following:*

- *Validating the new process;*
- *Implementing the new process*
- *Testing the new process.*

Q.NO.2. WHAT IS SYSTEMS DEVELOPMENT PROCESS? (B) (RTP N16)

1. **System Development** refers to the process of examining a business situation with the intent of improving it through better procedures and methods.
2. System development generally consists of two major components: System Analysis and System Design.

a) **System Analysis** is the process of gathering and interpreting facts, diagnosing problems, and using the information to recommend improvements to the system.

b) **System Design** is the process of planning/modeling a new business system or one to replace or complement an existing system.

3. Before planning can be done, everyone must thoroughly understand the old system and determine how computers can be used to make its operation more effective.

Q.NO.3. WHY ORGANIZATIONS FAILS TO ACHIEVE THEIR SYSTEM DEVELOPMENT OBJECTIVES? (OR) BRING OUT THE REASONS AS TO WHY ORGANIZATIONS FAIL TO ACHIEVE THEIR SYSTEMS DEVELOPMENT OBJECTIVES? (OR)
MANY – A – TIME ORGANIZATIONS FAIL TO ACHIEVE THEIR SYSTEM DEVELOPMENT OBJECTIVES. JUSTIFY THE STATEMENT GIVING REASONS. (A) (PM, M15 - 6M, RTP N16, N14)

There are many reasons why organizations fail to achieve their systems development objectives. Some of them are as follows:

1. **User Related Issues: (RTP N15)**
   a) *It refers to those issues where user/customer is estimated as the primary agent.*
   b) *Some of the aspects with regard to this problem are mentioned as follows:*
      i) **Shifting User Needs:** when user's requirements are constantly changing, more requests for systems development.
      ii) **Resistance to Change:** People have a natural tendency to resist change, hence they should be educated for the benefits of intended system.
      iii) **Lack of User Participation:** User participation also helps reduce user resistance to change. If users are not involved in the development effort, they may not feel responsible for the success of the project.
      iv) **Inadequate Testing and User Training:** New systems must be tested before installation to determine that they operate correctly. Users must be trained to effectively utilize the new system.

2. **Developer Related Issues:**
   a) *It refers to the issues and challenges with regard to the developers.*
   b) *Some of the critical bottlenecks are mentioned as follows:*
      i) **Lack of standard project management and systems development methodologies:** Some organizations do not formalize their project management and systems development methodologies, thereby making it very difficult to consistently complete projects on time or within budget.
      ii) **Overworked or under-trained development staff:** In many cases, systems developers often lack sufficient education background and many companies do little to help their development personnel stay technically sound.

3. **Management Related Issues:**
   a) *It refers to the area that regard to organizational set up, administrative and overall management to accomplish the system development goals.*
   b) *Some of such bottlenecks are mentioned as follows:*
      i) **Lack of senior management support and involvement:** Top management should be closely associated with MIS from beginning. Lack of top management involvement contributes to poor MIS performance.
      ii) **Development of strategic systems:** Since strategic decision making is unstructured, they require flexibility and also mapping may not be possible.

4. **New technologies:** When an organization tries to create a competitive advantage by applying advance technologies, it generally finds that attaining system development objectives is more difficult because personnel are not as familiar with the technology.

Q.NO.4. WRITE ABOUT SYSTEM DEVELOPMENT TEAM? (B)

1. Several people in the organization are responsible for systems development.
2. Project is decided by a top management level steering committee, usually consisting of a group of key Information Systems services users that acts as a review body for Information Systems plans and applications development.
3. A project management team generally consists of both computer professionals and key users.
4. System analysts are subsequently assigned to determine user requirements, design the system and assist in development and implementation activities.
5. In end-user developed systems, the end-user is ultimately responsible for the system.
6. Most accountants are uniquely qualified to participate in systems development activity associated with knowledge of IT, business, accounting, and internal control.
7. The steering committee ensures that ongoing systems development activities are consistently aimed at satisfying the information requirements of managers and users within the organization.

Q.NO.5. WRITE ABOUT ACCOUNTANT'S INVOLVEMENT IN DEVELOPMENT WORK? (B) (MTP M17 5M, M16 4M, N15)

1. Most 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.
2. They have specialized skills such as accounting and auditing that can be applied to the development project.
3. **An accountant can help in various related aspects during system development; some of them are as follows:**

   a) Return on Investment (referred as ROI):

   i) This defines the return, an entity shall earn on a particular investment i.e. capital expenditure.

   ii) The important data required for this analysis being the cost of project, the expected revenue/benefit for a given period.

   iii) For this analysis following data needs to be generated. **(RTP M17)**

   - **Cost:** This includes estimates for typical costs involved in the development, which are given as follows:
     - **Development Costs:** Development Costs for a computer based information system include costs of the system development process, like salaries of developers.
     - **Operating Costs:** Operating Costs of a computer based information system including hardware/software rental or depreciation charges; salaries of computer operators and other data processing personnel, who will operate the new system.
     - **Intangible Costs:** Intangible Cost that cannot be easily measured. For example, the development of a new system may disrupt the activities of an organization and cause a loss of employee productivity or morale.
   - **Benefits:**
     - The benefits, which result from developing new or improved information systems that can be subdivided into tangible and intangible benefits.

- A post implementation analysis is also done to see how the system development effort has benefitted the organization.

b) Computing Cost of IT Implementation and Cost Benefit Analysis:

i) For analysis of ROI, accountants need the costs and returns from the system development efforts.

ii) For correct generation of data, proper accounting needs to be done.

iii) Accountants shall be the person to whom management shall look for the purpose.

c) Skills expected from an Accountant:

i) An accountant, being an expert in accounting field must possess skills to understand the system development efforts and nuances of the same.

ii) They are expected to have various key skills, including understanding of the business objectives, expert book keeper, and understanding of system development efforts etc.

Q.NO.6. EXPLAIN SYSTEMS DEVELOPMENT METHODOLOGY? (A) (MTP N15 – 4M)

1. A system development methodology is a formalized, standardized, documented set of activities used to manage a system development project.

2. It refers to the framework that is used to structure, plan and control the process of developing an information system.

3. The methodology is characterized by the following:

a) The project is divided into a number of identifiable processes, and each process has a starting point and an ending point.

b) Each process comprises several activities, one or more deliverables, and several management control points.

c) Specific reports and other documentation, called Deliverables must be produced periodically during system development.

d) Users, managers, and auditors are required to participate in the project. which generally provide approvals, often called signoffs, at pre-established management control points.

e) The system must be tested thoroughly prior to implementation to ensure that it meets users' needs.

f) A training plan is developed for those who will operate and use the new system.

g) A post-implementation review of all developed systems must be performed to assess the effectiveness and efficiency of the new system.

Q.NO.7. WHAT ARE VARIOUS APPROACHES TO SYSTEM DEVELOPMENT? (A)

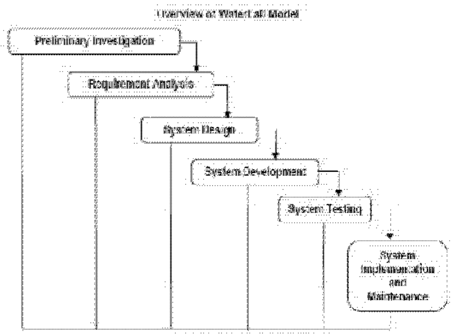
Several system development approaches are often used within an organization.

Approach	Framework	Concept
Traditional Approach	Linear	Step by step
Prototyping	Iterative	First module created with no controls etc - Then controls improved and first module completed in totality - Then other modules
The Incremental Model	Combination of Linear and Iterative	Here also we start with first module, which is a Prototype (Like in Prototyping) - But within that module, all stages of SDLC are tested (Like in Traditional approach)

Spiral Model	Combination of Linear and Iterative	Development is started with first two stages (Like in Traditional), but if it is felt going on next stages maybe risky, shift is made to Prototyping (Like in Prototyping)
Rapid Application Development (RAD)	Iterative	Faster version of Prototyping where planning of software developed using RAD is interleaved with writing the software itself
Agile Methodologies	Combination of Linear and Iterative	All stages of SDLC are followed up, and the project is delivered to the customer. Then new subproject is developed and integrated in to the already delivered system.

Q.NO.8. EXPLAIN THE TRADITIONAL / WATERFALL APPROACH / SEQUENTIAL APPROACH? (OR) DISCUSS THE KEY CHARACTERISTICS OF WATERFALL MODEL IN BRIEF. ALSO EXPLAIN ITS MAJOR WEAKNESSES. (A) (PM)

1. The waterfall approach is a traditional development approach in which each developer in a development team works in different phases.
2. These phases include requirement analysis, specifications and design requirements, coding, final testing, and release.
3. The waterfall approach is used on small projects because it eliminates testing to identity problems early in the process.
4. In the traditional approach of system development, all the activities are performed in sequence.
5. When the traditional approach is applied, an activity is undertaken only when the prior step is fully completed.


Overview of Waterfall Model
Preliminary Investigation
Requirement Analysis
System Design
System Development
System Testing
System Implementation and Maintenance

Steps in Traditional Approach

Framework type: Linear

BASIC PRINCIPLES/ KEY CHARACTERISTICS:

1. Project is divided into sequential phases, with some overlap and splash back acceptable between phases.
2. Emphasis is on planning, time schedules, target dates, budgets and implementation of an entire system at one time.
3. 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/signoffs.

STRENGTHS:

1. Simple to understand
2. Minimal resources required
3. Works for well-understood problems
4. Progress of system development is measurable.
5. Ideal for supporting less experienced project teams and project managers or project teams whose composition fluctuates.
6. Quality, reliability, adequacy and maintainability of the developed software.

WEAKNESSES: **(RTP M15) (MTP N16 – 4M)**

1. Produces inaccurate estimates
2. Slow, costly, and cumbersome due to significant structure and tight controls.

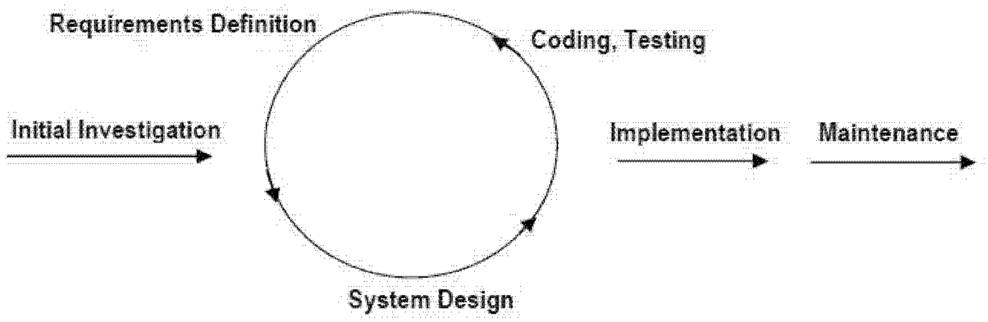
3. Not flexible
4. does not allow for changing requirements
5. Project progresses forward, with only slight movement backward.
6. Real projects rarely follow the sequential flow and iterations in this model are handled indirectly.
7. Problems are often not discovered until system testing.
8. System performance cannot be tested until the system is almost fully coded.
9. It produces excessive documentation which results in ambiguity

Projects where Waterfall Method is suitable for SDLC:

1. In development of database-related software, eg commercial projects.
2. In development of E-commerce website or portal.
3. In Development of network protocol software.

Q.NO.9. EXPLAIN THE PROTOTYPING APPROACHES TO SYSTEMS DEVELOPMENT? (OR) DESCRIBE THE PROTOTYPING MODEL OF SYSTEM DEVELOPMENT. EXPLAINING THE GENERIC PHASES OF THIS MODEL? (A) (M16 - 6M) (OR) DISCUSS THE FOUR STEPS OF THE PROTOTYPING APPROACH IN SYSTEM DEVELOPMENT? (OR) WHAT IS PROTOTYPING APPROACHES TO SYSTEMS DEVELOPMENT? DESCRIBE ITS ADVANTAGES AND DISADVANTAGES? (PM, M - 00, N - 02, M - 04, M – 07, MTP N16 – 6M]

1. The traditional approach sometimes may take years to analyze, design and implement a system.
2. In order to avoid such delays, organizations are increasingly using prototyping techniques to develop systems such as DSS, MIS and Expert systems.
3. The goal of prototyping approach is to develop a small or pilot version called a prototype of part or all of a system.
4. A prototype is a usable system or system component that is built quickly and at a lesser cost, and with the intention of being modifying or replacing it by a full-scale and fully operational system.
5. As users work with the prototype, they make suggestions and these suggestions are then incorporated into another prototype, so that high quality product can be implemented.
6. Finally, when a prototype is developed that satisfies all user requirements, either it is refined and turned into the final system or it is scrapped.



Prototyping Model

Framework type: Iterative.

GENERIC PHASES/BASIC PRINCIPLES: Prototyping can be viewed as a series of four steps. Wherein Implementation and Maintenance phases take place once the prototype model is tested and found to be meet users requirements.

Identify Information System Requirements:

1. *In traditional approach, the system requirements have to be identified before the development process starts.*
2. In Prototype approach, the design team needs only fundamental system requirements to build the initial prototype, the process of determining them can be less formal and time-consuming than when performing traditional systems analysis.

Develop the Initial Prototype:

In this step, the designers create an initial base model and give little or no consideration to internal controls, but instead emphasize such system characteristics such as simplicity, flexibility, and ease of use.

Test and Revise:

After finishing the initial prototype, the designers first demonstrate the model to users and then give it to them to experiment and ask users to record their likes and dislikes about the system and recommend changes.

Obtain User Signoff of the Approved Prototype:

At the end of Step 3, users formally approve the final version of the prototype, which commits them to the current design and establishes a contractual obligation about what the system will, and will not, do or provide.

STRENGTHS/ADVANTAGES: [Describe major strengths of Prototyping model]

(M16 – 6M, RTP N14, MTP M17 – 6M, N15)

1. Improves both user participation in system development and communication among project stakeholders.
2. When prototype is shown to the user, he gets a proper clarity and 'feel' of the functionality of the software and he can suggest changes and modifications.
3. Helps to easily identify confusing or difficult functions and missing functionality.
4. Iteration between development team and client provides a very good and conductive environment during project.
5. May generate specifications for a production application.
6. Provides quick implementation of an incomplete, but functional application.
7. It reduces risk of failure.

WEAKNESSES/DISADVANTAGES: **(RTP M-14)**

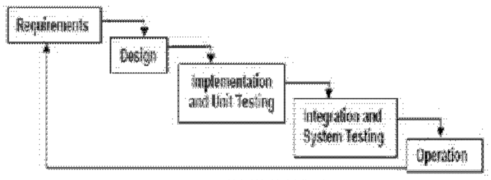
1. Approval process and control are not strict.
2. Requirements may frequently change significantly.
3. Identification of non-functional elements are difficult to document.
4. The Iterative process of prototyping causes the prototype to be experimented with quite extensively.
5. Prototyping may cause behavioral problems with system users.
6. Too much involvement of client is not always preferred by the developer.
7. Too many changes can disturb the rhythm of the development team.

Q.NO.10. WRITE ABOUT THE INCREMENTAL MODEL? DISCUSS ITS STRENGTHS AND WEAKNESS ALSO. (A) (PM)

Framework Type: Combination Linear and Iterative.

BASIC PRINCIPLES:

1. The Incremental build model is a method of software development where the model is designed, implemented and tested incrementally until the product is finished.
2. The product is defined as finished when it satisfies all of its requirements.
3. This model combines the elements of the waterfall model with the iterative philosophy of prototyping.
4. The product is decomposed into a number of components, each of which are designed and built separately (termed as builds).
5. Each component is delivered to the client when it is complete.


Requirements
Design
Implementation and Unit Testing
Integration and System Testing
Operation

Incremental Model

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

STRENGTHS:

1. More flexible - less costly to change scope and requirements.
2. Potential exists for exploiting knowledge gained in an early increment as later increments are developed.
3. Moderate control is maintained over the life of the project through the use of written documentation and the formal review and approval/signoff by the user and information technology management at designated major milestones.
4. Easier to test and debug during a smaller iteration.
5. It allows the delivery of a series of implementations that are gradually more complete and can go into production more quickly as incremental releases.
6. It helps to mitigate integration and architectural risks earlier in the project.
7. Gradual implementation provides the ability to monitor the effect of incremental changes.

WEAKNESSES:

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

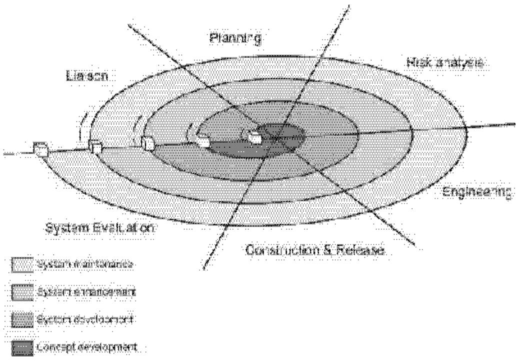
Q.NO.11. AS A PERSON IN-CHARGE OF SYSTEMS DEVELOPMENT LIFE CYCLE, YOU ARE ASSIGNED A JOB OF DEVELOPING A MODEL FOR A NEW SYSTEM WHICH COMBINES THE FEATURES OF A PROTOTYPING AND THE WATERFALL MODEL. WHICH WILL BE THE MODEL OF YOUR CHOICE AND WHAT ARE ITS STRENGTHS AND WEAKNESSES? (N10)

(OR)

EXPLAIN THE ABOUT SPIRAL MODEL? EXPLAIN MAJOR STRENGTHS AND WEAKNESSES OF SPIRAL MODEL (A) (PM)

Framework Type: Combination Linear and Iterative.

1. <u>**BASIC PRINCIPLES:**</u> The Spiral model is a <u>software development process</u> combining elements of both design and prototyping-in-stages, which <u>combines advantages of top-down and bottom-up</u> concepts. It is a Systems Development Method (SDM) which combines the features of the <u>prototyping model and the waterfall model.</u>



2. It is known as the Spiral Lifecycle.
3. A list of pertinent characterizing features includes the following:
   - **a.** 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.
   - **b.** A preliminary design is created for the new system. This phase is the most important part of "Spiral Model" in which all possible alternatives, that can help in developing a cost effective project are analyzed and strategies are decided to use them.
   - **c.** A first prototype of the new system in constructed from the preliminary design. This is usually a scaled-down system, and represents an approximation of the characteristics of the final product.
   - **d.** A second prototype is evolved by a fourfold procedure which includes evaluating the first prototype, defining the requirements, planning and designing, and constructing and testing the second prototype.
4. 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.

Q.NO.12. EXPLAIN MAJOR STRENGTHS AND WEAKNESSES OF SPIRAL MODEL (A) (PM)

<u>STRENGTHS:</u>

1. Spiral Life Cycle Model is one of the <u>most flexible</u> and <u>Development phases</u> can be determined by the project manager, according to the complexity of the project.
2. <u>Project monitoring</u> is <u>very easy and effective</u>.
3. It is suitable for <u>high risk projects</u>, where business needs may be unstable.
4. Useful in helping to select the <u>best methodology</u> to follow for development of a given software iteration based on project risk.
5. <u>Changes</u> can be introduced later in the life cycle as well. And coping with these changes isn't a very big headache for the <u>project manager</u>.

<u>WEAKNESSES:</u> **(MTP N16 – 4M) RTP M14)**

1. It is challenging to determine the <u>exact composition</u> of development methodologies to use for each <u>iteration</u> around the Spiral.

2. It may prove highly customized to each project, and thus is quite complex and limits reusability.
3. A skilled and experienced project manager is required to determine how to apply it to any given project.
4. No established controls exist for moving from one cycle to another cycle. Without controls, each cycle may generate more work for the next cycle.
5. There are no firm deadlines, cycles continue with no clear termination condition leading to, inherent risk of not meeting budget or schedule.

Q.NO.13 WRITE ABOUT RAPID APPLICATION DEVELOPMENT (RAD)? (A)

1. Rapid Application Development (RAD) refers to a type of software development methodology; which uses minimal planning in favor of rapid prototyping.
2. The planning of software developed using RAD is interleaved with writing the software itself. The lack of extensive pre-planning generally allows software to be written much faster, and makes it easier to change requirements.
3. Key features include the following:
   - a) Key objective is fast development and delivery of a high quality system at a relatively low investment cost,
   - b) Attempts to reduce inherent project risk by breaking a project into smaller segments and providing more ease-of-change during the development process.
   - c) Aims to produce high quality systems quickly, primarily through the use of iterative Prototyping (at any stage of development), active user involvement, and computerized development tools. Graphical User Interface (GUI) builders, Computer Aided Software Engineering (CASE) tools, Database Management Systems (DBMS), Fourth generation programming languages, Code generators and object-oriented techniques etc.
   - d) Key emphasis is on fulfilling the business need while technological or engineering excellence is of lesser importance.
   - e) Project control involves prioritizing development and defining delivery deadlines or "timeboxes."
   - f) If the project starts to slip, emphasis is on reducing requirements to fit the timebox, not in increasing the deadline.
   - g) Generally includes Joint Application Development (JAD), where users are intensely involved in system design, either through consensus building in structured workshops, or through electronically facilitated interaction.
   - h) Active user involvement is imperative.
   - i) Iteratively produces production software, as opposed to a throwaway prototype.
   - j) Produces documentation necessary to facilitate future development and maintenance.
   - k) Standard systems analysis and design techniques can be fitted into this framework.

STRENGTHS:

1. The operational version of an application is available much earlier than with_Waterfall, Incremental, or Spiral frameworks.
2. Because RAD produces systems more quickly and to a business focus, this_approach tends to produce systems at lower cost.
3. Quick initial reviews are possible.
4. Constant integration isolates problems and encourages customer feedback.

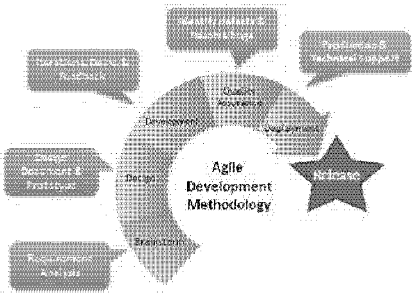
5. It holds a great level of commitment from stakeholders, both business and technical, than Waterfall, Incremental, or spiral frameworks
6. It concentrates on essential system elements from user viewpoint.
7. It provides for the ability to rapidly change system design as demanded by users.
8. It leads to a tighter fit between user requirements and system specifications.

WEAKNESSES: **(RTP M15)**

1. More speed and lower cost may lead to a lower overall system quality.
2. The project may end up with more requirements than needed (gold-plating).
3. Potential for designed system to lack scalability.
4. Potential for inconsistent designs within and across systems
5. It may call for violation of programming standards related to inconsistent naming conventions and inconsistent documentation,
6. It may call for lack of attention to later system administration needs built into_system.
7. Formal reviews and audits are more difficult to implement than for a complete_system.
8. Difficulty with module reuse for future systems.
9. Since some modules will be completed much earlier than others, well–defined interfaces are required.

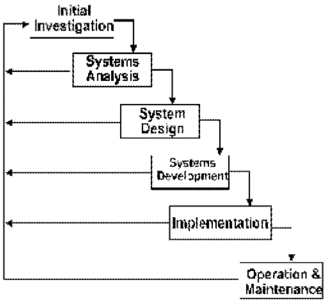
Q.NO.14. EXPLAIN AGILE METHODOLOGIES? (OR) WHAT DO YOU UNDERSTAND BY AGILE MODEL OF SOFTWARE DEVELOPMENT? ALSO EXPLAIN ITS MAJOR STRENGTHS AND WEAKNESSES IN BRIEF. (A) (PM, N14 – 6M, RTP N16, N14, N13)

1. Agile software development is a group of software development methods based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams.
2. It promotes adaptive planning, evolutionary development and delivery; time boxed iterative approach and encourages rapid and flexible response to change.
3. It is a conceptual framework that promotes foreseen interactions throughout the development life cycle.



4. Following are considered as the key features of the agile methodologies:
   a) Customer satisfaction by rapid delivery of useful software;
   b) Welcome changing requirements, even late in development;
   c) Working software is delivered frequently
   d) Working software is the principal measure of progress;
   e) Sustainable development, able to maintain a constant pace;
   f) Close, daily co-operation between business people and developers;
   g) Face-to-face conversation is the best form of communication (co-location);
   h) Projects are built around motivated individuals, who should be trusted;
   i) Continuous attention to technical excellence and good design;
   j) Simplicity;
   k) Self-organizing teams
   l) Regular adaptation to changing circumstances.

STRENGTHS: **(RTP M16, MTP N16 – 4M, N14)**



1. Agile methodology has the concept of an adaptive team, which enables to responds to the changing requirements.
2. Face to face communication and continuous inputs from customer representative leaves a little space for guesswork.
3. The documentation is rigid and to the point to save time.
4. The end result is generally the high quality software in least possible time duration and satisfied customer.
5. 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.

WEAKNESSES: **(RTP M14, MTP N14)**

1. There is lack of emphasis on necessary designing and documentation.
2. In case of some large software deliverables, it is difficult to assess the efforts required at the beginning of the software development life cycle.
3. Agile increases potential threats to business continuity and knowledge transfer.
4. Agile requires more re-work.
5. Agile lacks the attention to outside integration.
6. The project can easily get taken off track if the customer representative is not clear about the final outcome.

Q.NO.15. EXPLAIN SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) IN DETAIL? (N15 – 4M) (N07, 08)

(OR)

DISCUSS THE VARIOUS ACTIVITIES WHICH ARE PART OF THE SYSTEM DEVELOPMENT LIFE CYCLE?

(OR)

STATE AND BRIEFLY EXPLAIN THE SIX STAGES OF A SYSTEM DEVELOPMENT LIFE CYCLE? (A) (PM)

1. The System Development Life Cycle (SDLC) framework provides system designers and developers to follow a sequence of activities.
2. It consists of a set of steps or phases in which each phase of the SDLC uses the results of the previous one.
3. A phase of the SDLC is not complete until the appropriate documentation or artifact is produced also known as deliverables.
4. A deliverable may be a substantial written document, a software artifact, a system test plan or even a physical object such as a new piece of technology that has been ordered and delivered.
5. The SDLC can also be viewed from a more process oriented perspective.

PHASES OF SYSTEM DEVELOPMENT LIFE CYCLE:

1. **Preliminary Investigation:**
   a) Preliminary investigation is the first step in the system development projects. It is a way to handle the user request for change, improve or enhance an existing system.
   b) It determines and evaluates the strategic benefits of the system and ensure that the solution fits the business strategy. It also includes cost-benefit analysis of the proposed system.
2. **Systems Requirements Analysis:** Analyzing the present system involves collecting, organizing and evaluating facts about the system and the environment in which it operates.

3. **System Design:** Designing the system in terms of user interface, data storage and data processing functions. The goal of design is to transform the requirement specifications into a structure that is suitable for implementation in some programming language.
4. **Systems Development / Programming:** Once the system specifications are understood and designed, the required system is to be physically constructed. In this phase the required programs are coded, debugged and documented.
5. **Systems Testing:** Before the implementation of a system, it must be thoroughly tested to avoid any errors it ensures that system will not fail while running actually and it will function as per the requirements specification.

   Various kinds of testing are conducted such as Unit Testing, Integration Testing and System Testing etc.
6. **Systems Implementation:** It includes implementation of hardware and software through site preparation, user training and installation of developed system. It is a critical phase in SDLC because it requires many critical conversions from old to new system like data and procedure conversion.
7. **Post Implementation Review and Maintenance:** Post Implementation review evaluates, measures, compares the original objectives defined. Maintenance includes continuous evaluation of the system as it functions in the live environment and its updation.

Q.NO.16. WHAT ARE THE ADVANTAGES OF USING SDLC. (B) (PM)

The SDLC can be seen as a systematic process oriented system development framework. The advantages of using SDLC are:

1) Better planning and control by project managers.
2) Compliance to prescribed standards ensuring better quality.
3) Documentation that SDLC stresses on is an important measure of communication and control.
4) The phases are important milestones and help the project manager and the user for review and signoff.

Q.NO.17. FROM THE PERSPECTIVE OF IS AUDIT, WHAT ARE THE ADVANTAGES OF SYSTEM DEVELOPMENT LIFE CYCLE? (OR) WHAT THE POSSIBLE ADVANTAGES OF SDLC FROM THE PERSPECTIVE ARE OF IS AUDIT? (B) (PM, N – 10, RTP N – 14, MTP M16 – 6M)

1. The IS auditor can have clear understanding of the various phases of the SDLC on the basis of the detailed documentation created during each phase of the SDLC.
2. The IS Auditor on the basis of his examination, can state in his report about the compliance by the IS management of the procedures, if any, set by the management.
3. The IS Auditor, if has a technical knowledge and ability of the area of SDLC, can be a guide during the various phases of SDLC.
4. The IS auditor can provide an evaluation of the methods and techniques used through the various development phases of the SDLC.

Q.NO.18. WRITE THE SOME OF THE SHORTCOMINGS AND ANTICIPATED RISKS ASSOCIATED WITH THE SDLC? (B)

1. The development team may find it cumbersome (bulky).
2. The users may find that the end product is not visible for a long time.
3. The rigidity of the approach may prolong the duration of many projects.
4. It may not be suitable for small and medium sized projects.

Q.NO.19. WRITE IN BRIEF ABOUT PRELIMINARY INVESTIGATION? (B) (MTP N15 – 6M, N16)

1. Preliminary investigation is done to determine and analyze the strategic benefits in implementing the system.
2. A preliminary investigation is normally initiated by some sort of system request.
3. The main purpose of this phase is to validate the project request.
4. The steps involved in the preliminary investigation phase are as follows:
   - a) Identification of Problem
   - b) Identification of objective
   - c) Delineation/ Description of scope
   - d) Feasibility Study
5. It largely enables the requirement engineer to tackle the issues and Feasibility study for the following:
   - a) Determine whether the solution is as per business strategy
   - b) Determine whether the present system can rectify the situation without a major modification.
   - c) Define the time frame for which the solution is required.
   - d) Determine the approximate cost to develop the system.
   - e) Determine whether the vendor product offers a solution to the problem.
6. **Document / Deliverable:** A preliminary investigation report/ feasibility study for management.

Q.NO.20. WRITE SHORT NOTES ON IDENTIFICATION OF PROBLEM? (B)

1. The first step in an application development is to define the problem clearly and precisely which is done only after several rounds of discussions with the user group and then its frequency within the organization has to be assessed.
2. A problem that has a considerable impact on the organization is likely to receive immediate management attention.
3. User involvement will also be high, if they are convinced that the proposed solution will resolve the problem.
4. *For instance, personnel in a functional area may feel that an existing system is outdated or a manager might want access to specific new information that he claims will lead to better decisions.*
5. If the need seems genuine, a system analyst is assigned to make a preliminary investigation who submits all proposals to the steering committee for evaluation to identify those projects that are most beneficial to the organization.
6. The analyst working on the preliminary investigation should accomplish the following objectives:
   - a) Clarify and understand the project request;
   - b). Determine the size of the project;
   - c) Determine the technical and operational feasibility of alternative approaches;
   - d) Assess costs and benefits of alternative approaches; and
   - e) Report findings to the management with recommendation outlining the acceptance or rejection of the proposal.

Q.NO.21. WRITE ABOUT IDENTIFICATION OF OBJECTIVES? (B)

1. After the identification of the problem, it is easy to work out the objectives of the proposed solution.
2. For instance, inability to provide a convenient reservation system, for a large number of intending passengers was the problem of the Railways. So its objective was “to introduce a system wherein intending passengers could book a ticket from source to destination, faster than in real-time.”

Q.NO.22. EXPLAIN DELINEATION OF SCOPE OR DESCRIPTION? (OR)
EXPLAIN TWO PRIMARY METHODS, WHICH ARE USED FOR THE ANALYSIS OF THE SCOPE OF A PROJECT IN SDLC. (A) (PM)

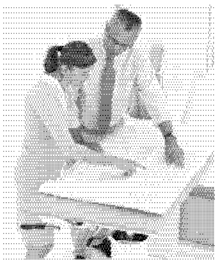
1. The scope of a solution defines its typical boundaries.
2. It should be clear and comprehensible to the user management stating the extent and ’what will be addressed by the solution and what will not’.
3. Outlining the scope in the beginning is essential and proves quite handy.
4. **Dimensions on which scope maybe performed:**
   a) **Functionality Requirements:** What functionalities will be delivered through the solution?
   b) **Data to be processed:** What data is required to achieve these functionalities?
   c) **Control Requirements:** What are the control requirements for this application?
   d) **Performance Requirements:** What level of response time, execution time and throughput is required?
   e) **Constraints:** What are the conditions the input data has to conform to?
   f) **Interfaces:** Is there any special hardware/software that the application has to interface with?
   g) **Reliability requirements:** Reliability of an application is measured by its ability to remain uncorrupted in the face of deliberate misuse and probability of failure-free operations.

[WHAT ARE THE MAJOR ASPECTS THAT NEED TO BE KEPT IN MIND WHILE ELICITING INFORMATION TO DELINEATE SCOPE?]

5. **Aspects to be kept in mind when determining scope:** While eliciting information to delineate the scope, few aspects needs to be kept in mind:
   a) Different users may represent the problem and required solution in different ways. *The system developer should elicit the need from the initiator of the project alternately called champion or executive sponsor of the project, addressing his concerns should be the basis of the scope.*
   b) While the initiator of the project may be a member of the senior management, the actual users may be from the operating levels in an organization. An understanding of their profile helps in designing appropriate user interface features.
   c) While presenting the proposed solution for a problem, the development organization has to clearly quantify the economic benefits to the user organization. The information required has to be gathered at this stage. *For example, when a system is proposed for Road tax collection, data on the extent of collection and defaults is required to quantify benefits that will result to the Transport Department.*
   d) It is also necessary to understand the impact of the solution on the organization- its structure, roles and responsibilities
   e) While economic benefit is a critical consideration when deciding on a solution, there are several other factors that have to be given weightage too. These factors are to be considered from the perspective of the user management and resolved. *For example, in a security system, how foolproof it is, may be a critical factor like the economic benefits that entail.*

[TWO PRIMARY METHODS, WHICH ARE USED FOR THE ANALYSIS OF THE SCOPE OF A PROJECT IN SDLC] (RTP N14,N15, MTP M16 – 6M, MTP N16 – 8M)

6. Two primary methods with the help of which the scope of the project can be analyzed are given as follows:



a) **Reviewing Internal Documents:**

i) The analysts conducting the investigation first try to learn about the organization involved in, or affected by, the project.

ii) For example, to review an inventory system proposal, an analyst may try to know how the inventory department does operate and who are the managers and supervisors.

iii) Analysts can usually learn these details by examining organization charts and studying written operating procedures.

b) **Conducting Interviews:**

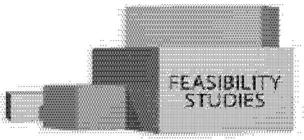
i) Written documents tell the analyst how the systems should operate, but they may not include enough details to allow a decision to be made about the merits of a systems proposal, nor do they present users' views about current operations.

ii) To learn these details, analysts use interviews.

iii) Interviews allow analysts to know more about the nature of the project request and the reasons for submitting it.

iv) Usually, preliminary investigation interviews involve only management and supervisory personnel.

Q.NO.23. WRITE SHORT NOTES ON FEASIBILITY STUDY (OR) FEASIBILITY STUDY IS AN IMPORTANT ASPECT OF SYSTEM DEVELOPMENT LIFE CYCLE (SDLC). EXPLAIN THE DIMENSIONS, WHICH ARE EVALUATED FOR THIS STUDY. (A) (PM, RTP M15, MTP M17- 4M, A16 - 4M, S16 - 4M)



1. A feasibility study is carried out by the system analysts, which refers to a process of evaluating alternative systems through cost/benefit analysis so that the most feasible and desirable system can be selected for development.

2. The Feasibility Study of a system is evaluated under following dimensions:

a) **Technical:** Is the technology needed available?

b) **Financial:** Is the solution viable financially?

c) **Economic:** Return on Investment?

d) **Schedule / Time:** Can the system be delivered on time?

e) **Resources:** Are human resources reluctant for the solution?

f) **Operational:** How will the solution work?

g) **Behavioral:** Is the solution going to bring any adverse effect on quality of work life?

h) **Legal:** Is the solution valid in legal terms?.

Q.NO.24. DESCRIBE THE VARIOUS TYPES OF FEASIBILITY STUDY THAT IS USED TO DEVELOP THE NEW SYSTEM? (RTP M15)

(OR)

THE TOP MANAGEMENT OF A COMPANY HAS DECIDED TO DEVELOP A COMPUTER INFORMATION SYSTEM FOR ITS OPERATION. IS IT ESSENTIAL TO CONDUCT THE FEASIBILITY STUDY OF SYSTEM BEFORE IMPLEMENTING IT? IF ANSWER IS YES, STATE THE REASONS. ALSO DISCUSS THE THREE DIFFERENT ANGLES THROUGH WHICH FEASIBILITY STUDY OF SYSTEM IS TO BE CONDUCTED? (PM, M– 09, MTP M16 – 4M)

(OR)

FEASIBILITY STUDY IS AN IMPORTANT ASPECT OF SYSTEM DEVELOPMENT LIFE CYCLE (SDLC). EXPLAIN THE DIMENSIONS, WHICH ARE EVALUATED FOR THIS STUDY. (A) (M16 – 4M, RTP N14)

1. After possible solution options are identified, project feasibility-the likelihood that these systems will be useful for the organization-is determined.
2. A feasibility study is carried out by the system analysts for this purpose.

Technical Feasibility

1. The analyst ascertains whether the proposed system is feasible with existing or expected computer hardware and software technology.
2. The technical issues usually raised during the feasibility stage of investigation include the following:
   a) Does the necessary technology exist to do what is suggested?
   b) Does the proposed equipment have the technical capacity to hold the data required to use the new system?
   c) Will the proposed system provide adequate responses to inquires, regardless of the number or location of users?
   d) Can the proposed application be implemented with existing technology?
   e) Can the system be expanded if developed?
   f) Are there technical guarantees of accuracy, reliability, ease of access, and data security?
   g) Some of the technical issues to be considered are given in the following Table

Design Considerations	Design Alternatives
Communications channel configuration	Point to point, multidrop, or line sharing
Communications channels	Telephone lines, coaxial cable, fiber optics, microwave, or satellite
Communications network	Centralized, decentralized, distributed, or local area
Computer programs	Independent vendor or in-house
Data storage medium	Tape, floppy disk, hard disk, or hard copy
Data storage structure	Files or database
File organization and access	Direct access or sequential files
Input medium	Keying, OCR, MICR, POS, EDI, or voice recognition
Operations	In-house or outsourcing
Output frequency	Instantaneous, hourly, daily, weekly, or monthly

Output medium	CRT, hard copy, voice, or turn-around document
Output scheduling	Pre-determined times or on demand
Printed output	Pre-printed forms or system-generated forms
Processor/Computer	Micro, mini, or mainframe
Transaction processing	Batch or online
Update frequency	Instantaneous, hourly, daily, weekly, or monthly

1. Financial Feasibility

a) The solution proposed may be prohibitively costly for the user organization.

b) For example, monitoring the stock through VSAT network connecting multiple locations may be acceptable for an organization with high turnover. But this may not be a viable solution for smaller ones.

2. Economic Feasibility

a) It includes an evaluation of all the incremental cost and benefits expected if the proposed system is implemented.

b) The analyst should make a primary estimate of each solution's costs and benefits.

c) The financial and economic questions raised by analysts during_the preliminary investigation are for the purpose of estimating the following:

i) The cost of conducting a full systems investigation;

ii) The cost of hardware and software for the class of applications being considered;

iii) The benefits in the form of reduced costs or fewer costly errors; and

iv) The cost if nothing changes (i.e. the proposed system is not developed).

d) After possible solution options are identified, an analyst should make a primary estimate_of each solution's costs and benefits.

3. Schedule or Time Feasibility **(RTP M15)**

a) Schedule feasibility involves the design teams estimating how long it will take a new or revised system to become operational and communicating this information to the steering committee.

b) For example, if a design team projects that it will take 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 company can implement in a shorter time frame.

4. Resources Feasibility

a) This focuses on human resources.

b) Implementing sophisticated software solutions becomes difficult in non-metro locations because of the reluctance of skilled personnel to move to such locations.

5. Operational Feasibility

a) It is concerned with ascertaining the views of workers, employees, customers and suppliers about the use of computer facility.

b) The support or lack of support that the firm's employees are likely to give to the system is a critical aspect of feasibility.

c) Some of the questions which help in testing the operational feasibility of a project are:

i) Is there sufficient support for the system from management? From users?

ii) Are current business methods acceptable to users?

iii) Have the users been involved in planning and development of the project?

iv) Will the proposed system cause harm, such as producing poorer results in any respect or area, loss of control, loss of accessibility of information, make the individual performance poorer than before, or make the performance slow in any areas?

6. **Behavioral Feasibility:** It refers to the systems, which is to be designed to process data and produce the desired outputs. However, if the data input for the system is not readily available or collectable, then the system may not be successful. **(RTP M17)**

7. **Legal Feasibility** **(RTP M17)**

a) Legal feasibility is largely concerned with whether there will be any conflict between a newly proposed system and the organization's legal obligations.

b) For example, a revised system should comply with all applicable federal (i.e. central) and state statutes about financial reporting requirements, as well as the company's contractual obligations.

8. **Reporting Results to Management:** After the analyst articulates the problem, defines the same along with its scope, s/he provides one or more solution alternatives and estimates the cost and benefits of each alternative and reports these results to the management.

9. **Internal Control Aspects:** Management implements proper internal control to ensure business objectives. As defined in section 217(2AA), Companies Act, 1956, Directors are responsible to have proper internal control for a company. In terms of system development, controls need to be well in place during the development of system. In systems, it is not possible to put in place controls post development. A better understanding of controls during planning and effective implementation of those controls shall help to achieve the above stated objectives.

For validating control aspects in system, entity may have an internal audit team. Few large software developers engage outside experts for the same. To check controls internally or through external auditor depends on size and nature of entities of the business. The same is also dependent upon management's attitude. Review by external consultant is more independent. External consultant may bring his/her expertise to entity. The flip side is that external consultant may be costly; secrecy is also a fact to consider. However, the key control queries regarding various aspects at this stage may include the following:

- Whether problem definition is proper?
- Whether all feasibility studies have been properly done?
- Whether results of feasibility studies have been documented?
- Whether management report submitted reflects the outcome of feasibility studies done?

Q.NO.25. WHAT IS REQUIREMENTS ANALYSIS OR SYSTEMS ANALYSIS? (OR)
WHAT DO YOU MEAN BY SYSTEM REQUIREMENTS ANALYSIS? WHAT ARE THE ACTIVATES TO BE PERFORMED DURING THE SYSTEM ANALYSIS PHASE? (OR)
WHAT ARE THE MAJOR OBJECTIVES OF SYSTEM REQUIREMENTS ANALYSIS PHASE IN THE SDLC? (A) (PM, M11, N11, M13 - 5M, M14 – 5M, MTP M16, RTP M14, N14)

1. This phase includes a thorough and detailed understanding of the current system, identifies the areas that need modification to solve the problem, the determination of user/managerial requirements and to have fair idea about various systems development tools.

2. The following objectives are performed in this phase in order to generate the deliverable, Systems Requirements Specification (SRS):

a) To identify and consult the stake owners to determine their expectations and resolve their conflicts.

b) To analyze requirements to detect and correct conflicts and determine priorities.

c) To verify the requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable.

- **d)** To gather data or find facts using tools like - interviewing, research/document collection, questionnaires, observation.
- **e)** To model activities such as developing models to document Data Flow Diagrams, E-R Diagrams.
- **f)** To document activities such as interview, questionnaires, reports etc. and development of a system (data) dictionary to document the modeling activities.

3. **Document/Deliverable:** A systems requirements report.

Q.NO.26. WHAT ARE THE KEY INTERNAL CONTROLS TO BE VERIFIED IN REQUIREMENT ANALYSIS PHASE OF SDLC? (C)

Requirements phase is the most important phases of SDLC. The issue of controls is very important here also. Some of the key control aspects at this stage may be taken care by the following queries:

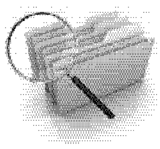
- **i)** Whether present system analysis has been properly done?
- **ii)** Whether appropriate domain, were expert was engaged?
- **iii)** Whether all user requirements of proposed system have been considered?
- **iv)** Whether SRS document has been properly made and vetted by Users, Domain Experts, System Analysts?

Q.NO.27. WHAT ARE THE FACT FINDING TECHNIQUES USED BY A SYSTEM ANALYST? (OR) EXPLAIN VARIOUS FACT FINDING TECHNIQUES USED BY THE SYSTEM ANALYST FOR DETERMINING THE USERS REQUIREMENTS NEEDS OF ORGANIZATION? (A)
(N05, 07, RTP M14, M15)

1. Every system is built to meet some set of needs, for example, the need of the organization for lower operational costs, better information for managers, smooth operations for users or better levels of service to customers.
2. To assess these needs, the analysts often interact extensively with people, who will be benefited from the system in order to determine 'what are their actual requirements'.
3. Various fact-finding techniques, which are used by the system analyst for determining these needs/ requirements, are:

a) Documents:

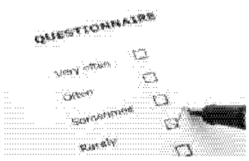
- **i)** Document means manuals, input forms, output forms, diagrams of how the current system works, organization charts showing hierarchy of users and manager responsibilities, job descriptions for the people who work with the current system, procedure manuals, program codes for the applications associated with the current system, etc.



- **ii)** Documents are a very good source of information about user needs and the current system.

b) Questionnaires:

- **i)** Users and managers are asked to complete questionnaire about the information system when the traditional system development approach is chosen.
- **ii)** The main strength of questionnaires is that a large amount of data can be collected through a variety of users quickly.
- **iii)** if the questionnaire is skillfully drafted, responses can be analyzed rapidly with the help of a computer.



c) **Interviews:**

i) Users and managers may also be interviewed to extract information in depth. The data gathered through interviews often provide systems developer with a complete picture of the problems and opportunities.

ii) Interviews also give analyst the opportunity to note user reaction first-hand and to probe for further information.

d) **Observation:**

i) The analyst should visit the user site to watch how the work was taking place. The value of observational visits by analyst can be great.

ii) It helps the analyst in getting a clear picture of the user's environment and to determine why a request for a new system was submitted.

Q.NO.28. DISCUSS IN DETAIL HOW THE ANALYSIS OF THE PRESENT SYSTEM IS MADE BY THE SYSTEM ANALYST? (OR) DISCUSS IN DETAIL, HOW THE INVESTIGATION OF PRESENT SYSTEM IS CONDUCTED BY THE SYSTEM ANALYST?

(OR)

DESCRIBE ANY FIVE FUNCTIONAL AREAS OF A SYSTEM WHICH NEEDS TO BE ANALYZED BY SYSTEM ANALYST FOR DETAILED INVESTIGATION OF THE PRESENT SYSTEM?

(OR)

A COMPANY IS OFFERING A WIDE RANGE OF PRODUCTS AND SERVICES TO ITS CUSTOMERS. IT RELIES HEAVILY ON ITS EXISTING INFORMATION SYSTEM TO PROVIDE UP TO DATE INFORMATION THE COMPANY WISHES TO ENHANCE ITS EXISTING SYSTEM. YOU BEING AN INFORMATION SYSTEM AUDITOR SUGGEST HOW THE INVESTIGATION OF THE PRESENT INFORMATION SYSTEM SHOULD BE CONDUCTED SO THAT IT CAN BE FURTHER IMPROVED UPON. (A) (PM, M – 99, 05, 06, 08, M11- 8M)

1. Detailed investigation of the present system involves collecting, organizing and evaluating facts about the system and the environment in which it operates.
2. Survey of existing methods, procedures, data flow, outputs, files, input and internal controls should he intensive in order to fully understand the present system and its related problems.
3. The following areas should be studied in depth:
4. **Review historical aspects:**
   a) A brief history of the organization is a logical starting point for an analysis of the present system.
   b) The historical facts should identify the major turning points and milestones that have influenced its growth.
   c) A review of annual reports and organization chart can identify the growth as well as the development of various management levels, functional areas and departments.
   d) The system analyst should investigate what system changes have occurred in the past that have been successful or unsuccessful.
5. **Analyze inputs:**
   a) A detailed analysis of present inputs is important since they are basic to the manipulation of data.
   b) Source documents are used to capture the originating data for any type of system.
   c) The system analyst should be aware of the various sources from where the data are initially captured, keeping in view the fact that outputs for one area may serve as an input for another area.
   d) The system analyst must understand the nature of each form, what is contained in it, who prepared it, from where the form is initiated, where it is completed, the distribution of the form and other similar considerations

6. **Review data files maintained:**

   a) The analyst should investigate the data files maintained by each department, where they are located, who uses them and the number of times per given time interval these files are used or accessed.

   b) Information on common data files and their size will be an important factor, which will influence the new information system.

   c) The system analyst should also review all on-line and off-line files which are maintained in the organization.

7. **Review methods, procedures and data communications:**

   a) Methods and procedures transform input data into useful output.

   b) A method is defined as a way of doing something; a procedure is a series of logical steps by which a job is accomplished.

   c) A procedure review is an intensive survey of the methods by which each job is accomplished, the equipment utilized and the actual location of the operations. Its basic objective is to eliminate unnecessary tasks or to locate improvement opportunities in the present information system.

   d) A system analyst also needs to review and understand the present data communications used by the organization.

   e) He must review the types of data communication equipments including data interface, data links, modems, dial-up and leased lines and multiplexers.

   f) The system analyst must understand how the data communications network is used in the present system so as to identify the need to revamp the network when the new system is installed.

8. **Analyze outputs:**

   a) The outputs or reports should be scrutinized carefully by the system analysts in order to determine how well they will meet the organization's needs.

   b) The analysts must understand what information is needed and why, who needs it and when and where it is needed.

   c) *Additional questions concerning the sequence of the data, how often the form reporting it is used, how long it is kept on file, etc. must be investigated.*

9. **Review internal controls:**

   a) Locating the control points helps the analyst to visualize the essential parts and framework of a system.

   b) An examination of the present system of internal controls may indicate weaknesses that should be removed in the new system. A detailed investigation of the present information system is not complete until internal control mechanism is reviewed.

   c) The adoption of advanced methods, procedures and equipments might allow much greater control over the data.

10. **Model the existing physical system and logical system:**

    a) The logic of inputs, methods, procedures, data files, data communications, reports, internal controls and other important items is reviewed and analyzed.

    b) The process must be properly documented in the form of flow charts and diagrams.

    c) The logical flow of the present information system may be depicted with the help of system flow charts.

    d) The physical flow of the existing system may be shown by employing data flow diagrams and flowcharting

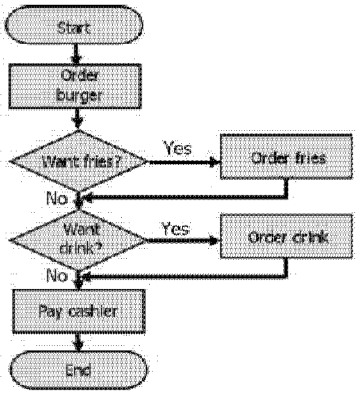
11. **Undertake overall analysis of present system:** Based upon the aforesaid investigation of the present information system, the final phase of the detailed investigation includes the analysis of the present work volume, the current personnel requirements and the present benefits and costs and each of these must be investigated thoroughly.

Q.NO.29. HOW IS A SYSTEM ANALYSIS OF PROPOSED SYSTEMS CARRIED OUT? (A)

1. After each functional area of the present information system has been carefully analyzed, the proposed system specifications must be clearly defined.
2. While defining such specifications consideration should be given to the strengths and short comings of the present system.
3. The required systems specifications which should be in conformity with the project's objectives are as follows:
   - **a)** Emphasis on timely managerial reports.
   - **b)** Database maintained with great focus on online processing capabilities.
   - **c)** Input data prepared directly from original source documents for processing by the computer system.
   - **d)** Methods and procedures that show the relationship of inputs and outputs to the database, utilizing data communications where deemed appropriate.
   - **e)** Work volumes and timings carefully considered for present and future periods including peak periods.

Q.NO.30. DESCRIBE THE CATEGORIES OF MAJOR TOOLS THAT ARE USED IN SYSTEM DEVELOPMENT? (PM) (OR) STATE THE MAIN OBJECTIVES OF SYSTEM DEVELOPMENT TOOLS? BRIEFLY DESCRIBE THE MAJOR CATEGORIES OF DOCUMENTATION TOOLS THAT ARE USED FOR SYSTEM DEVELOPMENT WITH ANY ONE OF THE SIMPLE ILLUSTRATIVE EXAMPLE FOR EACH? (B) (M – 03, N – 08)

1. Many tools and techniques have been developed to improve current information systems and to develop new ones.
2. Such tools help end users and systems analysts to –
   - **a)** Conceptualize, clarify, document and communicate the activities and resources.
   - **b)** Analyze present business operations, management decision making and information processing activities.
   - **c)** Propose and design new or improved information systems to solve business problems.
3. Many systems development tools take the form of diagrams and other graphic representations.
4. The major tools used for system development can be grouped into four categories based on broader features. They are:
   - **a) System components and flows:**
     - **i)** These tools help the system analysts to document the data flow among the major resources and activities of an information system.
     - **ii)** System flow charts are typically used to show the flow of data media as they are processed by the hardware devices and manual activities.
     - **iii)** A data flow diagram uses a few simple symbols to illustrate the flow of data among external entities (such as people or organizations, etc.), processing activities and data storage elements.



iv) A system component matrix provides a matrix framework to document the resources used, the activities performed and the information produced by an information system.

b) **User interface:**

i) Designing the interface between end users and the computer system is a major consideration of a system analyst while designing the new system.

ii) Layout forms and screens are used to construct the formats and contents of input/output media and methods.

iii) Dialogue flow diagrams analyze the flow of dialogue between computers and people.

c) **Data attributes and relationships:** The data resources in information system are defined, catalogued and designed by this category of tools.

i) Data Dictionary is centralized repository of information about data such as meaning, relationships to other data, origin, usage, and format.

ii) Entity-relationship diagrams are used to document the number and type of relationship among the entities in a system.

iii) File layout forms document the type, size and names of the data elements in a system.

iv) Grid charts help in identifying the use of each type of data element in input/output or storage media of a system.

d) **Detailed system process:**

i) These tools are used to help the programmer develop detailed procedures and processes required in the design of a computer program.

ii) Decision trees and decision tables use a network or tabular form to document the complex conditional logic involved in choosing among the information processing alternatives in a system.

iii) Structure charts document the purpose, structure and hierarchical relationships of the modules in a program.

SOME OTHER IMPORTANT SYSTEM DEVELOPMENT TOOLS: **(RTP M16)**

a) **Structured English or pseudo code: (RTP N15)**

i) Structured English, also known as Program Design Language (PDL) or Pseudo Code, is the use of the English language with the syntax of structured programming.

ii) Structured English aims at getting the benefits of both the programming logic and natural language.

iii) Program logic that helps to attain precision and natural language that helps in getting the convenience of spoken languages.

b) **Flowcharts: (RTP N15)**

i) Flowcharting is a graphic technique that can be used by analysts to represent the inputs, outputs and processes of a business in a pictorial form.

ii) It is a common type of chart that represents an algorithm or process showing the steps as boxes of various kinds, and their o rder by connecting these with arrows.

iii) Flowcharts are used in analyzing, designing, documenting or managing a process or program in various fields.

iv) A typical flowchart may have various kinds of symbols.

c) Data Flow Diagram (DFD): (RTP N15)

i) A Data Flow Diagram uses few simple symbols to illustrate the flow of data among external entities, processing activities and data storage elements.

ii) A DFD is composed of four basic elements:

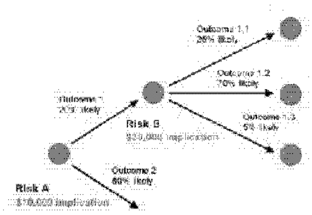
- Data Sources and Destinations
- Data Flows
- Transformation processes
- Data stores

Symbol	Name	Explanation
□	Data Source and destinations	The people and organizations that send data to and receive data from the system are represented by square boxes called Data destinations or Data Sinks.
↗	Data flows	The flow of data into or out of a process is represented by curved or straight lines with arrows.
○	Transformation	The processes that transform data from inputs to outputs are represented by circles, often referred to as bubbles.
═	Data stores	The storage of data is represented by two horizontal lines.

d) Decision Trees:

i) A Decision Tree or tree diagram is a support tool that uses a tree-like graph or model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility.

ii) Decision tree is commonly used in operations research, specifically in decision analysis to help identify a strategy most likely to reach a goal and to calculate conditional probabilities.



e) Decision Table:

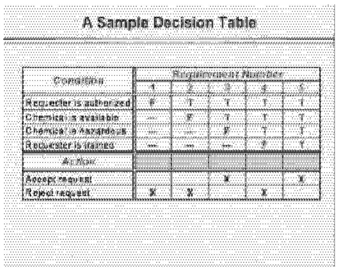
i) A Decision Table is a table which may accompany a flowchart, defining the possible contingencies that may be considered within the program and the appropriate course of action for each contingency.

ii) Decision table is tabular representation of rows and columns which represents set of conditions and its corresponding actions.

iii) Decision tables are necessitated by the fact that branches of the flowchart multiply at each diamond (comparison symbol) and may easily run into scores and even hundreds.

iv) The four parts of the decision table are :

- **Condition Stub:** Which comprehensively lists the comparisons or conditions;
- **Action Stub:** Which comprehensively lists the actions to be taken along the various program branches
- **Condition entries:** Which list in its various columns the possible permutations of answer to the questions in the conditions stub)
- **Action entries:** Which lists, in its columns corresponding to the condition entries the actions contingent upon the set of answers to questions of that column.



A Sample Decision Table

Condition	Requirement Number				
	1	2	3	4	5
Requester is authorized	F	T	T	T	T
Chemical is available	—	F	T	T	T
Chemical is hazardous	—	—	F	T	T
Requester is trained	—	—	—	F	T
Action					
Accept request			X		X
Reject request	X	X		X	

f) CASE TOOLS (M – 01)

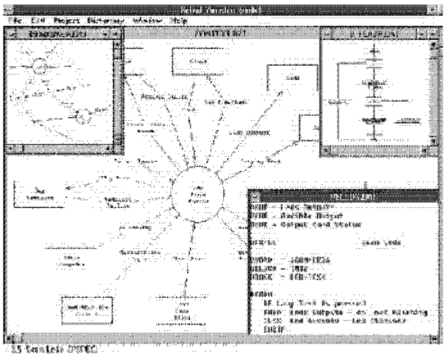
i) CASE tool refers to that software which helps to automatically develop high quality, defect free and maintainable software.

ii) CASE refers to the automation of anything that humans do to develop systems and support virtually all phases of system development process.

iii) CASE tools automate methods for designing, documenting, and producing structured computer code in the desired programming language.

iv) *For example, these packages can be used to create complete and internally consistent requirements specifications with graphic generators and specifications languages.*

v) Some of the features that various CASE products possess are - Data Dictionary tools; Computer aided Diagramming Tools; Screen and Report generator; Prototyping tools; Code Generation; and Reverse Engineering.

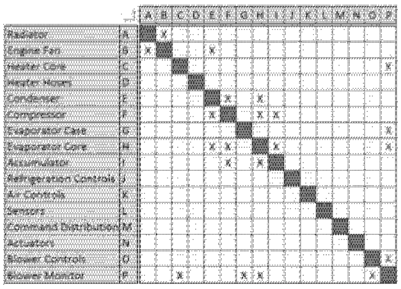


g) System component matrix:

i) A System Component Matrix provides a matrix framework to document the resources used, the activities performed and the information produced by an information system.

ii) It can be used as an information system framework for both systems analysis and system design and views the information system as a matrix of components that highlights how the basic activities of input, processing, output, storage and controls are accomplished in an information system.

iii) How the use of hardware, software and people resources can convert data resources into information products.



		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Radiator	A	▨	X														
Engine Fan	B	X	▨			X											
Heater Core	C			▨													X
Heater Hoses	D				▨												
Condenser	E					▨	X		X								
Compressor	F					X	▨		X	X							
Evaporator Case	G							▨									X
Evaporator Core	H					X	X		▨	X							X
Accumulator	I						X		X	▨							
Refrigeration Controls	J										▨						
Air Controls	K											▨					
Sensors	L												▨				
Command Distribution	M													▨			
Actuators	N														▨		
Blower Controls	O															▨	X
Blower Monitor	P			X				X	X							X	▨

h) User interface layout and forms:

i) Layout form/ Screen Generator: They are used to format or "paint" the desired layouts and contact without having to enter complex formatting information.

ii) Menu Generator: Menu generator outlines the functions which the system is aimed to accomplish. Menu may be linked to other submenus that will enable the user to understand how the screens and sub-screens will be used for data entry or inquiry.

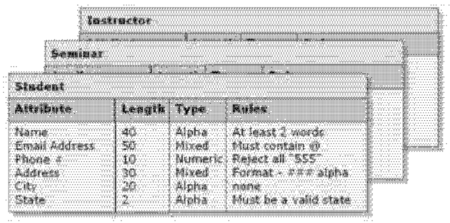
iii) Report Generator: Report generator has capacity of performing similar functions as found in screen generators. It can also indicate totals, paging, sequencing and control breaks in creating samples of the desired report.

iv) Code Generator: Code generator allows the analyst to generate modular units of source code from the high level specifications provided by the system analyst and play significant role in systems development process.

i) DATA DICTIONARY (Covered in Q.No: 30)

Q.NO.31. WRITE SHORT NOTES ON DATA DICTIONARY? (OR)
HOW WOULD YOU USE DATA DICTIONARY AS TOOL FOR A FILE SECURITY AND AUDIT TRAILS? (A) (N – 02, M 5, M7 – 5M, M12 – 4M)

1. A Data Dictionary is a centralized repository of information about data such as meaning, relationships to other data, origin, usage, and format.
2. A data dictionary is a computer file that contains descriptive information about the data items in the files of a business information system.
3. A data dictionary is a computer file about data.



Instructor
Seminar

Student

Attribute	Length	Type	Rules
Name	40	Alpha	At least 2 words
Email Address	50	Mixed	Must contain @
Phone #	10	Numeric	Reject all "555"
Address	30	Mixed	Format - ### alpha
City	20	Alpha	none
State	2	Alpha	Must be a valid state

4. This information include

a) The identity of the source documents used to create the data item

b) The names of the computer files that store the data item

c) The names of the computer programs that modify the data item

d) The identity of the computer programs or individuals permitted to access the data item for the purpose of file maintenance, upkeep, or inquiry

e) The identity of the computer programs or individuals not permitted to access the data item etc.

Q.NO.32. EXPLAIN THE SYSTEMS SPECIFICATION IN DETAIL OR SYSTEM REQUIREMENT SPECIFIFCATION (SRS). (B) (RTP M17)

1. At the end of the analysis phase, the systems analyst prepares a document called "Systems Requirement Specifications (SRS)", and submits the same to the management.

2. A well documented SRS may normally contains the following sections:

a) Introduction: Goals and Objectives of the software in the context of the computer-based Information system.

b) Information Description: Problem description; Information content, flow and structure; Hardware, software, User interfaces for external system elements and internal software functions.

c) Functional Description: Diagrammatic representation of functions; processing narrative for each function; Interplay among functions; Design constraints. The complete description of the functions to be performed by the software specified in the SRS will assist the potential users to determine if the software specified meets their needs or how the software must be modified to meet their needs.

d) Behavioral Description : Response to external events and internal controls

e) Validation Criteria: Organizations can develop their validation and Verification plans much more productively from a good SRS. Classes of tests to be performed to validate functions, performance and constraints.

f) Appendices: Data flow / Object Diagrams; Tabular Data; Detailed description of algorithms , flowcharts, graphs and other such material.

g) SRS Review: The development team makes a presentation and then hands over the SRS document to be reviewed by the user or customer.

Q.NO.33. WHAT ARE THE VARIOUS ROLES IN SDLC? (B) (RTP M14)

1. A variety of tasks during the SDLC are performed by special teams/committees/individuals based on requisite expertise as well as skills.

2. Some of the generic roles or functions includes:

3. Steering Committee **(RTP N15, M14, MTP M16 – 3M)**

a) To provide overall direction

b) To ensure appropriate representation of all users or department.

c) To monitor cost and schedule

d) To conduct meetings to track the progress of the project

e) To take corrective actions like rescheduling, re-staffing etc

4. Project Manager: **(N11 -2M, MTP M16 – 3M)**

- **a)** A project manager is responsible for the overall coordination and direction.
- **b)** He can have several projects under him at any point of time.
- **c)** He has to liaison with the client and coordinates with his team and project leader.
- **d)** He has to deliver the project within the time and budget allocated to him.

5. Project Leader: **(RTP M14, N16)**

- **a)** The project leader is dedicated to a project, who has to ensure its completion and fulfillment of objectives.
- **b)** He reviews the project position more frequently than a Project Manager and the entire project team reports to him.

6. Systems Analyst / Business Analyst: **(N11, N16- 2M)**

- **a)** The systems analysts' main responsibility is to conduct interviews with users and understand their requirements.
- **b)** He is a link between the users and the programmers who converts the user's requirements in the system requirements and plays a vital role in the Requirements analysis and Design phase.

7. Module Leader / Team Leader:

- **a)** A project is divided into several manageable modules, and the development responsibility for each module is assigned to Module Leaders.
- **b)** For example, while developing a financial accounting application – Treasury, Accounts payable, Accounts receivable can be identified as separate modules and can be assigned to different module leaders.
- **c)** Module leaders are responsible for the delivery of tested modules within the stipulated time and cost.

8. Programmer / Coder / Developer: **(N16)**

- **a)** A programmer is a main person of the software industry who converts design into programs by coding using programming language.
- **b)** Apart from developing the application in a programming language, he also tested the program for debugging activity.

9. Database Administrator (DBA): **(N11, RTP M14, N16)**

- **a)** The data in a database environment has to be maintained by a specialist in database administration so as to support the application program.
- **b)** The DBA handles multiple projects; ensures the integrity and security of information stored in the database and also helps the application development team in database performance issues.
- **c)** Inclusion of new data elements has to be done only with the approval of the database administrator.

10. Quality Assurance: **(N16)**

- **a)** This team sets the standards for development, and checks compliance with these standards by project teams on a periodic basis.
- **b)** Any quality assurance person who has participated in the development process shall not be viewed as "independent" to carry out quality audits.

11. Tester:

Tester is a junior level quality assurance personnel attached to a project that tests programs and subprograms as per the plan given by the module / project leaders and prepare test reports.

12. Domain Specialist: **(N16)**

a) Whenever a project team has to develop an application in a field that's new to them, they take the help of a domain specialist.

b) For example, if a team undertakes application development in Insurance, about which they have little knowledge, they may seek the assistance of an Insurance expert at different stages. This makes it easier to anticipate or interpret user needs.

c) A domain specialist need not have knowledge of software systems.

13. IS Auditor: **(N11, RTP M14, N16)**

a) As a member of the team, IS Auditor ensures that the application development also focuses on the control perspective.

b) He should be involved at the Design Phase and the final Testing Phase to ensure the existence and the operations of the Controls in the new software.

Q.NO.34. WHAT IS SYSTEMS DESIGN? WHAT ARE THE ACTIVITIES IN SYSTEM DESIGN? (A)

1. Systems design activity takes place for the alternative which is selected by management.

2. Designing an Information System is to optimally satisfies the user / managerial requirements.

3. It describes the parts of the system and their interactions, sets out how the system shall be implemented using the chosen hardware, software and network facilities, specifies the program, databases, the security plan and specify the change control mechanism.

4. Key design phase activities include

a) Describing inputs and outputs, such as screen design and reports

b) Determining the processing steps and computation rules for the new solution;

c) Determining data file or database system file design

d) Preparing the program specifications for the various types of requirements or information criteria defined

e) Internal / external controls.

5. Document / Deliverable :

a) Creates a 'blueprint' for the design with the necessary specifications for the hardware, software, people and data resources.

b) Once the detailed design is completed, the design is then distributed to the system developers for coding.

6. The design phase involves following steps :

a) Architectural design:

i) Architectural design deals with the organization of applications in terms of hierarchy of modules and sub -modules.

ii) At this stage, we identify

- Major modules
- Function and scope of each module
- Interface features of each module
- Modules that each module can call directly or indirectly
- Data received from / sent to / modified in other modules.

iii) The architectural design is made with the help of a tool called Functional Decomposition, which can be used to represent hierarchies. It has three elements – Module, Connection, and Couple.

b) Design of Data / Information flow:

i) The design of the data and information flows is a major step in the conceptual design of the new system.

ii) In designing the data / information flow for the proposed system, the inputs that are required are –

- Existing data / information flows
- Problems with the present system
- Objective of the new system.

iii) All these have been identified in the analysis phase and documented in Software Requirements Specification (SRS).

c) Design of database: [Refer Question 36]

d) Design of User Interface: [Refer Point no.6 in Question 36]

Q.NO.35. WRITE SHORT NOTE ON DESIGN OF DATABASE. (OR) WHAT ARE THE MAJOR ACTIVITIES INVOLVED IN DESIGNING OF THE DATABASE ? (A) (N 14 – 4 M, M12 – 4M)

1. **Design of database:**

   i) Design of the database involves determining its scope ranging from local to global structure.

   ii) The scope is decided on the basis of interdependence among organizational units.

   iii) The greater the need the interdependence, the greater the need for a global database to prevent sub-optimization by subunits.

   iv) The design of the database involves the following activities:

2. **Conceptual modeling:** These describe the application domain via entities/objects, attributes of these entities/objects and static and dynamic constraints and relationships.
3. **Data Modeling:** Conceptual Models need to be translated into data models so that they can be accessed and manipulated by high-level and low- level programming languages.
4. **Storage structure Design:** Decision must be made on how to linearize and partition the data structure so that it can be stored on some device.
5. **Physical Layout Design:** Decisions must be made on how to distribute the storage structure across specific storage media and locations – for example, the cylinders, tacks, and sectors on a disk and the computers in a LAN or WAN.
6. **Design of User Interface:**

   i) Design of user – interface involves determining the ways in which users will interact with a system.

   ii) The points that need to be considered while designing the user interface are

   - Source documents to capture raw data
   - Hard-copy output reports;
   - Screen layouts for dedicated source-document input;
   - Inquiry screens for database interrogation
   - Graphic or color displays
   - Requirements for special input/output device.

Q.NO.36. WHAT ARE KEY INTERNAL CONTROLS TO BE VERIFIED DURING SYSTEM DESIGN PHASE OF SDLC ? (C)

The key control aspects at this stage include the following:

i) Whether management reports of stage I and stage II, were referred by System Designer?

ii) Whether all control aspects have been properly covered?

iii) Whether controls put in place in system, appear in the documentation done at this stage?

iv) Whether a separate review of design document has been done by internal auditor?

Q.NO.37. WHAT ARE THE MAJOR FACTORS TO BE CONSIDERED IN DESIGNING USER INPUTS? (OR) YOU HAVE BEEN ASSOCAITED WITH A SYSTEM ANALYSIS TEAM. DESCRIBE THE IMPORTANT FACTORS THAT YOU WILL CONSIDER WHILE DESIGNING USER INPUT FORMS. (A) (N15-6M, N 02, M 06, 08, RTP N15, M17)

Characteristic	Definition	Input Design
Content	Refers to the actual pieces of data to be used as Input	The analyst is required to consider the types of data that are needed to be gathered to generate the desired user outputs.
Timeliness	Timeliness refers to the time or periodicity of data input	A plan must be established regarding when different types of inputs will enter system.
Format	Input format refers to the manner in which data are physically arranged.	After the data contents and media requirements are determined, input formats are designed on the basis of few constraints like - the type and length of each data field as well as any other special characteristics (number decimal places etc.).
Media	Input medium refers to the physical device used for input or storage.	Various user input alternatives may include key-boards, optical character recognition, pen – based computers and voice input etc. A suitable medium may be selected depending on the application to be computerized.
Input Volume	Input volume refers to the amount of data that has to be entered in computer system at any one time	In some decision-support systems and many real- time processing systems, input volume is light. In batch-oriented transaction processing systems, input volume could be heavy which involves thousands of records.
Form	Form refers to the way the information is inputted in the input form and the content is presented to users in various output forms - quantitative, non-quantitative, text, graphics, video and audio	Forms are preprinted papers that require people to fill in responses in a standardized way. Forms elicit and capture information required by organizational members that often will be input to the computer. Through this process, forms often serve as source documents for the data entry personnel.

Q.NO.38. WHAT ARE THE SIX IMPORTANT FACTORS WHICH SHOULD BE CONSIDERED WHILE DESIGNING THE USER OUTPUT? (OR)
WHAT ARE THE IMPORTANT FACTORS WHICH SHOULD BE CONSIDERED BY THE SYSTEMS ANALYST WHICH DESIGNING USER OUTPUT? (B) (M – 01, 04, N – 09, RTP M17)

Characteristic	Definition	Output Design
Content	Refers to the actual pieces of data to be used as Output	System analyst has to decide on the contents of the Output of the system. For instance, the contents of a weekly output report to a sales manager might consist of sales person's name, sales calls made by each sales person during the week, and the amount of each product sold.
Timeliness	Timeliness refers to the time or periodicity of data output.	It should be analyzed when users need outputs i.e. on a daily, weekly, monthly basis etc.
Format	Output format refers to the arrangement referring to data output on a printed report or in a display screen.	Format of information reports for the users should be devised so that it assists in decision-making, identifying and solving problems, planning and initiating corrective action and searching.
Media	Output medium refers to the physical device used for storage or output	A variety of output media are available in the market these days which include paper, video display, microfilm, magnetic tape/disk and voice output.
Output Volume	The amount of data output required at any one time is known as output volume.	It is better to use high- speed printers etc.
Form	Form refers to the way the information is inputted in the input form and the content is presented to users in various output forms - quantitative, non quantitative, text, graphics, video and audio.	The form of the output should be decided keeping in view the requirements for the concerned user. For example - Information on distribution channels may be more understandable to the concerned manager if it is presented in the form of a map, with dots representing individual outlets for stores

Q.NO.39. LIST THE OBJECTIVES IN DESIGNING SYSTEMS INPUTS AND SYSTEMS OUTPUT? (B)

1. One of the most important features of an information system for users is the output it generates.
2. Designing computer output must be in an organized, well define and consistent manner.

INPUT OBJECTIVES:

a) Developing specifications and procedures for data preparation

b) Developing steps which are necessary to put transactions data into a usable form for processing.

c) Data-entry, i.e., the activity of putting the data into the computer for processing.

OUTPUT OBJECTIVES:

a) Convey information about past activities, current status or projections of the future.

b) Signal important events, opportunities, problems or warnings.

c) Trigger an action.

d) Confirmation of an action.

Q.NO.40. WRITE SHORT NOTES ON PHYSICAL DESIGN. (C)

1. For the physical design, the logical design is transformed into units, which in turn can be decomposed further into implementation units such as modules and programs.
2. During physical design, the primary concern of the auditor is effectiveness and efficiency issues.
3. The auditor should seek evidence that designers follow some type of structured approach like – CASE tools to access their relative performance via simulations when they undertake physical design.
4. **Some of the issues addressed are:**

   a) Type of hardware for client application and server application

   b) Operating systems to be used

   c) Type of networking;

   d) Processing– batch – online, real – time

   e) Frequency of input, output

   f) Month-end cycles / periodical processing.

5. **Design Principles:** Some of the generic design principles being applied to develop the design of typical information systems include the following:

   a) Design two or three alternatives and choose the best one on pre-specified criteria.

   b) The design should be based on the analysis.

   c) The software functions designed should be directly relevant to business activities.

   d) The design should follow standards laid down.

   e) The design should be modular.

6. **Modularity:**

   a) A module is a manageable unit containing data and instructions to perform a well-defined task.

   b) Interaction among modules is based on well-defined interfaces.

   c) Modularity is measured by two parameters: Cohesion and Coupling.

   d) Cohesion refers to the manner in which elements within a module are linked.

   e) Coupling is a measure of the interconnection between modules.

   f) It refers to the number and complexity of connections between 'calling' and 'called' modules.

   g) In a good modular design, cohesion will be high and coupling low.

Q.NO.41. EXPLAIN THE PROCESS OF DESIGN OF THE HARDWARE / SYSTEM SOFTWARE PLATFORM? (OR) WRITE SHORT NOTES ON SYSTEM'S OPERATING PLATFORM? (B)

1. The new system requires hardware and system software not currently available in an organization.
2. For example – a DSS might require high-quality graphics output not supported by the existing hardware and software.
3. The new hardware/system software platform required to support the application system have to be designed.
4. If different hardware and software are not able to communicate with each, subsequent changes will have to be made and resources expanded in trying to make the hardware and software compatible to each other.
5. Auditors should be concerned about the extent to which modularity and generality are preserved in the design of the hardware/system software platform.

Q.NO.42. WHAT IS SYSTEM ACQUISITION? EXPLAIN PRINCIPLES OR STANDARD RELATED TO SYSTEM ACQUISITION? (B)

1. After a system is designed either partially or fully, the next phase of the systems development starts which relates to the acquisition of hardware, software and services.
2. Management should establish acquisition standards that address the same security and reliability issues as development standards.
3. Acquisition standards should focus on -
   a) Ensuring security, reliability, and functionality already built into a product.
   b) Ensuring managers complete appropriate vendor, contract, and licensing reviews and acquiring products compatible with existing systems.
   c) Including invitations-to-tender and request-for-proposals.
   d) Ensuring functional, security, and operational requirements to be accurately identified and clearly detailed in request-for- proposals.

Q.NO.43. WRITE ABOUT ACQUIRING SYSTEMS COMPONENTS FROM VENDORS? (A)

1. At the end of the design phase, the organization gets a reasonable idea of the types of hardware, software and services; it needs for the system being developed.
2. Acquiring the appropriate hardware and software is critical for the success of the whole project.
3. The organization can discover new hardware and software developments in various ways.
4. Management also decides whether the hardware is to be purchased, leased from a third party or to be rented.
5. A sub-committee steering committee, referred to as 'System Acquisition Committee' is constituted.
6. The sub-committee is mandated to ensure timely and effective completion of this stage.
7. The next aspect is call for Request For Proposal (RFP) from vendors.
8. This stage is one of the most critical phases for system acquisition; as well defined RFP leads to better acquisition.
9. RFP, means asking vendors to submit proposals for the requirements mentioned.
10. RFP process is the initiation of final stages for implementation.

Q.NO.44. DISCUSS THE FACTORS TO BE CONSIDERED TO VALIDATE A VENDOR'S PROPOSAL AT THE TIME OF SOFTWARE ACQUISITION. (B) (M16 - 4M)

The following considerations are valid for both acquisition of hardware and software:

a) **Vendor Selection:**

i) This step is a critical step for success of process of acquisition of systems.

ii) It is necessary to remember that vendor selection is to be done prior to sending RFP.

iii) The result of this process is that 'RFP are sent only to selected vendors'.

iv) For vendor selection, following things are kept in mind including the background and locational advantage of the vendor, the financial stability of vendor, the market feedback of vendor performance, in terms of price, services etc.

b) **Geographical Location of Vendor:**

i) The issue to look for whether the vendor has local support persons. Otherwise, the proposals submitted by vendor not as per RFP requirements need to rejected, with no further discussion on such rejected proposals.

ii) This stage may be referred to as 'technical validation', that is to check the proposals submitted by vendors, are technically complying with RFP requirements.

c) **Presentation by Selected Vendors:**

i) All vendors, whose proposals are accepted after "technical validation", are allowed to make presentation to the System Acquisition Team.

ii) The team evaluates the vendor's proposals by using various techniques.

d) **Evaluation of Users Feedback:**

i) The best way to understand the vendor systems is to analyze the feedback from present users.

ii) Present users can provide valuable feedback on system, operations, problems, vendor response to support calls.

Q.NO.45. DISCUSS SOME SPECIFIC CONSIDERATIONS FOR ACQUISITION OF HARDWARE AND SOFTWARE WITH REFERENCE TO ACQUISITION OF SYSTEM FROM SELECTED VENDORS (C)

The, some specific considerations for hardware and software acquisition are described as follows:

i) The benchmark tests to be done for proposed machine. For hardware's, there are specified standard benchmark tests defined based on the nature of hardware. These need to be applied to proposed equipment.

ii) Software considerations that can be current applications programs or new programs that have been designed to represent planned processing needs.

iii) The benchmarking problems are oriented towards testing whether a computer offered by the vendor meets the requirements of the job on hand of the buyer.

iv) The benchmarking problems would then comprise long jobs, short jobs, printing jobs, disk jobs, mathematical problems, input and output loads etc., in proportion typical of the job mix.

v) If the job is truly represented by the selected benchmarking problems, then this approach can provide a realistic and tangible basis for comparing all vendors' proposals. Tests should enable buyer to effectively evaluate cross performance of various systems in terms of hardware performance (CPU and input/output units), compiler language and operating system capabilities, diagnostic messages, ability to deal with certain types of data structures and effectiveness of software utilities.

vi) Benchmarking problems, however, suffer from a couple of disadvantages. It takes considerable time and efforts to select problems representative of the job mix which itself must be precisely defined. It also requires the existence of operational hardware, software and services of systems. Nevertheless, this approach is very popular because it can test the functioning of vendors' proposal. The manager can extrapolate in the light of the results of benchmarking problems, the performance of the vendors' proposals on the entire job mix.

Q.NO.46. WRITE SHORT NOTES ON SOFTWARE AND HARDWARE ACQUISITION? (C) (RTP N16)

1. After a system is designed, either partially or fully, the next phase of the system development starts which relates to the acquisition of hardware, software and services.
2. **Hardware Acquisition:**
   - **a)** In case of procuring such machinery such as machine tools, transportation equipment, air conditioning equipment, etc., the management can normally rely on the time tested selection techniques and the objective selection criteria can be delegated to the technical specialist.
   - **b)** The management depends upon the vendor for support services, systems design, education and training etc., and expansion of computer installation for almost an indefinite period; therefore, this is not just buying the machine and paying the vendor for it but it amounts to an enduring alliance with the supplier.
3. **Software Acquisition:**
   - **a)** Once user output and input designs are finalized, the nature of the application software requirements must be assessed by the systems analyst.
   - **b)** This determination helps the systems development team to decide what type of application software products is needed and consequently, the degree of processing that the system needs to handle.
   - **c)** This helps the system developers in deciding about the nature of the systems software and computer hardware that will be most suitable for generating the desired outputs, and also the functions and capabilities that the application software must possess.
   - **d)** At this stage, the system developers must determine whether the application software should be created in-house or acquired from a vendor.

Q.NO.47. WRITE SHORT NOTES CONTRACTS, SOFTWARE LICENSES AND COPYRIGHT VIOLATIONS? (B)

1. Contracts between an organization and a software vendor should clearly describe the rights and responsibilities of the parties to the contract.
2. The contracts should be in writing with sufficient detail to provide assurances for performance, source code accessibility, software and data security, and other important issues.
3. Software license is a license that grants permission to do things with computer software.
4. The usual goal is to authorize activities which are prohibited by default by copyright law, patent law, trademark law and any other intellectual property right.
5. The reason for the license, essentially, is that virtually all intellectual property laws were enacted to encourage disclosure of the intellectual property.
6. Copyright laws protect proprietary as well as open-source software. The use of unlicensed software or violations of a licensing agreement expose organizations to possible litigation.

Q.NO.48. WHAT IS VENDOR EVALUATION? DEFINE THE PROCESS FOR THE SAME? (OR) BRIEFLY DISCUSS ABOUT VARIOUS FACTORS WHICH SHOULD BE CONSIDERED EVALUATING THE VENDOR PROPOSAL FOR SUPPLY OF COMPUTER SYSTEM? (OR) DISCUSS THE FACTORS TO BE CONSIDERED FOR VALUATION OF A VENDOR'S PROPOSAL? (A) (PM, M – 05, 06, J – 09)

1. This process consists of evaluating and ranking the proposals submitted by vendors and is quite difficult, expensive and time consuming, but in any case it has to be gone through.
2. This problem is made difficult by the fact that vendors would be offering a variety of configurations.
3. The factors have to be considered towards rigorous evaluation.
   - a) The Performance Capability of Each Proposed System in Relation to its Costs
   - b) The Costs and Benefits of Each Proposed System
   - c) The Maintainability of Each Proposed System
   - d) The Compatibility of Each Proposed system with Existing Systems
   - e) Vendor Support

Q.NO.49. EXPLAIN THE VARIOUS METHODS FOR VALIDATING THE PROPOSALS? (A) (RTP M14, N16)

1. Mandatory requirements would constitute overriding criteria in that, if a vendor fails to meet them, he would be screened out without any further consideration.
2. The desirable characteristics would surely be more difficult to evaluate because the vendors may ignore them or offer several alternatives.
3. The criteria may be listed in a descending order of importance.
4. After having established and ranked the criteria, next comes the question of validating the vendor's proposals against these.
5. The method selected may be a simple or a sophisticated one.
6. Large organizations would naturally tend to adopt a sophisticated and objective approach.
7. The following are some of the validation methods.

1. Checklists:

- a) It is the most simple and rather a subjective method for validation and evaluation.
- b) The various criteria are put in check list in the form of suitable questions against which the responses of the various vendors are validated.
- c) For example : Support Service Checklists may have parameters like – Performance; System development; Maintenance; Conversion; Training; Back-up; Proximity; Hardware; Software.

2. Point-Scoring Analysis: (Point scoring analysis in vendor evaluation) (N - 03)

- a) Point-scoring analysis provides an objective method of selecting a final system.
- b) There are no absolute rules in the selection process, only guidelines for matching user needs with software capabilities.
- c) Thus, even for a small business, the evaluators must consider such issues as the company's data processing needs, its in-house computer skills, vendor reputations, software costs, and so forth.

3. Public evaluation reports:

- a) Several consultancy agencies compare and contrast the hardware and software performance for various manufacturers and publish their reports in this regard.

- **b)** This method has been frequently and usefully employed by several buyers in the past.
- **c)** For those criteria, however, where published reports are not available, resort would have to be made to other methods of validation.
- **d)** This method is particularly useful where the buying staff has inadequate knowledge of computer facts.

4. **Bench marking problem for vendor's proposals:** **(N 06 – 5M)**
   - **a)** Benchmarking problems for vendors' proposals are sample programs that represent actual processing workload or at least a part of the buyer's primary computer work load and include current applications programs or new programs that have been designed to represent processing needs.
   - **b)** That is, benchmarking problems are oriented towards testing whether a computer offered by the vendor meets the requirements of the job on hand of the buyer.
5. **Test problems:** Test problems disregard the actual job mix and are devised to test the true capabilities of the hardware, software or system.

Q.NO.50. DISCUSS THE CHARACTERISTICS OF A GOOD CODING SYSTEM? (OR) WHAT ARE THE FEATURES OF GOOD CODED PROGRAM? (A)

(PM, RTP N13, N15, M – 05, 08, N08, N16 – 6M)

1. **Reliability:** It refers to the consistence which a program provides over a period of time. However poor setting of parameters and hard coding some data subsequently could result in the failure of a program after some time.
2. **Robustness:** It refers to the process of taking into account all possible inputs and outputs of a program in case of least likely situations.
3. **Accuracy:** It refers not only to what program is supposed to do, but should also take care of what it should not do.
4. **Efficiency:** It refers to the performance which should not be unduly affected with the increase in input values.
5. **Usability:** It refers to a user-friendly interface and easy-to-understand document required for any program.
6. **Readability:** It refers to the ease of maintenance of program even in the absence of the program developer.

Q.NO.51. WHAT ARE THE STAGES OF PROGRAM DEVELOPMENT LIFE CYCLE? (B)

The stages are:

- **a)** Program analysis
- **b)** Program design
- **c)** Program coding
- **d)** Debug the program
- **e)** Program documentation
- **f)** Program maintenance

Q.NO.52. WRITE SHORT NOTES ON PROGRAM CODING STANDARDS. (C)

1. The logic of the program outlined in the flowcharts is converted into program statements or instructions at this stage.
2. For each language, there are specific rules regarding format or syntax. Syntax means vocabulary, punctuation and grammatical rules for a particular programming language.
3. Different programmers may write a program using different sets of instructions but each giving the same results.

4. Therefore, the coding standards are defined which serves as a method of communication between teams, amongst the team members and users, thus working as a good control. Coding standards minimize the system development setbacks due to programmer turnover.
5. Coding standards provide, simplicity, efficient utilization of storage and least processing time.

Q.NO.53. WRITE ABOUT PROGRAMMING LANGUAGES? (B)

1. Application programs are coded on the form of statements or instructions and the same is converted by the compiler to binary machine for the computer to understand and execute.
2. The programming languages commonly used are:
   a) High – level general purpose programming language such as COBOL and C language.
   b) Object oriented languages such as C++, JAVA etc.
   c) Scripting language like JavaScript, VBScript.
   d) Decision Support or Expert System languages like PROLOG.
3. **Choice of Programming Language:** The most important criteria on the basis of which the language to be used should be decided on
   a) The basis of application area
   b) Algorithmic complexity
   c) Environment in which software has to be executed
   d) Performance consideration
   e) Data structure complexity
   f) Knowledge of software development staff
   g) Capability of in-house staff for maintenance

Q.NO.54. WRITE ABOUT PROGRAM DEBUGGING? (B) (N – 01, RTP M16, M17)

1. The process of debugging a program refers to correcting programming language syntax and diagnostic errors so that the program "compiles cleanly".
2. A clean compile means that the program can be successfully converted from the source code written by the programmer into machine language instructions.
3. Once, the programmer achieves a clean compile, the program is ready for structured walk through.
4. Debugging consists of four steps:
   a) Inputting the source program to the compiler,
   b) Letting the compiler find errors in the program,
   c) Correcting lines of code that are in error, and
   d) Resubmitting the corrected source program as input to the compiler.

Q.NO.55. EXPLAIN ABOUT TESTING THE PROGRAM? (B) (RTP M16)

1. A careful and thorough testing of each program is imperative to the successful installation of any system.
2. The test plan should require the execution of all standard processing logic.
3. Software packages are available that allow interactive testing of batch-processing programs.
4. They greatly reduce the length of time required for testing.

5. Interactive testing allows the programmer to monitor each step required to process a program input.
6. If a problem in program logic flow is discovered, the programmer can stop the execution of the program, correct the problem, and have the program resume processing at a point just prior to the interruption.

Q.NO.56. WRITE ABOUT PROGRAM DOCUMENTATION? (B) (M – 08)

1. The writing of narrative procedures and instructions for people who will use software is done throughout the program life cycle.
2. Managers and users should carefully review documentation in order to ensure that the software and system behave as the documentation indicates.
3. If they do not, documentation should be revised.
4. User documentation should also be reviewed for understandability i.e. the documentation should be prepared in such a way that the user can clearly understand the instructions.

Q.NO.57. WRITE ABOUT PROGRAM MAINTENANCE? (A)

1. The requirements of business data processing applications are subject to continual change.
2. This calls for modification of the various programs.
3. Usually separate categories of programmers called maintenance programmers who are entrusted with this task.
4. There is a difficult task of understanding and then revising the program they did not write.

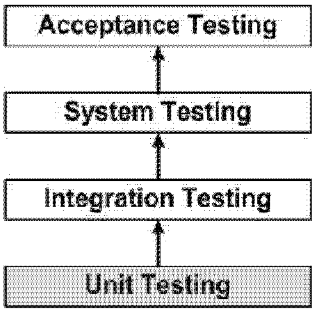
Q.NO.58. WRITE SHORT NOTES ON SYSTEM TESTING? (A) (M01, 08)

1. Testing is a process used to identify the correctness, completeness and quality of developed computer software.
2. Testing should systematically uncover different classes of errors in a minimum amount of time and with a minimum amount of effort.
3. The data collected through testing can also provide an indication of the software's reliability and quality.
4. Different levels of testing are:
   - a) Unit testing.
   - b) Integration testing.
   - c) System testing.
   - d) Final acceptance testing.

Q.NO.59. WHAT IS UNIT TESTING? WHAT ARE THE ASPECTS OF TESTS THAT CAN BE PERFORMED ON A PROGRAM UNIT? (OR) WHAT IS UNIT TESTING? EXPLAIN FIVE CATEGORIES OF TESTS THAT A PROGRAMMER TYPICALLY PERFORMS ON A PROGRAM UNIT. (OR) TESTING A PROGRAM UNIT IS ESSENTIAL BEFORE IMPLEMENTING IT. NAME ANY FOUR CATEGORIES OF TEST; A PROGRAMMER TYPICALLY PERFORMS ON A PROGRAM UNIT. (A) (PM, N14 - 5M, M15 - 4M, N15 - 6M, MTP N15)

1. Unit testing is a software verification and validation method in which a programmer tests if individual units of source code are fit for use.

2. A unit is the smallest testable part of an application which may be an individual program, function, procedure, etc.



3. There are five categories of tests that a programmer typically performs on a program unit:

   a) **Functional Tests:**

      i) Functional Tests check 'whether programs do what they are supposed to do or not'.

      ii) 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.

   b) **Performance Tests:** Performance Tests should be designed to verify the response time, the execution time, primary and secondary memory utilization and the traffic rates on data channels (or) communication links.

   c) **Stress Tests:**

      i) Stress testing is a form of testing that is used to determine the stability of a given system or entity.

      ii) It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results.

      iii) 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.

   d) **Structural Tests:**

      i) Structural Tests are concerned with examining the internal processing logic of a software system.

      ii) For example, if a function is responsible for tax calculation, the verification of the logic is a structural test.

   e) **Parallel Tests:**

      In Parallel Tests, the same test data is used in the new and old system and the output results are then compared.

Q.NO.60. EXPLAIN DIFFERENT TYPES OF UNIT TESTING?(A) (PM, MTP N16 - 8M)

STATIC ANALYSIS TESTING:

Some important Static Analysis Tests are:

1. **Desk Check:** This is done by the programmer himself. He checks for logical syntax errors, and deviation from coding standards.

2. **Structured walk-through:** The application developer leads other programmers through the text of the program and explanation to uncover errors.

3. **Code inspection:** The program is reviewed by a formal committee. Review is done with formal checklists.

DYNAMIC ANALYSIS TESTING: (RTP N13, N14, MTP N14, M16 – 6M)

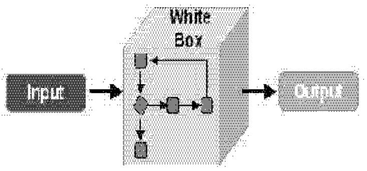
1. **Black Box Testing:**

   a) Black box testing is a software testing techniques in which functionality of the software under test is tested without looking at the internal code structure, implementation details and knowledge of internal paths of the software.

Input
Black Box
Output

- **b)** This type of testing is based entirely on the software requirements and specifications.
- **c)** These tests can be functional or non-functional, though usually functional.
- **d)** The test designer selects valid and invalid inputs and determines the correct output.
- **e)** There is no knowledge of test objects internal structures.
- **f)** While this method can uncover unimplemented parts of the specification, one cannot be sure that all existent paths are tested.
- **g)** If a module performs a function which is not supposed to, the black box test does not identify it.

2. White Box Testing:

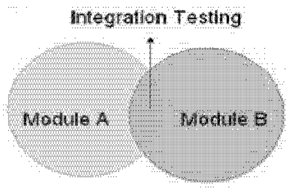


- **a)** White Box Testing also known as Clear Box Testing, Open Box Testing, and Glass Box Testing is a software testing method in which the internal structure/design/implementation of the item being tested is known to the tester.
- **b)** It requires programming skills to identify all paths through the software.
- **c)** It is applicable at the unit, integration and system levels of the testing process, it is typically applied to the unit.
- **d)** 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.
- **e)** After obtaining a clear picture of the internal workings of a product, software tests can be conducted to ensure that the internal operation of the product conforms to specifications and all the internal components are adequately exercised.

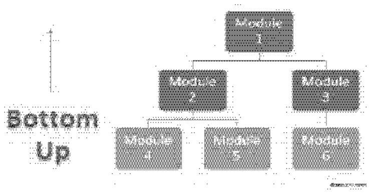
3. Grey Box Testing:

- **a)** Gray box testing is a software testing technique that uses a combination of black box testing and white box testing.
- **b)** In gray box testing, the tester applies a limited number of test cases to the internal workings of the software under test.
- **c)** In the remaining part of the gray box testing, one takes a black box approach in applying inputs to the software under test and observing the outputs.

Q.NO.61. WRITE SHORT NOTES ON INTEGRATION TESTING? EXPLAIN THE DIFFERENT METHODS OF INTEGRATION TESTING AND ALSO EXPLAIN ABOUT REGRESSION TESTING? (A) (MTP M16 – 6M)



1. Integration testing is an activity of software testing in which individual software modules are combined and tested as a group.
2. It occurs after unit testing and before system testing with an objective to evaluate the connection of two or more components that pass information from one area to another.
3. Integration testing takes as its input - modules that have been unit tested, groups them in larger aggregates, applies tests defined in an integration test plan to those aggregates, and delivers as its output the integrated system ready for system testing.
4. This is carried out in the following manner:



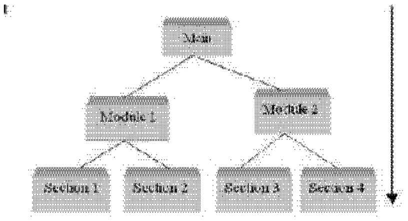
- **a) Bottom-up Integration:**
  - **i)** Bottom-up integration is the traditional strategy used to integrate the components of a software system into a functioning whole.

ii) It consists of unit testing, followed by sub-system testing, and then testing of the entire system.

iii) Bottom-up testing is easy to implement as at the time of module testing, tested subordinate modules are available.

iv) The disadvantage is that testing of major decision / control points is deferred to a later period.

b) Top-down Integration:



i) Top-down integration starts with the main routine, and then testing as we do further down the system.

ii) Since decision- making processes are likely to occur in the higher levels of program hierarchy, the top-down strategy emphasizes on major control decision points encountered in the earlier stages of a process and detects any error in these processes.

c) Regression Testing:

i) Each time a new module is added as part of integration testing, the software changes.

ii) New data flow paths are established, new I/O may occur and new control logic is invoked.

iii) These changes may cause problems with functions that previously worked flawlessly.

iv) In the context of the integration testing, the regression tests ensure that changes or corrections have not introduced new errors.

v) The data used for the regression tests should be the same as the data used in the original test.

Q.NO.62. WHAT ARE THE DIFFERENT TYPES OF SYSTEM TESTING? (A) (N13- 4M, RTP M15)

1. System testing is a process in which software and other system elements are tested as a whole.
2. System testing begins either when the software as a whole is operational or when the well defined subsets of the software's functionality have been implemented.
3. The purpose of system testing is to ensure that the new or modified system functions properly.
4. These test procedures are often performed in a non- production test environment.
5. The types of testing that might be carried out are as follows :

a) Recovery Testing:

i) This is the activity of testing 'how well the application is able to recover from crashes, hardware failures and other similar problems'.

ii) Recovery testing is the forced failure of the software in a variety of ways to verify that recovery is properly performed.

b) Security Testing:

i) This is the process to determine that an Information System protects data and maintains functionality as intended or not.

ii) The six basic security concepts that need to be covered by security testing are – confidentiality, integrity, authentication, authorization, availability and non-repudiation.

iii) This testing technique also ensures the existence and proper execution of access controls in the new system.

c) Stress or Volume Testing:

i) Stress testing is a form of testing that is used to determine the stability of a given system or entity.

ii) It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results.

iii) Stress testing may be performed by testing the application with large quantity of data during peak hours to test its performance.

d) **Performance Testing:**

i) In the computer industry, software performance testing is used to determine the speed or effectiveness of a computer, network, software program or device.

ii) This testing technique compares the new system's performance with that of similar systems using well defined benchmarks.

Q.NO.63. WRITE SHORT NOTES ON USER FINAL ACCEPTANCE TESTING? EXPLAIN THE MAJOR ASPECTS OF SUCH TESTING? (B) (N16 – 4M, RTP M - 14)

1. Final Acceptance Testing is conducted when the system is just ready for implementation.
2. During this testing, it is ensured that the new system satisfies the quality standards adopted by the business and the system satisfies the users.
3. Thus the final acceptance testing has two major parts:

a) **Quality Assurance Testing:** It ensures that the new system satisfies the prescribed quality standards and the development process is as per the organization's quality assurance methodology.

b) **User Acceptance Testing:**

i) It ensures that the functional aspects expected by the users have been well addressed in the new system.

ii) There are two types of the user acceptance testing :

- **Alpha Testing:** This is the first stage, often performed by the users within the organization.
- **Beta Testing:** This is the second stage, generally performed by the external users.

Q.NO.64. THERE ARE SEVERAL CONTROLS THAT CAN BE EXERCISED INTERNALLY TO ASSURE THE TESTING PHASE QUALITY AND EFFICIENCY. THOUGH IT VARIES FROM ONE ORGANIZATION TO ANOTHER, SOME OF THE GENERIC KEY CONTROL ASPECTS APPEAR TO BE ADDRESSED BY THE RESPONSES TO SOME QUERIES. DISCUSS THE QUERIES TO BE ADDRESSED (C)

Internal Testing Controls: There are several controls that can be exercised internally to assure the testing phase quality and efficiency. Though it varies from one organization to another, some of the generic key control aspects appear to be addressed by the responses to following queries:

i) Whether the test-suite prepared by the testers includes the actual business scenarios?

ii) Whether test data used covers all possible aspects of system?

iii) Whether CASE tools like 'Test Data Generators' have been used?

iv) Whether test results have been documented?

v) Whether tests have been performed in their correct order?

vi) Whether modifications needed based on test results have been done?

vii) Whether modifications made have been properly authorized and documented?

Q.NO.65. WRITE ABOUT SYSTEM IMPLEMENTATION. (A)

a) Systems implementation includes all those activities that take place to convert from the old system to the new.

b) The new system may be totally new, replacing an existing manual or automatic system or it may be a major modification in an existing system.

c) Objective:

To implement the new system i.e. put it into production.

d) Activities: The activities involved in System Implementation are as follows :

- **i)** Conversion of data to the new system files.
- **ii)** Training of end users.
- **iii)** Completion of user documentation.
- **iv)** System changeover.
- **v)** Evaluation of the system at regular intervals.

e) Document / Deliverable: A full functional / documented system in its operational environment.

Q.NO.66. DESCRIBE THE VARIOUS STEPS THAT SHOULD BE TAKEN FOR SUCCESSFUL INSTALLATION OF EQUIPMENT DURING THE SYSTEM IMPLEMENTATION PHASE? (B) (M - 07)

1. The process of ensuring that the information system is operational and then allowing users to take over its operation for use and evaluation is called systems implementation.
2. Implementation includes all those activities that take place to convert from the old system to the new.
3. Aspects of implementation are as follows.

Equipment Installation :

a) The hardware required to support the new system is selected prior to the implementation phase.

b) The necessary hardware should be ordered in time to allow for installation and testing of equipment during the implementation phase.

c) An installation checklist should be developed at this time with operating advice from the vendor and system development team.

d) In those installations where people are experienced in the installation of the same or similar equipment, adequate time should be scheduled to allow completion.

i) Site Preparation:

- An appropriate location must be found to provide an operating environment for the equipment that will meet the vendor's temperature, humidity and dust control specifications.
- It is very important to lay down proper procedures for acquiring and planning space layout in the systems implementation.
- If the system is a microcomputer, little layout and site preparation work is needed.
- The electric lines should be checked to ensure that they are free of static or power fluctuation. It will be better to install a clean line that is not shared by other equipments.

ii) Equipment check out :

- The equipment must be turned on for testing under normal operating conditions.

- Not only the routine should be run by the vendor, but also the implementation team should devise and run extensive tests of its own to ensure that equipments are in proper working condition.

iii) Installation of New Hardware / Software:

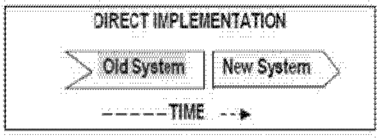
- The equipment must be physically installed by the manufacturer, connected-to the power source and wired to communication lines, if required.
- If the new system interfaces with the other systems or is distributed across multiple software platforms, some final commissioning tests of the production environment may be desirable to prove end to end connectivity.

Q.NO.67. WHAT IS THE PURPOSE OF SYSTEM TRAINING? HOW THE USER AND OPERATOR TRAINING DO DIFFER? (OR)
WHAT IS PERSONNEL TRAINING IMPORTANT FOR THE SUCCESSFUL IMPLEMENTATION OF INFORMATION SYSTEM? WHAT TYPE OF TRAINING SHOULD BE IMPORTANT TO SYSTEM OPERATORS AND USERS? (A) (M – 03, 06, 10)

1. A system can succeed or fail depending on the way it is operated and used.
2. The quality of training received by the personnel involved with the system in various capacities helps the successful implementation of information system.
3. Training is becoming a major component of systems implementation.
4. When a new system is acquired which often involves new hardware and software, both users and computer professionals generally need some type of training. Often this is imparted through classes, which are organized by vendor, and through hands-on learning techniques.

Q.NO.68. EXPLAIN THE MAJOR STRATEGIES INVOLVED IN CONVERSION OF CHANGEOVER FROM MANUAL SYSTEM TO COMPUTERIZED SYSTEMS OR EXPLAIN VARIOUS SYSTEM IMPLEMENTATION CONVERSION STRATEGIES? (OR)
EXPLAIN THE DIFFERENT CONVERSION STRATEGIES USED FOR CONVERSION FROM MANUAL TO COMPUTERIZED SYSTEM? ENUMERATE THE ADVANTAGES AND DISADVANTAGES OF EACH STRATEGY? (OR)
EXPLAIN THE ADVANTAGES OF AND ALSO DISADVANTAGES OF PARALLEL CONVERSION FROM MANUAL TO COMPUTERIZED SYSTEM? (OR)
EXPLAIN DIFFERENT CHANGEOVER STRATEGIES USED FOR CONVERSION FROM OLD SYSTEM TO NEW SYSTEM. (A) (PM, M –07, 09, RTP M15, M16, M14)

1. Conversion or changeover is the process of changing from the old system (manual system) to the new system.
2. It requires careful planning to establish the basic approach to be used in the actual changeover.
3. **Conversion strategies:**



Direct Implementation

a) Direct Implementation / Abrupt change-over:

i) This is achieved through an abrupt (sudden) takeover – an all or nothing approach.

ii) With this strategy, the changeover is done in one operation, completely replacing the old system in one go.

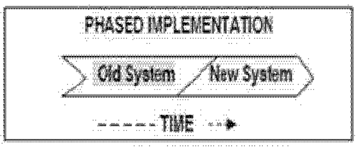
iii) Direct Implementation which usually takes place on a set date, often after a break in production or a holiday period so that time can be used to get the hardware and software for the new system installed without causing too much disruption.

b) Phased Implementation:

i) With this strategy, implementation can be staged with conversion to the new system taking place by degrees.

ii) For example - some new files may be converted and used by employees whilst other files continue to be used on the old system ie. the new is brought in stages (phases).

iii) If each phase is successful then the next phase is started, eventually leading to the final phase when the new system fully replaces the old one.

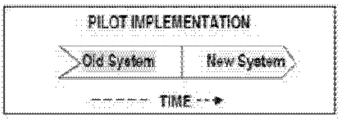


Phase Implementation

c) Pilot Implementation :

i) With this strategy, the new system replaces the old one in one operation but only on a small scale.

ii) Any errors can be rectified or further beneficial changes can be introduced and replicated throughout the whole system in good time with the least disruption.

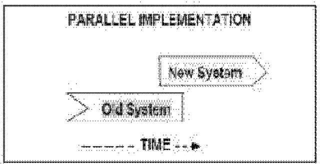


Pilot Implementation

iii) For example - it might be tried out in one branch of the company or in one location. If successful then the pilot is extended until it eventually replaces the old system completely.

d) Parallel Running Implementation: (RTP M14)

i) This is considered the most secure method with both systems running in parallel over an introductory period.



ii) The old system remains fully operational while the new systems come online.

iii) With this strategy, the old and the new system are both used alongside each other, both being able to operate independently.

iv) If all goes well, the old system is stopped and new system carries on as the only system.

Q.NO.69. EXPLAIN THE MAJOR ACTIVITIES INVOLVED IN CONVERSION PROCEDURE? (OR) DISCUSS BRIEFLY VARIOUS ACTIVITIES INVOLVED FOR SUCCESSFUL CONVERSION OF AN EXISTING MANUAL SYSTEM TO A COMPUTERIZED INFORMATION SYSTEM? (OR) WHEN THE EXISTING INFORMATION SYSTEM IS TO BE CONVERTED INTO A NEW SYSTEM, WHAT ARE THE ACTIVITIES INVOLVED IN THE CONVERSION PROCESS? (B) (PM, M – 10, N07, N 10, RTP M15)

1. Conversion includes all those activities which must be completed to successfully convert from the previous system to the new information system.

2. These activities can be classified as follows:

   a) Procedure conversion;

   b) File conversion

   c) System conversion

   d) Scheduling personnel and equipment;

a) Procedure conversion:

i) Operating procedures should be completely documented for the new system.

ii) This applies to both computer-operations and functional area operations.

iii) Information on input, data files, methods, procedures, output, and internal control must be presented in clear, concise and understandable terms for the average reader.

iv) Written operating procedures must be supplemented by oral communication during the training sessions on the system change.

b) File conversion: (RTP N16)

- **i)** Large files of information must be converted from one medium to another.
- **ii)** Present manual files are likely to be inaccurate and incomplete where deviations from the accepted format are common.
- **iii)** These files suffer from the shortcomings of inexperienced - and, at times, indifferent - personnel whose jobs are to maintain them.
- **iv)** Computer generated files tend to be more accurate and consistent.
- **v)** If the existing system is operating on a computer but of different configuration, the formats of the present computer files are generally unacceptable for the new system.

c) System conversion: (M13, RTP N16)

- **i)** After on-line and off-line files have been converted and the reliability of the new system has been confirmed for a functional area, daily processing can be shifted from the existing information system to the new one.
- **ii)** All transactions initiated after this time are processed on the new system.
- **iii)** System development team members should be present to assist and to answer any questions that might develop.
- **iv)** Consideration should be given to operating the old system for some more time to permit checking and balancing the total results of both systems.

d) Scheduling personnel and equipment:

- **i)** Scheduling data processing operations of a new information system for the first time is a difficult task for the system manager.
- **ii)** As users become more familiar with the new system, however, the job becomes more routine.
- **iii)** Schedules should be set up by the system manager in conjunction with departmental managers of operational units serviced by the equipment.
- **iv)** The master schedule for next month should provide sufficient computer time to handle all required processing.

e) Alternative plans in case of equipment failure:

- **i)** Alternative-processing plans must be implemented in case of equipment failure. Who or what caused the failure is not as important in case of equipment failure as the fact that the system is down.
- **ii)** Priorities must be given to those jobs critical to an organization, such as billing, payroll, and inventory. Critical jobs can be performed manually until the equipment is set right.
- **iii)** Documentation of alternative plans is the responsibility of the computer section and should be fully covered by the organization's systems and procedures manual.
- **iv)** A written manual of procedures concerning what steps must be undertaken will help to over come the unfavorable situation.

Q.NO.70. EXPLAIN THE CONCEPT OF POST IMPLEMENTATION REVIEW? (B) (N11- 4M)

1. A Post Implementation review answers the questions "did we achieve what we set out to do in business terms? And if not, what should be done?
2. The specific aims of a Post Implementation Review are:

a) Evaluate the project team's achievements against the original objectives set out in the Business Case

b) Measure and compare actual system performance against that specified

c) Compare actual incurred project costs against the original estimated costs, and make revised cost projections

d) Learn from the existing project for the future in order to avoid repeating mistakes.

In order to assess, review and assure the complete working solution, a number of activities may be planned. As no phase may be assured to be perfect, errors are liable to occur. Therefore, a well-formalized review must be undertaken including some of the systems maintenance activities, such as adding new data elements, modifying reports, adding new reports; and changing calculations. As the deliverable of this phase, a well written document stating observations, modifications, controls, scope of further improvements etc. may be prepared. Such aspects may also be availed in the form of responses to following queries:

a) Could further training or coaching improve the degree of benefit being generated?

b) Are there further functional improvements or changes that would deliver greater benefit?

c) Are specific improvements required in procedures, documentation, support, etc.?

d) What learning points are there for future projects?

Q.NO.71. EXPLAIN THE CONCEPT OF DEVELOPMENT EVALUATION, OPERATION EVALUATION AND INFORMATION EVALUATION? (A)

1. **Development evaluation:**

a) Evaluation of the development process is primarily concerned with whether the system was developed on schedule and within budget.

b) It requires schedules and budgets to be established in advance and those records of actual performance and cost be maintained.

c) It may be noted that very few information systems have been developed on schedule and within budget.

d) Many information systems are developed without clearly defined schedules or budgets.

e) Due to the uncertainty and mystique associated with system development, they are not subjected to traditional management control procedures.

2. **Operation evaluation:**

a) The evaluation of the information system's operation pertains to whether the hardware, software and personnel are capable to perform their duties. Operation evaluation answers such questions.

b) Operation evaluation is relatively straightforward if evaluation criteria are established in advance.

c) For example, if the systems analyst lays down the criterion that a system which is capable of supporting one hundred terminals should give response time of less than two seconds, evaluation of this aspect of system operation can be done easily after the system becomes operational.

3. **Information evaluation:**

a) An information system should also be evaluated in terms of information it provides.

b) This aspect of system evaluation is difficult and it cannot be conducted in a quantitative manner, as is the case with development and operation evaluations.

c) The objective of an information system is to provide information to support the organizational decision system.

d) Therefore, the extent to which information provided by the system is supportive to decision making is the area of concern in evaluating the system.

**Q.NO.72. WRITE SHORT NOTES ON SYSTEM MAINTENANCE? WHAT ARE THE DIFFERENT TYPES OF MAINTENANCE? (OR)
DEFINE AND DEFERENCE BETWEEN THE SCHEDULED AND RESCUE MAINTENANCE ALONG WITH THEIR RESPECTIVE BENEFITS? (OR)
MAINTAINING THE SYSTEM IS AN IMPORTANT ASPECT OF SYSTEM DEVELOPMENT. ELABORATE THE VARIOUS CATEGORIES OF SYSTEM MAINTENANCE. (A)
(PM, M16 - 6M, M17-5M, M14 – 6M, N08, M07 – 5M, N11 -4M, RTP N15, M16, MTP M16 – 4M)**

1. Most information systems require at least some modification after development.
2. The need for modification arises from a failure to anticipate all requirements during system design and/or from changing organizational requirements.
3. The changing organizational requirements continue to impact most information systems as long as they are in operation.
4. Consequently periodic systems maintenance is required for most of the information systems.
5. Systems maintenance involves adding new data elements, modifying reports, adding new reports, changing calculations, etc
6. Maintenance can be categorized in to :

a) **Scheduled maintenance:**

i) Scheduled maintenance is anticipated and can be planned for.

ii) For example, the implementation of a new inventory coding scheme can be planned in advance.

b) **Rescue maintenance:**

i) Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate solution.

ii) A system that is properly developed and tested should have few occasions of rescue maintenance.

c) **Corrective maintenance** **(MTP-N15-3M)**

i) Corrective maintenance deals with fixing bugs in the program code or defects found during executions.

ii) An error can result from design errors, coding errors etc.

iii) The need for corrective maintenance is usually initiated by bug reports drawn by end users.

d) **Adaptive maintenance:** **(MTP-N15-3M)**

i) Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system.

ii) The term environment in this context refers to the totality of all conditions and influences which act from outside upon the system. For example, business rule, government policies, work patterns, software and hardware operating platforms.

iii) The need for adaptive maintenance can only be recognized by monitoring the environment.

e) **Perfective maintenance:** Perfective maintenance mainly deals with accommodating to new or changed user requirements and concerns functional enhancements to the system and activities to increase the system's performance or to enhance its user interface.

f) **Preventive maintenance**

i) Preventive maintenance concerns activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system.

ii) The long-term effect of corrective, adaptive and perfective changes increases the system's complexity.

iii) As a large program is continuously changed, its complexity, which reflects deteriorating structure, increases unless work is done to maintain or reduce it. This work is known as preventive change.

Q.NO.73. WRITE SHORT NOTES OPERATIONS MANUAL? (B)

1. A user's guide known as an Operation Manual is a technical communication document intended to give assistance to people using a particular system.
2. It is usually written by a technical writer, although user guides are written by companies.
3. Operation manuals are most commonly associated with electronic goods, computer hardware and software.
4. The section of an operation manual include the following :

   a) A cover page, a title page and copyright page;

   b) A preface, containing details of related documents and information on how to navigate the user guide;

   c) A contents page;

   d) A guide on how to use at least the main functions of the system;

   e) A troubleshooting section detailing possible errors or problems that may occur, along with how to fix them;

   f) A FAQ (Frequently Asked Questions);

   g) Where to find further help, and contact details;

   h) A glossary and, for larger documents, an index;

Q.NO.74. EXPLAIN THE AUDITOR'S ROLE IN SDLC? (B) (RTP M16)

1. The audit of systems under development can have three main objectives. It is primarily aimed to provide an opinion on the efficiency, effectiveness, and economy of project management.
2. An auditor's role is to assess the extent to which the system being developed provides for adequate audit trails and controls to ensure the integrity of data processed and stored; and the effectiveness of controls being enacted for the management of the system's operation.
3. In order to achieve these goals, an auditor has to attend project and steering committee meetings and examine project control documentation and conducting interviews.
4. A list of such objectives should be provided to the auditor.
5. The auditor should provide a list of the standard controls.
6. An Auditor may adapt a rating system such as on a scale of 1 to 10 in order to give rating to the various phases of SDLC.
7. While rating a Feasibility Study, an auditor can review Feasibility Study Report and different work products of this study phase.
8. An interview with personnel, who have conducted this feasibility study, can be conducted.
9. However, auditor will have to give control objectives, directives and in general, validate the opinion expressed by technical experts.
10. Some of the control considerations for an auditor include the following:

    a) Documented policy and procedures;

b) Established Project team with all infrastructure and facilities ;

c) Developers/ IT managers are trained on the procedures ;

d) Appropriate approvals are being taken at identified mile-stones;

e) Development is carried over as per standards, functional specifications;

f) Separate test environment for development/ test/ production / test plans;

g) Design norms and naming conventions are as per standards and are adhered to;

h) Business owners testing and approval before system going live;

i) Version control on programs;

j) Source Code is properly secured;

k) Adequate audit trails are provided in system

l) Appropriateness of methodologies selected.

11. Further, Post-Implementation Review is performed to determine whether the system adequately meets earlier identified business requirements and needs.

12. Auditors should be able to determine if the expected benefits of the new system are realized and whether users are satisfied with the new system.

13. In post implementation review, auditors need to review which of the SDLC phases have not met desired objectives and whether any corrective actions were taken.

14. If there are differences between expectations and actual results, auditors need to determine the reasons for the same.

15. Such reasons can help auditors to evaluate the current situation and offer guidelines for future projects.

Q.NO.75. IF YOU ARE THE PROJECT MANAGER OF A SOFTWARE COMPANY WITH THE RESPONSIBILITY FOR DEVELOPING A BREAK-THROUGH PRODUCT, COMBINING STATE OF THE ART HARDWARE AND SOFTWARE; WILL YOU OPT FOR PROTOTYPING AS A PROCESS MODEL FOR A PRODUCT MEANT FOR THE INTENSELY COMPETITIVE ENTERTAINMENT MARKET? (B) (PM)

Prototyping as a process model will be inappropriate and hence inadvisable for the following reasons:

a) Prototyping requires user involvement. Here, users are consumers of the product who are diffused and may not be inclined to join in.

b) When we try to test the product with the involvement of customers, confidential or critical information might get leaked to the competitors on our line of thinking. The element of surprise and also the opportunity to capture the market will be lost.

c) Prototyping requires significant time for experimenting. Since the product is meant for the intensely competitive entertainment market, the project manager may not have that much time to experiment, and the competitor may capture the market by entering the market in advance.

THE END

6. AUDITING OF INFORMATION SYSTEMS

Q.No.1. Define Information Systems Control? (B)

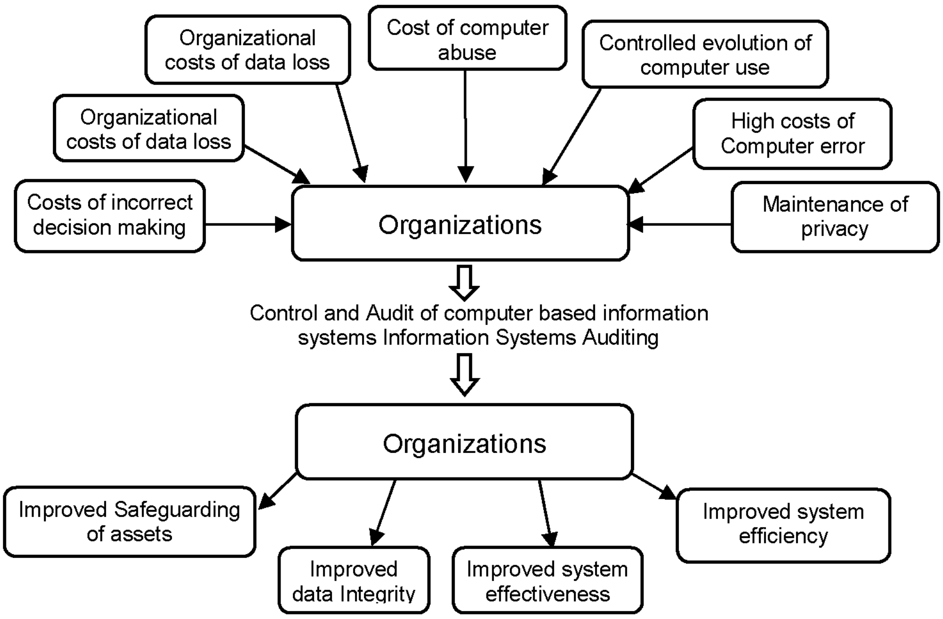
a) Controls are the Policies, Procedures, Practices and Organizational Structures, Designed to Provide Reasonable Assurance that Business Objectives will be achieved and that Undesired Events will be Prevented or Detected and Corrected.

b) Controls pertaining specifically to the Information Systems are referred as Information Systems Controls.

Q.No.2. What Is Information Systems Auditing? (B)

It is the process of attesting Objectives that focus on asset safeguarding and data integrity and Management Objectives that include not only attest objectives but also effectiveness and efficiency objectives.

Q.No.3. Why do we need Control and Audit of Information Systems? (OR) What are the factors influencing an organization towards control and audit of computers? (A) (PM, RTP M-16)



Organizational costs of data loss
Cost of computer abuse
Controlled evolution of computer use
Organizational costs of data loss
High costs of Computer error
Costs of incorrect decision making
Organizations
Maintenance of privacy
Control and Audit of computer based information systems Information Systems Auditing
Organizations
Improved Safeguarding of assets
Improved data Integrity
Improved system effectiveness
Improved system efficiency

Impact of control and audit influencing an organization

a) **To prevent Organizational Costs of Data Loss:** Control and Audit of Information Systems is required to protect Data Loss, as data is the most critical resource for an organization for its present as well as future development.

b) **To ensure Correct Decision Making:** Control and Audit of Information Systems ensure that accurate data is available for managers to take high level decisions for detection, investigations and correction of out-of-control processes.

c) **To control Costs of Computer Abuse:** Unauthorized access to computer systems, computer viruses, unauthorized physical access to computer facilities and unauthorized copies of sensitive data can lead to destruction of assets (hardware, software, documentation etc.), and Control and Audit of Information Systems is required to control such access.

d) **Value of Computer Hardware, Software and Personnel:** These are critical resources of an organization which has a credible impact on its infrastructure and business competitiveness.

e) **High Costs of Computer Error:** In a computerised enterprise environment where many critical business processes are performed a data error during entry or process would cause great damage.

f) **Maintenance of Privacy:** Control and Audit of Information Systems ensures that data collected in a business process are adequately guarded and their privacy is maintained. These data could contain sensitive information about any individual, company etc.

g) **Controlled evolution of computer Use:** Technology use and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.

h) **Information Systems Auditing:** It is the process of attesting objectives that focus on asset safeguarding and data integrity and management objectives include not only attest objectives but also effectiveness and efficiency objectives.

(Write short notes on Objectives of IS Audit) (N15-4M)

i) **Asset Safeguarding Objectives:** The information system assets (hardware, software, data files etc.) must be protected by a system of internal controls from unauthorized access.

j) **Data Integrity Objectives:** The importance to maintain integrity of data of an organization depends on the value of information, the extent of access to the information and the value of data to the business from the perspective of the decision maker, competition and the market environment.

k) **System Effectiveness Objectives:** Audit of Information Systems ensures effectiveness of a system is continuously evaluated by auditing the characteristics and objective of the system to ascertain that it meets substantial user requirements.

l) **System Efficiency Objectives:** Control and Audit of Information Systems are required to optimize the use of various information system resources (machine time, peripherals, system software and labor) along with the impact on the computing environment.

Q.No.4. Discuss the effect of computers on audit trail and audit evidance due to computerization? (OR) Write short notes on effect of computers on evidence collection for audit (A) [PM, N15 - 6M, M15 - 4M, N14 - 6M RTP N13, MTP N16, M16,M15, N15]

Changes to Evidence Collection: Due to advent of information systems, there are several issues which are faced by the auditor:

(Discuss the issues relating to the performance of evidence collection and understanding the Reliability of controls. (OR) Compared to traditional audit, evidence collection has become more challenging with the use of computers to the auditors. What are the issues which affect evidence collection and understanding the reliability of controls in financial audit?)

a) **Data retention and storage:**

i) A client's storage capabilities may restrict the amount of historical data that can be retained "on-line" and readily accessible to the auditor.

ii) If the client has insufficient data retention capacities the auditor may not be able to review a whole reporting period transactions on the computer system.

b) **Absence of input documents:**

i) Transaction data may be entered into the computer directly without the presence of supporting documentation e.g. input of telephone orders into a telesales system.

ii) This results in less paperwork being available for audit examination.

c) Lack of a visible audit trail :

- **i)** The audit trails in some computer systems may exist for only a short period of time.
- **ii)** The absence of an audit trail will make the auditor's job very difficult and may call for an audit approach which involves auditing around the computer system by seeking other sources of evidence to provide assurance that the computer input has been correctly processed and output.

d) Lack of visible output :

- **i)** The results of transaction processing may not produce a hard copy form of output, i.e. a printed record.
- **ii)** In the absence of physical output it may be necessary for the auditor to directly access the electronic data retained on the client's computer.
- **iii)** This is normally achieved by having the client provide a computer terminal and being granted "read" access to the required data files.

e) Audit evidence.

- **i)** Certain transactions may be generated automatically by the computer system.
- **ii)** For example, a fixed asset system may automatically calculate depreciation on assets at the end of each calendar month.
- **iii)** The depreciation charge may be automatically transferred (journalized) from the fixed assets register to the depreciation account and hence to the client's income and expenditure account.

f) Legal evidence :

- **i)** Advent of information systems also causes impact on legal issues.
- **ii)** For example, the admissibility of the evidence provided by a client's computer system may need special consideration.

Changes to Evidence Evaluation: Evaluation of audit trail and evidence is to trace consequences of control strength and weakness through the system which includes:

a) System generated transactions: Financial systems may have the ability to initiate, approve and record financial transactions.

b) Automated transaction processing:

- **i)** Automated transaction processing systems can cause the auditor problems.
- **ii)** For example when gaining assurance that a transaction was properly authorized or in accordance with delegated authorities.

c) Systematic Error :

- **i)** Computers are designed to carry out processing on a consistent basis.
- **ii)** Given the same inputs and programming, they invariably produce the same output.
- **iii)** This consistency can be viewed in both a positive and a negative manner.

Q.No.5. Explain the responsibility for controls? (B)

a) Management is responsible for establishing and maintaining control to achieve the objectives of effective and efficient operations, and reliable information systems.

b) Management should consistently apply the internal control to meet each of the internal control objectives and to assess internal control effectiveness.

c) The number of management levels depends on the company size and organization structure, but generally there are three such levels senior, middle and supervisory.

d) Senior management is responsible for strategic planning and objectives, thus setting the course in the lines of business that the company will pursue.

e) Middle management develops the tactical plans, activities and functions that accomplish the strategic objectives.

f) Supervisory management oversees and controls the daily activities and functions of the tactical plan.

Q.No.6. What are the concepts covered under is audit? (B)

The Audit of an IS environment to evaluate the systems, practices and operations may include:

a) Assessment of internal controls within the IS environment to assure validity, reliability, and security information.

b) Assessment of the efficiency and effectiveness of the IS environment in economic terms.

Q.No.7. What are the skills requiered for an IS auditor? (or) Responsibility of IS auditor? (OR) ABC Ltd. is looking for a suitable IS Auditor. Please send an introductory note to ABC Ltd. Explaining your suitability by describing the skill set and competence you possess for the job other than your qualification. (A) (PM, RTP M17)

The audit objective and scope has a significant bearing on the skill and competence requirements of an IS auditor.

The set of skills that is generally expected of an IS auditor include:

i) Sound knowledge of business operations, practices and compliance requirements,

ii) Should possess the requisite professional technical qualification and certifications,

iii) An good understanding of information Risks and Controls,

iv) Knowledge of IT strategies, policy and procedure controls,

v) Ability to understand technical and manual controls relating to business continuity, and

vi) Good knowledge of Professional Standards and Best practices of IT controls and security.

Q.No.8. What are the functions of IS auditor? (B) (N15-5M)

a) Review of Inadequate information security controls (e.g. Missing or out of date antivirus controls, open computer ports, open systems without password or weak passwords etc.)

b) Review of Inefficient use of corporate resources, or poor governance (e.g. Huge spending on unnecessary IT projects like printing resources, storage devices, high power servers and workstations etc.)

c) Review of Ineffective IT strategies, policies and practices (including a lack of policies for use of Information and Communication Technology (ICT) resources, Internet usage policies, Security practices etc.)

d) Review of IT-related frauds (including phishing, hacking etc)

Q.No.9. Explain the various categories of IS audits? (OR) Explain major types of IS Audits in brief. (A) (PM, M17 - 6M, M15 - 6M, RTP N16, M15 MTP M17, N16, M14)

IT audits has been categorized in to five types:

a) **Systems and Applications:** An audit to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.

b) **Information Processing Facilities :** An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.

c) **Systems Development :** An audit to verify that the systems under development meet the objectives of the organization and to ensure that the systems are developed in accordance with generally accepted standards for systems development.

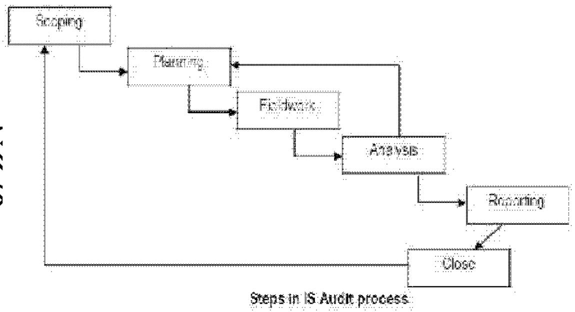
d) **Management of IT and Enterprise Architecture:** An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.

e) **Telecommunications, Intranets, and Extranets:** An audit to verify that controls are in place on the client (computer receiving services), server, and on the network connecting the clients and servers.

Q.No.10. What are the steps in information systems audit process? (OR) Explain major stages of IS Audits in brief? (OR) Different auditors go about IS auditing in different ways. Despite this, IS audit process can be categorized into broad categories. Discuss the statement explaining broad steps involved in the process (A) (PM, MTP N16)

.

Different audit organizations go about IS auditing in different ways and individual auditors have their own favorite ways of working.



Steps in IS Audit process

It can be categorized into six stages:

a) **Scoping and pre-audit survey :**

i) The auditors determine the main area/s of focus and any areas that are explicitly out-of-scope, based normally on some form of risk-based assessment.

ii) Information sources at this stage include background reading and web browsing, previous audit reports, pre audit interview, observations and, sometimes, subjective impressions that simply deserve further investigation.

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

c) **Fieldwork:** Gathering evidence by interviewing staff and managers, reviewing documents, printouts and data, observing processes etc.

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

e) **Reporting:** Reporting to the management is done after analysis of data gathered and analysis.

f) **Closure:** Closure involves preparing notes for future audits and following –up management to complete the actions they promised after previous audits.

Q.No.11. Write short notes on audit standards and best practices? (C)

a) IS auditors need guidance and a standard to measure the 3Es' (Economy, Efficiency and Effectiveness) of a system.

b) The objective is to determine on how to achieve implementation of the IS auditing standards, use professional judgment in its application and be prepared to justify any conflict.

c) The auditor needs guidance on how:

- Information System should be assessed to plan their audits effectively and efficiently.
- To focus their effort on high-risk areas
- To assess the severity of any errors or weaknesses found during the IS audit process.

d) The Institute of Chartered Accountants of India has issued various Standards on Auditing covering various aspects.

e) Although these standards are primarily concerned with the audit of financial information; they can be adapted for the purposes of IS Audit depending on its scope and objectives.

f) Several well-known organizations have given practical and useful information on IS Audit, which are given as follows:

i) ISACA (Information Systems Audit and Control Association): **Refer - Q.No.11**

ii) ISO 27001: **Refer - Q.No.12**

iii) **Internal Audit Standards:** IIA (The Institute of Internal Auditors) is an international professional association. This association provides dynamic leadership for the global profession of internal auditing. IIA issued Global Technology Audit Guide (GTAG). GTAG provides management of organisation about information technology management, control, and security and IS auditors with guidance on various information technology associated risks and recommended practices.

iv) **Standards on Internal Audit issued by ICAI:** The Institute of Chartered Accountants of India (ICAI) has issued various standards; the details are given in the Study Material of Auditing paper. The standards issued by the ICAI highlight the process to be adopted by internal auditor in specific situation.

v) The **Information Technology Infrastructure Library (ITIL): Refer - Q.No.13**

Q.No.11. Write short notes on ISACA (C)

ISACA (Information Systems Audit and Control Association): ISACA is a global leader in information governance, control, security and audit. ISACA developed the following to assist IS auditor while carrying out an IS audit.

a) **IS auditing standards:** ISACA issued 16 auditing standards, which defines the mandatory requirements for IS auditing and reporting.

b) **IS auditing guidelines:** ISACA issued 39 auditing guidelines, which provide a guideline in applying IS auditing standards.

c) **IS auditing procedures:** ISACA issued 11 IS auditing procedures, which provide examples of procedure an IS auditor need to follow while conducting IS audit for complying with IS auditing standards.

d) **COBIT (Control objectives for information and related technology):** This is a framework containing good business practices relating to information technology.

Q.No.12. Write short notes on ISO 27001. (C)

a) ISO 27001 is the international best practice and certification standard for an Information Security Management System (ISMS). An ISMS is a systematic approach to manage Information security in an IS environment It encompasses people and, processes.

b) ISO 27001 defines how to organise information security in any kind of organization, profit or non-profit, private or state-owned, small or large. It is safe to say that this standard is the foundation of information security management.

c) It also enables an organization to get certified, which means that an independent certification body has confirmed that information security has been implemented in the organisation as defined policies and procedures.

d) Many Indian IT companies have taken this certification, including INFOSYS, TCS, WIPRO. Companies getting themselves certified by as ISO 27001, are better competitor's to those not certified.

e) Companies certified generate a greater client assurance. It removes the dependency from individuals and put reliance on processes.

Q.No.13. Write short notes on ITIL. (C)

a) The ITIL is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business.

b) In its current form (known as ITILv3 and ITIL 2011 edition), ITIL is published in a series of five core publications, each of which covers an ITSM lifecycle stage.

c) ITIL describes procedures, tasks and checklists that are not organization-specific, used by an organization for establishing a minimum level of competency.

d) It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement.

Q.NO.14. How to perform is audit? (B)

a) An IS Auditor uses the equivalent concepts of materiality (in financial audits) and significance (in performance audits) to plan both effective and efficient audit procedures.

b) Materiality and significance are concepts the auditor uses to determine the planned nature, timing, and extent of audit procedures.

c) Materiality and significance include both quantitative and qualitative factors in relation to the subject matter of the audit.

d) For example, an application that provides public information via a website, if improperly configured, may expose internal network resources, including sensitive systems, to unauthorized access.

e) Planning occurs throughout the audit as an iterative process.

f) Planning activities are concentrated in the planning phase, during which the objectives are to obtain an understanding of the entity and its operations, including its internal control, identify significant issues, assess risk, and design the nature, extent, and timing of audit procedures.

g) The auditor must address many considerations that cover the nature, timing, and extent of testing.

h) The auditor must devise an auditing testing plan and a testing methodology to determine whether the previously identified controls are effective.

i) The auditor also tests whether the end-user applications are producing valid and accurate information.

j) Depending on the nature of the audit, computer-assisted techniques could also be used to audit the application.

k) The auditor should also conduct several tests with both valid and invalid data to test the ability and extent of error detection, correction, and prevention within the application.

l) Auditor may test the critical controls, processes, and apparent exposures.

m) The auditor performs the necessary testing by using documentary evidence, corroborating interviews, and personal observation.

n) Validation of the information obtained is prescribed by the auditor's work program. Again, this work program is the organized, written, and pre-planned approach to the study of the IT department.

o) It calls for validation in several ways, which are as follows:

i) Asking different personnel the same question and comparing the answers;

ii) Asking the same question in different ways at different times;

iii) Comparing checklist answers to work papers, programs, documentation, tests, or other verifiable results;

iv) Comparing checklist answers to observations and actual system results; and

v) Conducting mini-studies of critical phases of the operation.

p) The audit team selects one of the many Generalized Audit Software (GAS) packages such as Microsoft Access or Excel, IDEA, or ACL and determines what changes are necessary to run the software at the installation.

q) The auditor is to use one of these software's to do sampling, data extraction, exception reporting, summarize and foot totals, and other tasks to perform in-depth analysis and reporting capability.

Q.No.15. Write about basic planning phase in audit? (B)

a) Planning is one of the primary and important phases in an Information System Audit, which ensures that the audit is performed in an effective manner.

b) Planning takes more significance in case of Information Systems Audit since the audit risks are significantly impacted by inherent risk (inbuilt risk).

c) Planning develops the annual audit schedule to perform the individual audits.

d) It includes budgets of time and costs, and state priorities according to organizational goals and policies.

e) The objective of audit planning is to optimize the use of audit resources.

f) Planning also assists in proper assignment of work to assistants and in coordination of the work done by other auditors and experts.

g) Important points to be considered are :

i) The extent of planning will vary according to the size of the entity, the complexity of the audit and the auditor's experience with the entity and knowledge of the business.

ii) Obtaining knowledge of the business is an important part of planning the work.

iii) The auditor's knowledge of the business assists in the identification of events, transactions and practices which may have a material effect on the financial statements

iv) The auditor may wish to discuss elements of the overall audit plan and certain audit procedures with the entity's audit committee, the management and staff to improve the effectiveness and efficiency of the audit and to coordinate audit procedures with work of the entity's personnel.

v) The auditor should develop and document an overall audit plan describing the expected scope and conduct of the audit.

vi) The audit should be guided by an overall audit plan and underlying audit program and methodology.

h) The documentation of the audit plan is also a critical requirement. All changes to the audit plan should follow a change management procedure. Every change should be recorded with reason for change.

Q.No.16. Write about preliminary review phase? (A) (N16 - 4M, MTP N15)

The preliminary review of audit environment enables the auditor to gain understanding of the business, technology and control environment and also gain clarity on the objectives of the audit and scope of audit.

The following are some of the critical factors, which should be considered by an IS auditor as part of the preliminary review.

1. **Knowledge of the Business:**
   - **a)** General economic factors and industry conditions affecting the business,
   - **b)** Nature of Business, its products & services,
   - **c)** General exposure to business,
   - **d)** Its customers, vendors and most importantly, strategic business partners/associates to whom critical processes have been outsourced,
   - **e)** Level of competence of the Top management and IT Management, and
   - **f)** Finally, Set up and organization of IT department.
2. **Understanding the Technology:**

   [An important task for the auditor as a part of his/her preliminary evaluation is to gain a good understanding of the technology environment and related control issues. Explain major aspects that should be considered in this exercise.] (PM)
   - **a)** An important task for the auditor as a part of his preliminary evaluation is to gain a good understanding of the technology environment and related control issues.
   - **b)** This could include consideration of the following:
     - **i)** Analysis of business processes and level of automation,
     - **ii)** Assessing the extent of dependence of the enterprise on Information Technology.
     - **iii)** Understanding technology architecture.
     - **iv)** Studying network diagrams to understand physical and logical network connectivity,
     - **v)** Understanding extended enterprise architecture wherein the organization systems connect seamlessly with other stakeholders such as vendors (SCM), customers (CRM), employees (ERM) and the government,
     - **vi)** Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems,
     - **vii)** And finally, Studying Information Technology policies, standards, guidelines and procedures.
3. **Understanding Internal Control Systems:** For gaining understanding of Internal Controls emphasis to be placed on compliance and substantive testing.
4. **Legal Considerations and Audit Standards:**
   - **a)** The auditor should carefully evaluate the legal as well as statutory implications on his/her audit work.
   - **b)** The Information Systems audit work could be required as part of a statutory requirement in which case he should take into consideration the related stipulations, regulations and guidelines for conduct of his audit.
   - **c)** The IS Auditor should also consider the Audit Standards applicable to his conduct and performance of audit work.

5. **Risk Assessment and Materiality:**
   - **a)** Risk Assessment is a critical and inherent part of the Information Systems Auditor's planning and audit implementation.
   - **b)** It implies the process of identifying the risk, assessing the risk, and recommending controls to reduce the risk to an acceptable level, considering both the probability and the impact of occurrence.
   - **c)** Risk assessment allows the auditor to determine the scope of the audit and assess the level of audit risk and error risk.

Q.No.17. What are the key steps that can be followed for a risk-based approach to make an audit plan? Explain in brief. (C) (PM, N16-4M)

The steps that can be followed for a risk-based approach to make an audit plan are given as follows :

a. Inventory the information systems in use in the organization and categorize them.

b. Determine which of the systems impact critical functions or assets, such as money, materials, customers, decision making, and how close to real time they operate.

c. Assess what risks affect these systems and the likelihood and severity of the impact on the business.

d. Based on the above assessment, decide the audit priority, resources, schedule and frequency.

Q.No.18. What are the material errors that an auditor need to verify in information/financial report that may go undetected during the course of the audit in the stage of risk assessment. (C)

Risks that affect a system and taken into consideration at the time of assessment can be differentiated as inherent risks, control risks and detection risks. These factors directly impact upon the extent of audit risk which can be defined as the risk that the information/financial report may contain material error that may go undetected during the course of the audit. At this stage, the auditor needs to:

a) Assess the expected inherent, control and detection risk and identify significant audit areas.

b) Set materiality levels for audit purposes.

c) Assess the possibility of potential vulnerabilities, including the experience of past periods, or fraud.

Q.No.19. Explain different types of risks? (A) (M17 - 4M, N16 - 6M, N14 - 4M, RTPN15)

1. **Inherent Risk:** **(MTPM17, A16)**
   - **a)** Inherent risk is the susceptibility of information resources controlled by the information system to material theft, destruction, disclosure, unauthorized modification, or other harms, assuming that there are no related internal controls.
   - **b)** Inherent risk is the measure of auditor's assessment that there may or may not be material vulnerabilities or gaps in the audit subject exposing it to high risk before considering the effectiveness of internal controls.
   - **c)** If the auditor concludes that there is a high likelihood of risk exposure, ignoring internal controls, the auditor would conclude that the inherent risk is high.
   - **d)** For example, inherent risk would be high in case of auditing internet banking in comparison to branch banking or inherent risk would be high if the audit subject is an off-site. ATM in an example of the same.

2. **Control Risk: (RTP M17, N15, MTPM17, F15)**

   a) Control risk is the risk that could occur in an audit area, and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system.

   b) Control risk is a measure of the auditor's assessment of the likelihood that risk exceeding a tolerable level and will not be prevented or detected by the client's internal control system.

   c) This assessment includes an assessment of whether a client's internal controls are effective for preventing or detecting gaps and the auditor's intention to make that assessment at a level below the maximum (100 percent) as a part of the audit plan.

3. **Detection Risk: (RTP M17, N15, MTP F15)**

   a) Detection risk is the risk that the IT auditor's substantive procedures will not detect an error which could be material, individually or in combination with other errors.

   b) For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high because logs for the whole period of the audit are not available at the time of the audit.

   c) The detection risk associated with lack of identification of disaster recovery plans is ordinarily low since existence is easily verified.

Q.No.20. Explain IS audit and audit evidence? (C)

a) According to SA-230, Audit Documentation refers to the record of audit procedures performed, relevant audit evidence obtained, and conclusions the auditor reached.

b) The objects of an auditor's working papers are to record and demonstrate the audit work from one year to another.

c) Evidences are also necessary for the following purposes:

   i) Means of controlling current audit work;

   ii) Evidence of audit work performed;

   iii) Schedules supporting or additional item in the accounts; and

   iv) Information about the business being audited, including the recent history.

d) In IS environment, the critical issue is that evidences are not available in physical form, but are in electronic form.

Q.No.21. Explain documentation by auditor? (C)

1. To be able to prepare proper report, auditor needs documented evidences. The problem of documents not available in physical form has been highlighted at many places.

2. Following is list of actions that auditor needs to take to address the problems:

   a) Use of special audit techniques, referred to as Computer Assisted Audit Techniques, for documenting evidences. Elaborated under this part, later on.

   b) Audit timing can be so planned that auditor is able to validate transactions as they occur in system.

   c) Auditor shall form his/her opinion based on above processes. As per (SA 200) "Overall Objectives of An Independent Auditor and Conduct of An Audit in Accordance With Standards of Auditing", any opinion formed by the auditor is subject to inherent limitations of an audit, which include

   d) The nature of financial reporting

- **e)** The nature of audit procedures
- **f)** The need for the audit to be conducted within a reasonable period of time and at a reasonable cost.
- **g)** The matter of difficulty, time, or cost involved is not in itself a valid basis for the auditor to omit an audit procedure for which there is no alternative or to be satisfied with audit evidence that is less than persuasive.
- **h)** Fraud, particularly fraud involving senior management or collusion.
- **i)** The existence and completeness of related party relationships and transactions.
- **j)** The occurrence of non-compliance with laws and regulations.
- **k)** Future events or conditions that may cause an entity to cease to continue as a going concern

Q.No.22. Write short notes on Provisions relating to Digital Evidences. (C)

As per Indian Evidence Act, 1872, "Evidence" means and includes:

- **i)** All statements, which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called oral evidence;
- **ii)** All documents produced for the inspection of the Court, such documents are called documentary evidence.

Documentary Evidence also includes 'Electronic Records'. The Information Technology Act, 2000 provides the legal recognition of electronic records and electronic signature through its various sections. The said Act also highlights Electronic Governance and accordingly, digital evidences are recognized legally.

Q.No.23. Explain concurrent or continuous audit? (B)

- **a)** Continuous auditing enables auditors to significantly reduce and perhaps to eliminate the time between occurrence of the client's events and the auditor's assurance services thereon.
- **b)** Errors in a computerized system are generated at high speeds and the cost to correct and rerun programs are high.
- **c)** If these errors can be detected and corrected at the point or closest to the point of their occurrence the impact thereof would be the least.
- **d)** Continuous auditing techniques use two bases for collecting audit evidence.
- **e)** One is the use of embedded modules in the system to collect, process, and print audit evidence and the other is special audit records used to store the audit evidence collected.

Q.No.24. Explain different audit tools? (B)

- **a)** Different types of continuous audit techniques may be used.
- **b)** Some modules for obtaining data, audit trails and evidences may be built into the programs. Audit software is available, which could be used for selecting and testing data.
- **c)** Many audit tools are also available. Some of them are:
  - **i)** Snapshot
  - **ii)** Integrated test facility (ITF)
  - **iii)** System control audit and review file (SCARF)
  - **iv)** Continuous and intermittent simulation (CIS)
  - **v)** Audit hooks

Q.No.25. Write short notes on snapshot techniques? (A) (PM, RTPN14, N13)

a) Tracing a transaction is a computerized system can be performed with the help of snapshots or extended records.

b) The snapshot software is built into the system at those points where material processing occurs which takes images of the flow of any transaction as it moves through the application.

c) These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction.

d) The main areas to dwell upon while involving such a system are

- **i)** to locate the snapshot points based on materiality of transactions
- **ii)** when the snapshot will be captured
- **iii)** The reporting system design and implementation to present data in a meaningful way.

Q.No.26. Write short notes on integrated test facility? (B) (MTP O15)

a) The ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness.

b) This test data would be included with the normal production data used as input to the application system.

c) In such cases the auditor has to decide what would be the method to be used to enter test data and the methodology for removal of the effects of the ITF transactions.

Q.No.27. Write short notes on methods of entering test data under ITF? (B)

a) Tagging:

- **i)** The transactions to be tested have to be tagged.
- **ii)** The application system has to be programmed to recognize the tagged transactions and have them invoke two updates, one to the application system master file record and one to the ITF dummy entity.
- **iii)** Auditors can also embed audit software modules in the application system programs to recognize transactions having certain characteristics as ITF transactions.
- **iv)** Tagging live transactions as ITF transactions has the advantages of ease of use and testing with transactions representative of normal system processing.
- **v)** However, use of live data could mean that the limiting conditions within the system are not tested and embedded modules may interfere with the production processing.

b) Use of Special data:

- **i)** The auditors may also use test data that is specially prepared.
- **ii)** Test transactions would be entered along with the production input into the application system.
- **iii)** In this approach the test data is likely to achieve more complete coverage of the execution paths in the application system to be tested than selected production data and the application system does not have to be modified to tag the ITF transactions and to treat them in a special way.
- **iv)** However, preparation of the test data could be time consuming and costly.

Q.NO.28. List the methods of removing the effects of ITF transactions from the system? (A)

The presence of ITF Transactions within an application system affects the output results obtained. So the effects of these transactions have to be removed.

a) The application system may be programmed to recognize ITF transactions and to ignore them in terms of any processing that might affect users.

b) Another method would be the removal of effects of ITF transactions by submitting additional inputs that reverse the effects of the ITF transactions. Another less used approach is to submit trivial entries so that the effects of the ITF transactions on the output are minimal.

c) The effects of the transactions are not really removed.

Q.NO.29. Write short notes on System Control Audit Review File (SCARF)? (A)
(RTP M16, M15, N14, N13, MTP S15)

a) The system control audit review file (SCARF) technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions.

b) The information collected is written onto a special audit file- the SCARF master files.

c) Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up.

d) In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities.

Q.No.30. What are the types of audit information that can be collected using SCARF? (OR) What do you understand by SCARF technique? Explain various types of information collected by using SCARF technique in brief. (OR) As an IS Auditor of a company, you want to use SCARF technique for collecting some information, which you want to utilize for discharging some of your functions Briefly describe the type of information that can be collected using SCARF technique. (A) (PM, RTP M16, N15, N14, N13)

Auditors might use SCARF to collect the following types of information:

a) **Application system errors:** SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.

b) **Policy and procedural variances:** Organizations have to adhere to the policies, Procedures and standards of the organization and the industry to which they belong.

c) **System exception:** SCARF can be used to monitor different types of application system exceptions. For example, salespersons might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.

d) **Statistical sample:** Some embedded audit routines might be statistical sampling routines, SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.

e) **Snapshots and extended records:** Snapshots and extended records can be written into the SCARF file and printed when required.

f) **Profiling data:** Auditors can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.

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

Q.No.31. Write short notes on continuous and intermittent simulation (CIS)? (B) (M14 - 4M)

a) CIS is a variation of the SCARF continuous audit technique.

b) This technique can be used to trap exceptions whenever the application system uses a database management system.

c) During application system processing, CIS executes in the following way:

- **i)** The database management system reads an application system transaction. It is passed to CIS.
- **ii)** CIS then determines whether it wants to examine the transaction further. If yes, the next steps are performed or otherwise it waits to receive further data from the database management system.
- **iii)** CIS replicates or simulates the application system processing.
- **iv)** Every update to the database that arises from processing the selected transaction will be checked by CIS to determine whether discrepancies exist between the results it produces and those the application system produces.
- **v)** Exceptions identified by CIS are written to exception log file.

d) The advantage of CIS is that it does not require modifications to the application system and yet provides an online auditing capability.

Q.No.32. What are the potential benefits of continuous auditing. (B)

Continuous auditing enables auditors to shift their focus from the traditional "transaction" audit to the "system and operations" audit. Continuous auditing has a number of potential benefits including:

a) Reducing the cost of the basic audit assignment by enabling auditors to test a larger sample (up to 100 percent) of client's transactions and examine data faster and more efficiently than the manual testing required when auditing around the computer;

b) Reducing the amount of time and costs auditors traditionally spend on manual examination of transactions

c) Increasing the quality of audits by allowing auditors to focus more on understanding a client's business and industry and its internal control structure; and

d) Specifying transaction selection criteria to choose transactions and perform both tests of controls and substantive tests throughout the year on an ongoing basis.

Q.No.33. Write the advantages and disadvantages of various concurrent audit techniques? (A)

Advantages of continuous audit techniques:

(PM, N15-5M, M14-6M, MTP M16, M16, N15, N15, M15, M14)

a) Timely, comprehensive and detailed auditing: Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analyzed rather than examining the inputs and the outputs only.

b) Surprise test capability: As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.

c) Information to system staff on meeting of objectives: Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.

d) **Training for new users:** Using the ITFs new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

e) **Disadvantages and limitations:** **(RTP M14, MTP M15, F14)**

 i) Auditors should be able to obtain resources required from the organization to support development, implementation, operation, and maintenance of continuous audit techniques.

 ii) Continuous audit techniques are more likely to be used if auditors are involved in the development work associated with a new application system.

 iii) Auditors need the knowledge and experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.

 iv) Continuous auditing techniques are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.

 v) Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.

Q.No.34. Write short notes on audit hooks? (B) (PM, RTP N14, N13, MTP M16)

a) There are audit routines that flag suspicious transactions.

b) For example, internal auditors at Insurance Company determined that their policyholder system was vulnerable to fraud every time a policyholder changed his or her name or address and then subsequently withdrew funds from the policy.

c) They devised a system of audit hooks to tag records with a name or address change.

d) The internal audit department will investigate these tagged records for detecting fraud.

e) When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur.

f) This approach of real-time notification may display a message on the auditor's terminal.

Q.No.35. What is an audit trail? In what ways does and audit trail safeguard both data and organization in an online environment? How do audit trails support security objectives? (OR) Discuss various ways in which audit trail can be used to support security objectives? (OR) What are the objectives if audit trail? (OR) The management of abc ltd wants to design a detective control mechanism for achieving security policy objective in a computerized environment. as an auditor explain, how audit trails can be used to support the security objectives? (A)
(PM, N16 - 6M, M – 10, N – 09, N – 05, RTP N16, M15, MTP A16, M16, N15, N15, M15)

Audit Trail or audit Log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function.

a) **Audit Trail Objectives:** Audit trails can be used to support security objectives in three ways:

b) **Detecting Unauthorized Access :**

 i) Detecting unauthorized access can occur in real time.

 ii) The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls.

 iii) A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by a virus or worm.

 iv) Depending upon how much activity is being logged and reviewed; real-time detection can impose a significant overhead on the operating system, which can degrade operational performance.

v) After-the-fact detection logs can be stored electronically and reviewed periodically or as needed.

vi) When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.

c) Reconstructing Events :

i) Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors.

ii) Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future.

iii) Audit trail analysis also plays an important role in accounting control.

iv) For example, by maintaining a record of all changes to count balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.

d) Personal Accountability :

i) Audit trails can be used to monitor user activity at the lowest level of detail.

ii) This capability is a preventive control that can be used to influence behavior.

iii) Individual are likely to violate an organization's security policy if they know that their actions are recorded in an audit log.

Q.NO.36. Write about audit and evaluation techniques for physical and environmental controls? (B)

Role of IS Auditor in Physical Access Controls:

1. Auditing physical access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls.
2. This involves the following:

a) **Risk Assessment:** The auditor must satisfy him/herself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures there from.

b) **Controls Assessment:** The auditor based on the risk profile evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks.

c) **Review of Documents:** It requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams.

3. **Audit of Environmental Controls:**

Related aspects are given as follows:

a) Role of Auditor in Environmental Controls:

i) Audit of environmental controls should form a critical part of every IS audit plan.

ii) The IS auditor should satisfy not only the effectiveness of various technical controls but also the overall controls safeguarding the business against environmental risks.

b) Audit Planning and Assessment:

As part of risk assessment,

- The risk profile should include the different kinds of environmental risks that the organization is exposed to; these may be natural and man-made threats.
- The controls assessment must ascertain that controls safeguard the organization against all acceptable risks including probable ones are in place.

- The security policy of the organization should be reviewed to assess policies and procedures that safeguard the organization against environmental risks.
- Building plans and wiring plans need to be reviewed to determine the appropriateness of location of IPF, review of surroundings, power and cable wiring etc.
- The IS auditor should interview relevant personnel to satisfy himself about employees' awareness of environmental threats and controls.
- Administrative procedures such as preventive maintenance plans and their implementation, incident reporting and handling procedures, inspection and testing plan and procedures need to be reviewed.

c) Audit of Environmental Controls: Refer Q.No. 37

d) Documentation:

i) As part of the audit procedures, the IS auditor should also document all findings.

ii) The working papers could include audit assessments, audit plans, audit procedures, questionnaires, interview sheets, inspection charts etc.

Q.No.37. As an IS Auditor, what are the environmental controls verified by you, while conducting physical inspections? (OR) What are the major aspects that should be thoroughly examined by an IS Auditor during the audit of Environmental Controls? Explain in brief. (A)
(PM, N15 - 6M, MTP M15)

Audit of environmental controls requires the Information Systems 'auditor to conduct physical inspections and observe practices. The Auditor should verify:

i) The IPF (Infrastructure Planning and Facilities) and the construction with regard to the type of materials used for construction

ii) The presence of water and smoke detectors, power supply arrangements to such devices, and testing logs

iii) The location of fire extinguishers, firefighting equipment and refilling date of fire extinguishers

iv) Emergency procedures, evacuation plans and marking of fire exits. There should be half - yearly Fire drill to test the preparedness

v) Documents for compliance with legal and regulatory requirements with regards to fire safety equipment, external inspection certificate and shortcomings pointed out by other inspectors/auditors

vi) Power sources and conduct tests to assure the quality of power, effectiveness of the power conditioning equipment, and generators. Also the power supply interruptions must be checked to test the effectiveness of the back-up power

vii) Environmental control equipment such as air-conditioning, dehumidifiers, heaters, ionizers etc.

viii) Compliant logs and maintenance logs to assess if MTBF (Mean Time Between Failures) and MTTR (Mean Time To Repair) are within acceptable levels; and

ix) Identify undesired activities such as smoking, consumption of eatables etc.

Q.No.38. Write about Documentation of Auditing of Environmental Controls (B)

Control Activities	Control Techniques	Audit Procedures
Safeguards against the risks of heating, ventilation and air conditioning systems.	Identify systems that provide constant temperature and humidity levels within the organization.	Review a heating, ventilation and air conditioning design to verify proper functioning within an organization

Control of radio emissions affect on computer systems	Evaluate electronic shielding to control radio emissions that affect the computer systems	Review any shielding strategies against interference or unauthorized access through emissions
Establish adequate interior security based on risk	Critical systems have emergency power supplies for alarm systems; monitoring devices, exit lighting, communication systems	Verify critical systems (alarm systems, monitoring devices, and entry control systems) have emergency power supplies.
Adequately protect against emerging threats, based on risk	Appropriate plans and controls such as shelter in place or for a potential CBR attack(chemical, biological and radioactive attack)	Interview officials, review planning documents and related test results.
Adequate environmental controls have been implemented	**i)** Fire detection and suppression devices are installed and working.(smoke detectors, fire extinguishers and sprinkle systems) **ii)** Redundancy exists in critical systems like, uninterrupted power supply, air cooling system, and backup generators	Interview managers and scrutinize that operations staff are aware of the locations of fire alarms, extinguishers, emergency power off switches, air ventilation apparatus and other emergency devices.
Staff have been trained to react to emergencies x	Operational and support personnel are trained and understand emergency procedures.	**i)** Interview security personnel to ensure their awareness and responsibilities. **ii)** Review training records and documentation. Determine the scope and adequacy of training.

Q.No.39. Discuss Managerial Controls and their Audit Trails. (B) (PM)

The Managerial controls and their Audit trails are as follows:

[what are the information systems management controls ?Explain?]

a) **Top Management and Information Systems Management Controls:** The major activities that senior management must perform are – Planning, Organizing, Controlling and Leading.

i) **Planning:** Auditors evaluate whether top management has formulated a high-quality information system's plan that is appropriate to the needs of an organization or not.

ii) **Organizing:** Auditors should be concerned about how well top management acquires and manage staff resources.

iii) **Leading:** Generally, the auditors examine variables that often indicate when motivation problems exist or suggest poor leadership – for example, staff turnover statistics, frequent failure of projects to meet their budget and absenteeism level to evaluate the leading function.

iv) **Controlling:** Auditors must evaluate whether top management's choice to the means of control over the users of Information System services is likely to be effective or not.

[Explain about system Development Management Controls]

b) **System Development Management Controls:** Three different types of audits may be conducted during system development process as follows:

i) **Concurrent Audit:** Auditors are members of the system development team. They assist the team in improving the quality of systems development for the specific system they are building and implementing.

ii) Post - implementation Audit: Auditors seek to help an organization learn from its experiences in the development of a specific application system. In addition, they might be evaluating whether the system needs to be scrapped, continued, or modified in some way.

iii) General Audit: Auditors evaluate systems development controls overall. They seek to determine whether they can reduce the extent of substantive testing needed to form an audit opinion about management's assertions relating to the financial statements for systems effectiveness and efficiency.

[What are the Programming Management Controls (OR) You are appointed as an auditor by the Top management of an enterprise to conduct an audit and evaluate the performance of various controls under managerial controls. Discuss the major concerns that you should address under different activities involved in programming management control Phase.]

c) **Programming Management Controls:** Some of the major concerns that an Auditor should address under different activities are as under: **(PM, M17 - 6M, RTP M17, MTP A16)**

i) Planning: They should evaluate whether the nature of and extent of planning are appropriate to the different types of software that are developed or acquired and how well the planning work is being undertaken.

ii) Control: They must evaluate whether the nature of an extent of control activities undertaken are appropriate for the different types of software that are developed or acquired. They must gather evidence on whether the control procedures are operating reliably.

iii) Design: Auditors should find out whether programmers use some type of systematic approach to design. Auditors can obtain evidence of the design practices used by undertaking interviews, observations, and reviews of documentation.

iv) Coding: Auditors should seek evidence on the level of care exercised by programming management in choosing a module implementation and integration strategy. Auditors determine whether programming management ensures that programmers follow structured programming conventions.

v) Testing: Auditors can use interviews, observations, and examination of documentation to evaluate how well unit testing is conducted. They are concerned primarily with the quality of integration testing work carried out by information systems professionals rather than end users.

d) **Operation and Maintenance:**

i) Auditors need to ensure effectively and timely reporting of maintenance needs occurs and maintenance is carried out in a well-controlled manner.

ii) Auditors should ensure that management has implemented a review system and assigned responsibility for monitoring the status of operational programs

e) **Data Resource Management Controls**:

i) Auditors should determine what controls are exercised to maintain data integrity.

ii) They might also interview database users to determine their level of awareness of these controls.

iii) Auditors might employ test data to evaluate whether access controls and update controls are working.

f) **Quality Assurance Management Controls:** **(RTP M16)**

i) Auditors might use interviews, observations and reviews of documentation to evaluate how well Quality Assurance (QA) personnel perform their monitoring role.

ii) Auditors might evaluate how well QA personnel make recommendations for improved standards or processes through interviews, observations, and reviews of documentation.

g) **Security Management Controls:** **(RTP M16)**

i) Auditors must evaluate whether security administrators are conducting ongoing, high-quality security reviews or not; check whether the organizations

ii) Audited have appropriate, high-quality disaster recovery plan in place; and check whether the organizations have opted for an appropriate insurance plan or not.

h) Operations Management Controls:

i) Auditors should pay concern to see whether the documentation is maintained securely and that it is issued only to authorized personnel.

ii) Auditors can use interviews, observations, and review of documentation to evaluate the activities of documentation librarians;

iii) How well operations management undertakes the capacity planning and performance monitoring function

iv) The reliability of outsourcing vendor controls; whether operations management is monitoring compliance with the outsourcing contract and

v) Whether operations management regularly assesses the financial viability of any outsourcing vendors that an organization uses.

Q.No.40. Describe how the application controls and their audit trail are categorized. (B) (PM)

The Application Controls are categorized as below:

Boundary Controls: Establishes interface between the user of the system and the system itself. The system must ensure that it has an authentic user. Users allowed using resources in restricted ways.

Input Controls: These are responsible for bringing both the data and instructions in to the information system. Input Controls are validation and error detection of data input into the system.

Communication Controls: These are responsible for controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, audit trail controls, and existence controls.

Processing Controls: These are responsible for computing, sorting, classifying and summarizing data. It maintains the chronology of events from the time data is received from input or communication systems to the time data is stored into the database or output as results.

Output Controls: These are the controls to provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared and routed to users.

Database Controls: These are responsible to provide functions to define, create, modify, delete and read data in an information system. It maintains procedural data-set of rules to perform operations on the data to help a manager to take decisions.

(What are the types of audit trail controls that should exist in each sub system with respect to application control)

Audit Trail Controls

The following two types of Audit Trail controls should exist in each application control

i) An Accounting Audit Trail to maintain a record of events within the subsystem; and

ii) An Operations Audit Trail to maintain a record of the resource consumption associated with each event in the subsystem.

Q.No.41. Discuss the chronology of events that occur when a user attempts to gain access to and employ systems resources in Boundary controls with respect to application controls. (B)

Boundary Controls: This maintains the chronology of events that occur when a user attempts to gain access to and employ systems resources.

i) Identity of the would-be user of the system

ii) Authentication information supplied

iii) Resources requested

iv) Action privileges requested

v) Terminal Identifier

vi) Start and Finish Time

vii) Number of Sign-on attempts

viii) Resources provided/denied and

Accounting Audit Trail: Action privileges allowed/denied.

Operations Audit Trail:

i) Resource usage from log-on to log-out time.
ii) Log of Resource consumption.

Q.No.42. Discuss the chronology of events from the time data and instructions are captured and entered into an application system in Input Controls with respect to application controls. (B)

This maintains the chronology of events from the time data and instructions are captured and entered into an application system until the time they are deemed valid and passed onto other subsystems within the application system.

Accounting Audit Trail

i) The identity of the person(organization) who was the source of the data

ii) The identity of the person(organization) who entered the data into the system

iii) The time and date when the data was captured

iv) The identifier of the physical device used to enter the data into the system

v) The account or record to be updated by the transaction

vi) The standing data to be updated by the transaction

vii) The details of the transaction and

viii) The number of the physical or logical batch to which the transaction belongs.

Operations Audit Trail

i) Time to key in a source document or an instrument at a terminal

ii) Number of read errors made by an optical scanning device

iii) Number of keying errors identified during verification

iv) Frequency with which an instruction in a command language is used; and

v) Time taken to invoke an instruction using a light pen versus a mouse.

Q.No.43. Discuss the chronology of events from the time a sender dispatches a message to the time a receiver obtains the message in Communication Controls with respect to application controls. (OR) Discuss the Accounting and Operations audit trails with respect to Communication controls. (B) (RTP N15)

This maintains a chronology of the events from the time a sender dispatches a message to the time a receiver obtains the message.

Accounting Audit Trail:

i) Unique identifier of the source/sink node

ii) Unique identifier of each node in the network that traverses the message. Unique identifier of the person or process authorizing dispatch of the message. Time and date at which the message was dispatched

iii) Time and date at which the message was received by the sink node.

iv) Time and date at which node in the network was traversed by the message; and

v) Message sequence number; and the image of the message received at each node traversed in the network.

Operations Audit Trail:

i) Number of messages that have traversed each link and each node.

ii) Queue lengths at each node; Number of errors occurring on each link or at each node. Number of retransmissions that have occurred across each link, Log of errors to identify locations and patterns of errors.

iii) Log of system restarts; and

iv) Message transit times between nodes and at nodes.

Q.No.44. Discuss the chronology of events from the time the time data is received from the input or communication subsystem to the time data is dispatched to the database in processing Controls with respect to application controls. (C)

The audit trail maintains the chronology of events from the time data is received from the input or communication subsystem to the time data is dispatched to the database, communication, or output subsystems.

Accounting Audit Trail:

i) To trace and replicate the processing performed on a data item.

ii) Triggered transactions to monitor input data entry, intermediate results and output data values.

Operations Audit Trail:

i) A comprehensive log on hardware consumption – CPU time used, secondary storage space used, and communication facilities used.

ii) A comprehensive log on software consumption – compilers used, subroutine libraries used, file management facilities used, and communication software used.

Q.No.45. Discuss the chronology of events that occur either to the database definition or the database itself in Data Base Controls with respect to application controls. (C)

Database Controls: The audit trail maintains the chronology of events that occur either to the database definition or the database itself

Accounting Audit Trail:

i) To attach a unique time stamp to all transactions,

ii) To attach before - images and after-images of the data item on which a transaction is applied to the audit trail; and

iii) Any modifications or corrections to audit trail transactions accommodating the changes that occur within an application system.

Operations Audit Trail: To maintain a chronology of resource consumption events that affects the database definition or the database

Q.No.46. Discuss the chronology of events that occur from the time the content of the output is determined until the time users complete their disposal of output in Output Controls with respect to application controls. (B) (N14 - 6M)

Output Controls: The audit trail maintains the chronology of events that occur from the time the content of the output is determined until the time users complete their disposal of output because it no longer should be retained.

Accounting Audit Trail:

i) What output was presented to users

ii) Who received the output

iii) When the output was received; and

iv) What actions were taken with the output?

Operations Audit Trail: To maintain the record of resources consumed – graphs, images, report pages, printing time and display rate to produce the various outputs.

Q.No.47. Write about audit of application security controls? (B)

1. The objective of this exercise is to establish whether the application security controls are operating effectively to protect the confidentiality, integrity and availability of information.
2. Application security is concerned with maintaining confidentiality, integrity and availability of the information.

a) Approach to Application Security Audit:

i) A layered approach is used based on the functions and approach of each layer.

ii) Layered approach is based on the activities being undertaken at various levels of management, namely supervisory, tactical and strategic.

iii) The approach is in line with management structure that follows top-down approach.

iv) For this, auditors need to have a clear understanding of the following.

- Business process for which the application has been designed;
- The source of data input to and output from the application;
- The various interfaces of the application under audit with other applications;
- The various methods that may be used to login to application
- The roles, descriptions, user profiles and user groups that can be created in an application
- The policy of the organization for user access and supporting standards.

v) There are various layers, which are:

- **Operational Layer:** The basic layer, where user access decision are generally put in place.
- **Tactical Layer:** This is a management layer, which includes supporting functions such as security administration, IT risk management and patch management.
- **Strategic Layer:** This is the layer used by TOP management. It includes the overall information security governance, security awareness, supporting information security policies and standards, and the overarching an application security perspective.

b) Understanding the Layers and Related Audit Issues

c) Operational Layer

Q.No.48. Discuss major audit issues of operational layer with reference to application security audit. (A) (PM, MTP M16)

The **operational layer** audit issues include:

1. **User Accounts and Access Rights:**
   - **a)** This includes defining unique user accounts and providing them access rights appropriate to their roles and responsibilities.
   - **b)** Auditor needs to always ensure the use of unique user IDs, and this need to be traced able to individual for who created.
2. **Password Controls:**
   - **a)** In general, password strength, password minimum length, password age, password non-repetition and automated lockout after three attempts should be set a s a minimum.
   - **b)** Auditor needs to check whether there are applications where password controls are weak.
   - **c)** In case such instances are found, then auditor may look for compensating controls against such issues.
3. **Segregation of duties:**
   - **a)** As frauds due to collusions / lack of segregations increase across the world, importance of segregation of duties also increases.
   - **b)** Segregation of duties is a basic internal control that prevents or detects errors and irregularities by assigning to separate individual's responsibility for initiating and recording transactions and custody of assets to separate individuals.

Q.No.49. Discuss major audit issues of Tactical layer with reference to application security audit. (B)

Tactical Layer: At the tactical layer, security administration is put in place.

a) Timely updates to user profiles, like creating/deleting and changing of user accounts.

b) Auditor needs to check that any change to user rights is a formal process including approval from manager of the employee.

i) IT Risk Management: This function is another important function performed, it includes the following activities:

- Assessing risk over key application controls;
- Conducting a regular security awareness programme on application user;
- Enabling application users to perform a self-assessment/complete compliance checklist questionnaire to determine the users' understanding about application security;
- Reviewing application patches before deployment and regularly monitoring critical application logs;
- Monitoring peripheral security in terms of updating antivirus software;

ii) Interface Security:

- This relates to application interfaced with another application in an organization.
- An auditor needs to understand that data flow to and from the application.

iii) Audit Logging and Monitoring:

- Regular monitoring the audit logs is required.
- The same is not possible for all transactions, so must be done on an exception reporting basis.

Q.No.50. Discuss major audit issues of Strategic layer with reference to application security audit. (B)

Strategic Layer:

a) At this layer, the top management takes action, in form of drawing up security policy, security training, security guideline and reporting.

b) The security policy should be supported and supplemented by detailed standards and guidelines.

c) These guidelines shall be used at the appropriate level of security at the application, database and operating system layers.

d) One of the key responsibilities of the IT risk management function is to promote ongoing security awareness to the organization's users.

e) Security metrics are now becoming popular to gauge the performance of the security management function.

f) Auditor needs to check whether all guidelines have been properly framed and are they capable of achieving the business objectives sought from the application under audit.

g) Based on the key controls described previously, the risk assessment of failure/weakness in the operating effectiveness of the key application security controls shall be made and acted upon by auditor.

THE END

7. INFORMATION TECHNOLOGY REGULATORY ISSUES

Q.NO. 1. What is IT Act and explain its objectives? (A) (PM)

The Information Technology Act was enacted on 17th May 2000 primarily to provide legal recognition for electronic transactions and facilitate e-commerce. it was the first information technology legislation introduced in India. The IT Act is based on Model law on e-commerce adopted by UNCITRAL (United Nations Commission on International Trade) of United Nations organization. The IT Act was amended by passing of the Information Technology (Amendment) Act 2008 (Effective from October 27, 2009).The amended Act casts responsibility on body corporate to protect sensitive personal information (Sec. 43A).

The Objectives of the Act are given as follows:

a) To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as “electronic commerce” in place of paper based methods of communication;

b) To give legal recognition to Digital signatures for authentication of any information or matter, which requires authentication under any law;

c) To facilitate electronic filing of documents with Government departments;

d) To facilitate electronic storage of data;

e) To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions;

f) To give legal recognition for keeping of books of accounts by banker’s in electronic form; and

g) To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker’s Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934.

(Explain the objectives of the Information Technology Act 2000.)

Q.No.2. Write Some of the key Issues of electronic information impacting enterprises and auditors? (B)

Some of the key Issues of electronic information impacting enterprises and auditors are:

a) **Authenticity:** How do we implement a system that ensures that transactions are genuine and authorized?

b) **Reliability:** How do we rely on the information, which does not have physical documents?

c) **Accessibility:** How do we gain access and authenticate this information, which is digital form?

A good understanding of the provisions of IT Act will provide answer to these issues.

Q.No.3. What are the Key Definitions in IT Act? (B)

Some of the key definitions are given below:

1. "**Access**" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;
2. "**Addressee**" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;
3. "**Adjudicating Officer**" means adjudicating officer appointed under subsection (1) of section 46;

4. **"Affixing Electronic Signature**" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Electronic Signature;

5. "**Appropriate Government**" means as respects any matter.

   i) enumerated in List II of the Seventh Schedule to the Constitution;

   ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;

6. "**Certifying Authority"** means a person who has been granted a license to issue a Electronic Signature Certificate under section 24;

7. "**Certification Practice Statement"** means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Electronic Signature Certificates;

8. "**Communication Device"** means Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image.

9. **"Computer**" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

10. "**Computer Network**" means the interconnection of one or more Computers or Computer systems or Communication device through-

    i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

    ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;

11. **"Computer Resource**" means computer, communication device, computer system, computer network, data, computer database or software;

12. "**Computer System**" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

13. **"Controller"** means the Controller of Certifying Authorities appointed under sub- section (7) of section 17;(n) "Cyber Appellate Tribunal" means the Cyber Appellate* Tribunal established under sub-section (1) of section 48.

14. "**Cyber Cafe**" means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public.

15. "**Cyber Security**" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

16. "**Data**" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

17. "**Digital Signature Certificate**" means a Digital Signature Certificate issued under sub-section (4) of section 35;

18. **"Electronic Gazette**" means official Gazette published in the electronic form;

19. "Electronic Record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

20. "**Electronic Signature**" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature

21. "**Electronic Signature Certificate"** means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate"

22. "**Function**", in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

23. "**Indian Computer Emergency Response Team**" means an agency established under sub-section (1) of section 70 B

24. "Information" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;

25. "**Intermediary**" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes;

26. "Law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be. Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, bye-laws and orders issued or made thereunder;

27. "License" means a license granted to a Certifying Authority under section 24;

28. "**Originator"** means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

29. "**Prescribed**" means prescribed by rules made under this Act;

30. "Private Key" means the key of a key pair used to create a digital signature;

31. "**Public Key"** means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

32. "**Secure System"** means computer hardware, software, and procedure that -: (a) are reasonably secure from unauthorized access and misuse; (b) provide a reasonable level of reliability and correct operation; (c) are reasonably suited to performing the intended functions; and (d) adhere to generally accepted security procedures;

33. "Security Procedure" means the security procedure prescribed under section 16 by the Central Government;

34. "**Subscriber"** means a person in whose name the Electronic Signature Certificate is issued;

35. "**Verify"** in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether

i) The initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

ii) The initial electronic record is retained intact or has been altered since such electronic record was .so affixed with the digital signature.

Q.No.4. What is Digital Signature? Explain? (A)

a) IT Act gives legal recognition to electronic records and digital signatures. It contains only Section 3. The digital signature is created in two distinct steps.

b) First the electronic record is converted into a message digest by using a mathematical function known as “hash function” which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record.

c) Any tampering with the contents of the electronic record will immediately invalidate the digital signature.

d) Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the public key corresponding to such private key.

e) This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature.

Q.No.5. Define the following terms with reference to Information Technology Act 2000:
(i) Digital signature
(ii) Electronic form
(iii) Key Pair
(iv) Asymmetric Crypto System (A) (PM)

i) Digital Signature: It means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.

ii) Electronic form: With reference to information, it means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated micro fiche or similar device.

iii) Key Pair: In an asymmetric cryptosystem, it means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.

iv) Asymmetric Crypto System: It is a system of secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

Q.No.6. Explain ‘Authentication of Electronic Records’ with reference to Section 3 of Information Technology Act 2000. (OR) (PM)
How does the Information Technology Act 2000 enable the authentication of records using digital signatures? (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.

Q.No.7. Explain ‘Electronic Signature’ with reference to Section 3A of Information Technology Act 2000. (A) (PM)

Electronic Signature [Section 3A]:

1. Notwithstanding anything contained in section 3, but subject to the provisions of subsection (2) a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which-

(a) is considered reliable; and

(b) may be specified in the Second Schedule

2. For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if-

a) The signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or , as the case may be, the authenticator and of no other person

b) The signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person

c) Any alteration to the electronic signature made after affixing such signature is detectable

d) Any alteration to the information made after its authentication by electronic signature is detectable; and

e) It fulfils such other conditions which may be prescribed.

3. The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated.

4. The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the Second Schedule

Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable.

5. Every notification issued under sub-section (4) shall be laid before each "House of Parliament”.

Q.No.8 Discuss the main provisions provided in Information Technology Act 2000 to facilitate e- Governance. (A)

E-Governance sections of chapter III 6, 7 and 8 are the main sections for provisions related to e-Governance provided in Information Technology Act 2000 to facilitate e-governance.

Section 6 lays down the foundation of electronic Governance. It provides that the filling of any form, application or other documents; creation, retention or preservation of records, issue or grant of any license or permit; receipt or payment in Government offices and its agencies may be done by means of electronic form. The appropriate Government has the power to prescribe the manner and format of the electronic records.

Section 7 provides legal sanctity and documents, records or information can be retained in electronic form thus removing the need to retain it in physical form. To safeguard the information even when technology changes, it provides that:

a) It should be possible to access and use the information later ;

b) Whenever the original format of the information is changed (e.g. due to technology) the new content should accurately represent the original information;

Section 8 provides that rules, regulations, orders, bye-laws and notifications required under any law to be published in the official Gazette can be published in the electronic gazette substituting the need for manual documents.

Q.No.9. Discuss the 'Legal Recognition of Electronic Records' in the light of Section4 of Information Technology Act 2000. (B)

[Section 4] Legal Recognition of Electronic Records

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is -

a) Rendered or made available in an electronic form; and

b) Accessible so as to be usable for a subsequent reference.

Q.No.10. Discuss the 'Legal recognition of Electronic Signatures' in the light of Section5 of Information Technology Act 2000. (B)

[Section 5] Legal recognition of Electronic Signatures: Where any law requires that any information or matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government.

Explanation – For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construe d accordingly.

Q.No.11. Discuss the 'Use of Electronic Records in Government and its agencies' in the light of Section6 of Information Technology Act 2000. (B) (PM)

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

a) Filing any form, application or other documents;

b) Creation, retention or preservation of records, issue or grant of any license or permit;

c) Receipt or payment of money in Government offices.

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

Q.No.12. Discuss the 'Delivery of services by Service Provider' in the light of Section6A of Information Technology Act 2000. (C)

[Section 6A] Delivery of services by Service Provider:

1. The appropriate Government may, for efficient delivery of services to the public through electronic means authorize, by order, any service provider to setup, maintain and upgrade the computerized facilities and perform such other services as it may specify by notification in the Official Gazette.

Explanation – For the purposes of this section, service provider so authorized includes any individual, private agency, private company, partnership firm, sole proprietor firm or any such other body or agency which has been granted permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector.

2. The appropriate Government may also authorize any service provider authorized under sub-section (1) to collect, retain and appropriate such service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service.
3. Subject to the provisions of sub-section (2), the appropriate Government may authorize the service providers to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate eservice charges by the service providers.
4. The appropriate Government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers under this section: Provided that the appropriate Government may specify different scale of service charges for different types of services.

Q.No.13. Discuss the 'Retention of Electronic Records' in the light of Section7 of Information Technology Act 2000. (A) (M16 - 4M, RTP N15, M15, MTP M17- 5M, N16 - M2 - 4M, M16 - M1 - 4M, N15 - M2 - 5M, M15 - M1- 6M)

[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, if -
   - **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

     provided that 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.

Q.No.14. Discuss the 'Audit of Documents, etc. maintained in Electronic form' in the light of Section7A of Information Technology Act 2000. (C)

Section 7A] Audit of Documents, etc. maintained in Electronic form: Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in electronic form.

Q.No.15. Discuss the 'Publication of rules, regulation, etc., in Electronic Gazette' in the light of Section8 of Information Technology Act 2000. (B)

[Section 8] Publication of rules, regulation, etc., in Electronic Gazette: Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

Provided that where any rule, regulation, order, bye-law, notification or any other matters published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

Q.No.16. Discuss the 'Sections 6, 7 and 8 not to confer right to insist document should be accepted in electronic form' in the light of Section9 of Information Technology Act 2000. (A)

[Section 9] Sections 6, 7 and 8 not to confer right to insist document should be accepted in electronic form

Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

Q.NO.17. Describe the 'Power to make rules by Central Government in respect of Electronic Signature' in the light of Section 10 of Information Technology Act 2000. (B) (PM)

Section 10 gives the Central Government following powers to make rules in respect of Electronic Signature -

a) Specify the type of Electronic audit of systems Signature

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

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

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

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

Q.No.18. Describe the 'Validity of contracts formed through electronic means' in the light of Section 10A of Information Technology Act 2000. (B)

[Section 10A] Validity of contracts formed through electronic means

Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

Q.No.19. Describe the 'Secure Electronic Records and Secure Electronic Signatures' in the light of Sections 14, 15 and 16 of Information Technology Act 2000. (C)

Secure Electronic Records and Secure Electronic Signatures

1. **[Section 14] Secure Electronic Record:** Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.
2. **[Section 15] Secure Electronic Signature:** An electronic signature shall be deemed to be a secure electronic signature if -

a) The signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and

b) The signature creation data was stored and affixed in such exclusive manner as may be prescribed.

Explanation – In case of Digital signature, the "signature creation data" means the private key of the subscriber.

3. **[Section 16] Security Procedures and Practices:** The Central Government may, for the purposes of sections 14 and 15, prescribe the security procedures and practices:

   Provided that in prescribing such security procedures and practices, the Central Government shall have regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.

Q.No.20. Discuss 'Penalty and Compensation for damage to computer, computer system, etc.' under Section 43 of Information Technology Act 2000. (C)

[Section 43] Penalty and Compensation for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is in -charge of a computer, computer system or computer network, -

a) Accesses or secures access to such computer, computer system or computer network or computer resource;

b) Downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

d) Damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

e) Disrupts or causes disruption of any computer, computer system or computer network;

f) Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

g) Provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;

h) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;

i) Destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, he shall be liable to pay damages by way of compensation to the person so affected.

Q.No.21. What are different purposes of section 43? (C)

Purposes of section 43:

1. "**Computer contaminant**" means any set of computer instructions that are designed -

   a) To modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

   b) By any means to usurp the normal operation of the computer, computer system, or computer network;

2. "**Computer database**" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;
3. "**Computer virus**" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;
4. "**Damage**" means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means.
5. "**Computer source code**" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Q.No.22. Discuss 'Compensation for failure to protect data' under Section 43A of Information Technology Act 2000. (C)

[Section 43A] Compensation for failure to protect data: Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected.

Explanation-

For the purposes of this section -

a) "**Body Corporate**" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;
b) "**Reasonable Security Practices and Procedures**" means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law.
c) "**Sensitive Personal Data or Information**" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

Q.No.23. Discuss 'Power Penalty for failure to furnish information return, etc.' under Section 44 of Information Technology Act 2000. (B) (RTP M17)

[Section 44] Penalty for failure to furnish information return, etc.

If any person who is required under this Act or any rules or regulations made thereunder to -

a) Furnish any document, return or report to the Controller or the Certifying Authority, fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;
b) File any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;
c) Maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

Q.No.24. Discuss 'Residuary Penalty' under Section 45 of Information Technology Act 2000. (C)

[Section 45] Residuary Penalty: Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

Q.No.25. Describe the 'Tampering with Computer Source Documents' in the light of Section 65 of Information Technology Act 2000. (C) (PM)

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation - For the purposes of this section, "Computer Source Code" means the listing of programme, computer commands, design and layout and program analysis of computer resource in any form.

Q.No.26. Discuss 'Computer Related Offences' under Section 66 of Information Technology Act 2000. (C)

[Section 66] Computer Related Offences: If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Explanation -

For the purpose of this section,-

a) The word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code (45 of 1860);

b) The word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860).

Q.No.27. Discuss 'Punishment for sending offensive messages through communication service, etc.' under Section 66A of Information Technology Act 2000. (C)

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

A Division bench of Supreme Court decided on 24th March, 2015 in Shreya Singhal v. Union of India to struck down section 66A of Information Technology Act, 2000 as unconstitutional, as it is violative of Article 19(1)(a) related to freedom of speech and expressions. Now comments on social networking sites will not be offensive unless they come under the provisions of the Indian Penal Code, 1860.

Q.No.28. Discuss 'Punishment for dishonestly receiving stolen computer resource or communication device' under Section 66B of Information Technology Act 2000. (C)

[Section 66B] Punishment for dishonestly receiving stolen computer resource or communication device: Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Q.No.29. (a) Mr. A has received some information about Mr. B on his cell phone. He knows that this information has been stolen by the sender. He not only retained this information but also sends it to Mr. B and his friends. Because of this act, Mr. B is annoyed and his life is in danger.
(b) Mr. B seeks your advice, under what sections of Information Technology (Amendment) Act, 2008; he can file an FIR with police against Mr. A? Advise Mr. B detailing the applicable sections of the Act. (B) (RTP M15)

1. If Mr. B wants to file an FIR against Mr. A, then he may file the same under the following

Section of Information Technology (Amendment) Act, 2008:

a) **Section 66A:** Punishment for sending offensive messages through communication service, etc.; and

b) **Section 66B:** Punishment for dishonestly receiving stolen computer resource or communication device.

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

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

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

a) Any information that is grossly offensive or has menacing character; or

b) Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently by making use of such computer resource or a communication device,

c) Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.

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

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

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

Q.No.30. Discuss 'Punishment for identity theft' under Section 66C of Information Technology Act 2000. (C)

[Section 66C] Punishment for identity theft
Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Q.No.31. Discuss 'Punishment for cheating by personation by using computer resource' under Section 66D of Information Technology Act 2000. (C)

[Section 66D] Punishment for cheating by personation by using computer resource
Whoever, by means of any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Q.No.32 (a) Mr. X is a Government servant whose profile is to maintain the records of all the employees of the organization. The intruder Mr. Z personates as the senior member of the organization's management team and retrieved the critical data from Mr. X on mobile phone. State the liabilities of Mr. Z under the given situation.
(b) Also, state the liability of Mr. X in the above situation. (B) (RTP M16)

(a) Mr. Z is liable under Section 66D of IT Act, 2000. Section 66D deals with the punishment for cheating by personation by using computer resource. According to the provision, whoever, by means of any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

(b) Mr. X is not liable as he was convinced that he is providing the data to the rightful person. So providing the information will utmost good faith will not make him liable.

Q.No.33 Discuss 'Punishment for violation of privacy' under Section 66E of Information Technology Act 2000. (C)

[Section 66E] Punishment for violation of privacy
Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.
Explanation -
For the purposes of this section -

a) "**Transmit**" means to electronically send a visual image with the intent that it be viewed by a person or persons;

b) "**Capture**", with respect to an image, means to videotape, photograph, film or record by any means;

c) "**Private area**" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

d) "**Publishes**" means reproduction in the printed or electronic form and making it available for public;

e) "**Under circumstances violating privacy**" means circumstances in which a person can have a reasonable expectation that-

   i) He or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

   ii) Any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

Q.No.34. Discuss 'Punishment for cyber terrorism' under Section 66F of Information Technology Act 2000. (B)

[Section 66F] Punishment for cyber terrorism

A) Whoever -

1. with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

a) Denying or cause the denial of access to any person authorized to access computer resource; or

b) Attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

c) Introducing or causing to introduce any computer contaminant,

2. And by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

B) Knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations;

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

Q.No.35. Discuss 'Punishment for publishing or transmitting obscene material in electronic form' under Section 67 of Information Technology Act 2000. (C)

[Section 67] Punishment for publishing or transmitting obscene material in electronic form: Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Q.No.36. Discuss 'Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form' under Section 67A of Information Technology Act 2000. (C)

[Section 67A] Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form: Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Q.No.37. Discuss 'Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form' under Section 67B of Information Technology Act 2000. (B)

[Section 67B] Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form

Whoever, -

a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

d) facilitates abusing children online; or

e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form –

i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

ii) Which is kept or used for bona fide heritage or religious purposes.

Explanation - For the purposes of this section, "children" means a person who has not completed the age of 18 years.

Q.No.38. Discuss 'Preservation and Retention of information by intermediaries' under Section 67C of Information Technology Act 2000. (B)

[Section 67C] Preservation and Retention of information by intermediaries:

1. Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.
2. Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Q.No.39. Discuss 'Power of the Controller to give directions' under Section 68 of Information Technology Act 2000. (OR) Explain the power of Controller to give directions under Section 68 of the Information Technology (Amendment) Act, 2008. (B) (PM, RTP M15)

Certifying Authorities create digital signatures and provide them to subscribers. People use and rely on Digital signatures for carrying on electronic commerce. If signatures are compromised, or if there are insufficient safeguards over their creation or provision, the system will be weakened. To prevent this, the Controller is provided following powers:

[Section 68] Power of Controller to give directions

1. The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.
2. Any person who intentionally or knowingly fails to comply with any order under subsection (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or with both.

Q.No.40. Discuss 'Power to issue directions for interception or monitoring or decryption of any information in any computer resource' under Section 69 of Information Technology Act 2000. (C) (PM)

Section 69 gives powers to Central & State Governments to issue directions empowering a Government agency to intercept, monitor or decrypt any information through or in any computer if it is for important purposes as specified in the section. These include:

1. Where the Central Government or a State Government or any of its officers specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States.
2. The Procedure and safeguards over such interception or monitoring or decryption, shall be prescribed.
3. The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by the agency, extend all facilities and technical assistance to -
   a) Provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or
   b) Intercept, monitor, or decrypt the information, as the case may be; or
   c) Provide information stored in computer resource.
4. The subscriber or intermediary or any person who fails to assist such agency shall be punished with imprisonment up to seven years and fine.

Q.No.41. Discuss 'Power to issue directions for blocking for public access of any information through any computer resource' under Section 69A of Information Technology Act 2000. (C) (RTP N15, MTP - M2 - 6M)

[Section 69A] Power to issue directions for blocking for public access of any information through any computer resource

1. Where the Central Government or any of its officers specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign states.
2. The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.
3. The intermediary who fails to comply with the directio itiln issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

Q.No.42. Discuss 'Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security' under Section 69B of Information Technology Act 2000. (B)

[Section 69B] Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security

1. The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.
2. The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorised under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.
3. The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.
4. Any intermediary who intentionally or knowingly contravenes the provisions of subsection shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

   Explanation:

   For the purposes of this section, -

   a) "**Computer Contaminant**" shall have the meaning assigned to it in section 43;

   b) "**Traffic Data**" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

Q.No.43. Discuss 'Protected system' under Section 70 of Information Technology Act 2000. (B) (M17 - 4M)

[Section 70] Protected system

1. The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

   Explanation -

   For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.
2. The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1).
3. Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.
4. The Central Government shall prescribe the information security practices and procedures for such protected system.

Q.No.44. Discuss 'National nodal agency' under Section 70 of Information Technology Act 2000. (C)

[Section 70A] National nodal agency

1. The Central Government may, by notification published in the official Gazette, designate any organization of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.
2. The national nodal agency designated under sub-section (1) shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.
3. The manner of performing functions and duties of the agency referred to in sub –section (1) shall be such as may be prescribed.

Q.No.45. Discuss 'Indian Computer Emergency Response Team to serve as national agency for incident response' under Section 70B of Information Technology Act 2000. (C) (N16 - 4M)

[Section 70B] Indian Computer Emergency Response Team to serve as national agency for incident response

1. The Central Government shall, by notification in the Official Gazette, appoint an agency of the government to be called the Indian Computer Emergency Response Team.
2. The Central Government shall provide the agency referred to in sub-section (1) with a Director-General and such other officers and employees as may be prescribed.
3. The salary and allowances and terms and conditions of the Director -General and other officers and employees shall be such as may be prescribed.
4. The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of Cyber Security, -
   - **a)** Collection, analysis and dissemination of information on cyber incidents;
   - **b)** Forecast and alerts of cyber security incidents;
   - **c)** Emergency measures for handling cyber security incidents;
   - **d)** Coordination of cyber incidents response activities;
   - **e)** Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
   - **f)** Such other functions relating to cyber security as may be prescribed.
5. The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.
6. For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person.
7. Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.
8. No Court shall take cognizance of any offence under this section, except on a complaint made by an officer authorized in this behalf by the agency referred to in sub-section (1).

Q.No.46. Discuss 'Penalty for misrepresentation' under Section 71 of Information Technology Act 2000. (C)

[Section 71] Penalty for misrepresentation: Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Q.No.47. Discuss 'Penalty for breach of confidentiality and privacy' under Section 72 of Information Technology Act 2000. (B) (RTP N16)

[Section 72] Penalty for breach of confidentiality and privacy: Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Q.No.48. Discuss 'Punishment for Disclosure of information in breach of lawful contract' Under Section 72A of Information Technology Act 2000. (C)

[Section 72A] Punishment for Disclosure of information in breach of lawful contract: Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

Q.No.49. Discuss 'Penalty for publishing Electronic Signature Certificate false in certain particulars' under Section 73 of Information Technology Act 2000. (B) (PM)

[Section 73] Penalty for publishing Electronic Signature Certificate false in certain particulars

1. No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that -
   - **a)** The Certifying Authority listed in the certificate has not issued it; or
   - **b)** The subscriber listed in the certificate has not accepted it; or
   - **c)** The certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.
2. Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Q.No.50. Discuss 'Publication for fraudulent purpose' under Section 74 of Information Technology Act 2000. (C)

[Section 74] Publication for fraudulent purpose: Whoever knowingly creates, publishes or otherwise makes available an Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Q.No.51. Discuss 'Act to apply for offences or contraventions committed outside India' under Section 75 of Information Technology Act 2000. (C)

[Section 75] Act to apply for offences or contraventions committed outside India:

1. Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.
2. For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Q.No.52. Discuss 'Power Confiscation' under Section 76 of Information Technology Act 2000. (C)

[Section 76] Confiscation

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation:

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

Enterprises need to take steps to ensure compliance with cyber laws. Some key steps for ensuring compliance are given below:

a) Designate a Cyber Law Compliance Officer as required.

b) Conduct regular training of relevant employees on Cyber Law Compliance.

c) Implement strict procedures in HR policy for non-compliance.

d) Implement authentication procedures as suggested in law.

e) Implement policy and procedures for data retention as suggested.

f) Identify and initiate safeguard requirements as applicable under various provisions of the Act such as: Sections 43A, 69, 69A, 69B, etc.

g) Implement applicable standards of data privacy on collection, retention, access, deletion etc.

Q.No.53. Discuss 'Exemption from liability of intermediary in certain cases' under Section 79 of Information Technology Act 2000. (C)

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

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

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

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

b) the intermediary does not -

i) initiate the transmission,

ii) select the receiver of the transmission, and

iii) select or modify the information contained in the transmission

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

3. The provisions of sub-section (1) shall not apply if -

a) the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act;

b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation - For the purposes of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

Q.No.54. Discuss 'Central Government to notify Examiner of Electronic Evidence' under Section of Information Technology Act 2000. (C)

[Section 79A] Central Government to notify Examiner of Electronic Evidence: The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Explanation - For the purposes of this section, "electronic form evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines.

Q.NO.55. Mr. A has hacked into Defence Information Systems with an intention to steal classified information that threatens the security and sovereignty of India. He has used the services of a local cafe, 'Cyber Net' for this purpose. The owner of 'Cyber Net' tries to stop Mr. A but is threatened by Mr. A. Hence the owner of 'Cyber Net' does not disclose A's activities to anyone.
Mr. A is caught by the Vigilance Officers of the department.
(i) Is Mr. A punishable for his activities?
(ii) Is the intermediary, 'Cyber Net' liable?
Please discuss the liabilities enunciated under the relevant sections of the Information Technology Act, 2000 in the above two cases. (B) (PM, M15 - 6M)

1. Yes, Mr. A is punishable for his activities under the Section 66F.

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

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

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

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

2. Yes, Intermediary 'Cyber Net' is liable under the Section 79.

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

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

b) He provisions of sub-section (1) shall apply if -

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

c) The intermediary does not-

i) Initiate the transmission,

ii) Select the receiver of the transmission, and

iii) Select or modify the information contained in the transmission

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

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

Q.No.56. Discuss 'Power of police officer and other officers to enter, search, etc' under Section 80 of Information Technology Act 2000. (C)

[Section 80] Power of police officer and other officers to enter, search, etc.

1. Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Inspector or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.

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

2. Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer -in-charge of a police station.

3. The provisions of the Code of Criminal Procedure, 1973 (2 of 1974)shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

Q.No.57. Discuss 'Act to have Overriding effect cheque' under Section 81 of Information Technology Act 2000. (C)

[Section 81] Act to have Overriding effect: The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force. Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act 1957 or the Patents Act, 1970.

Q.No.58. Discuss 'Application of the Act to electronic cheque and truncated cheque' under Section 81A of Information Technology Act 2000. (C)

[Section 81A] Application of the Act to electronic cheque and truncated cheque

1. The provisions of this Act, for the time being in force, shall apply to, or in relation to, electronic cheques and the truncated cheques subject to such modifications and amendments as may be necessary for carrying out the purposes of the Negotiable Instruments Act, 1881 (26 of 1881) by the Central Government, in consultation with the Reserve Bank of India, by notification in the Official Gazette.

2. Every notification made by the Central Government under subsection (1) shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both houses agree in making any modification in the notification or both houses agree that the notification should not be made, the notification shall thereafter have effect only in such modified form or be of no effect, as the case may be.

   Explanation - For the purpose of this Act, the expression "electronic cheque" and "truncated cheque" shall have the same meaning as assigned to them in section 6 of the Negotiable Instruments Act 1881 (26 of 1881).

Q.No.59. Discuss 'Punishment for abetment of offence' under Section 84B of Information Technology Act 2000. (C)

[Section 84B] Punishment for abetment of offence: Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

Explanation – An Act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

Q.No.60. Discuss 'Punishment for attempt to commit offences' under Section 84C of Information Technology Act 2000. (C)

[Section 84C] Punishment for attempt to commit offences: Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.

Q.No.61. Discuss 'Offences by Companies' under Section 85 of Information Technology Act 2000. (C)

[Section 85] Offences by Companies

1. Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a Company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

   provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

2. Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

   Explanation –

   For the purposes of this section, -

   a) "**Company**" means any Body Corporate and includes a Firm or other Association of individuals; and

   b) "**Director**", in relation to a firm, means a partner in the firm.

Q.No.62. what are the Requirements of IRDA for System Controls & Audit? (A)

The **Insurance Regulatory and Development Authority of India (IRDA)** is the apex body overseeing the insurance business in India. It protects the interests of the policyholders, regulates, promotes and ensures orderly growth of the insurance in India.
Information System Audit aims at providing assurance in respect of Confidentiality, Availability and Integrity for Information systems. It focuses on compliance with laws and regulations, which are given as follows:

1. **System Audit:** These are as follows:

   a) All insurers shall have their systems and process audited at least once in three years by a CA firm.

   b) In doing so, the current internal or concurrent or statutory auditor is not eligible for appointment.

   c) CA firm must be having a minimum of 3-4 years experience of IT systems of banks or mutual funds or insurance companies.

2. **Preliminaries:** **(N16 – 5M)**

   Before proceeding with the audit, the auditor is expected to obtain the following information at the audit location:

   a) Location(s) from where Investment activity is conducted.

   b) IT Applications used to manage the Insurer's Investment Portfolio.

   c) Obtain the system layout of the IT and network infrastructure including: Server details, database details, type of network connectivity, firewalls other facilities/ utilities (describe).

d) Are systems and applications hosted at a central location or hosted at different office?

e) Previous Audit reports and open issues / details of unresolved issues from:

i) Internal Audit,

ii) Statutory Audit, and

iii) IRDA Inspection / Audit.

f) Internal circulars and guidelines of the Insurer.

g) Standard Operating Procedures (SOP).

h) List of new Products/funds introduced during the period under review along with IRDA approvals for the same.

i) Scrip wise lists of all investments, fund wise, classified as per IRDA Guidelines, held on date.

j) IRDA Correspondence files, circulars and notifications issued by IRDA.

k) IT Security Policy.

l) Business Continuity Plans.

m) Network Security Reports pertaining to IT Assets.

3. **System Controls:** These are as follows:

a) There should be Electronic transfer of Data without manual intervention. All Systems should be seamlessly integrated. Audit Trail required at every Data entry point. Procedures for reviewing and maintaining audit trail should be implemented.

The auditor should comment on the audit trail maintained in the system for various activities. The auditor should review the Front Office Systems (FOS), MOS (Mid Office Systems) and BOS (Back Office Systems) and confirm that the system maintains audit trail for data entry, authorization, cancellation and any subsequent modifications.

b) Further, the auditor shall also ascertain that the system has separate logins for each user and maintains trail of every transaction with respect to login ID, date and time for each data entry, authorization and modifications.

Q.No.63. What are the Requirements of RBI for System Controls & Audit? (A)

The **Reserve Bank of India (RBI)** is India's central banking institution, which formulates the monetary policy with regard to the Indian rupee. The Bank was constituted for the need of following:

a) To regulate the issue of banknotes,

b) To maintain reserves with a view to securing monetary stability, and

c) To operate the credit and currency system of the country to its advantage.

Primarily, RBI suggests that senior management and regulators need an assurance on the effectiveness of internal controls implemented and expect the IS Audit to provide an independent and objective view of the extent to which the IT related risks are managed. Sample areas of review covered by IS Audit assignments are given here.

1. **System Controls:** These are given as follows: **(M16 – 5M)**

a) Duties of system programmer/designer should not be assigned to persons operating the system and there should be separate persons dedicated to system programming/design. System person would only make modifications/improvements to programs and the operating persons would only use such programs without having the right to make any modifications.

b) Board of Directors and senior management are responsible for ensuring that an institution's system of internal controls operates effectively.

c) There should also be annual review of IS Audit Policy or Charter to ensure its continued relevance and effectiveness.

d) With a view to provide assurance to bank's management and regulators, banks are required to conduct a quality assurance, at least once every three years, on the banks Internal Audit including IS Audit to validate the approach and practices adopted by them in the discharge of its responsibilities as laid out in the Audit Charter/Audit Policy.

2. **System Audit:** Relevant points are given as follows:

a) In this regard, banks require a separate IS Audit function within an Internal Audit department led by an IS Audit Head reporting to the Head of Internal Audit or Chief Audit Executive (CAE). The personnel needs to assume overall responsibility and accountability of IS Audit functions. Where the bank leverages external resources for conducting IS Audit on areas where skills are lacking, the responsibility and accountability for such external IS Audits still remain with the IS Audit Head and CAE.

b) Because the IS Audit is an integral part of the Internal Auditors, auditors will also be required to be independent, competent and exercise due professional care.

c) The IS Audit should be independent of the auditee, both in attitude and appearance. The Audit Charter or Policy, or engagement letter (in case of external professional service provider), should address independence and accountability of the audit function.

d) Additionally, to ensure independence for the IS Auditors, Banks should make sure that:

i) Auditors have access to information and applications, and

ii) Auditors have the right to conduct independent data inspection and analysis.

e) IS Audits should also cover branches, with focus on large and medium branches, in areas such as control of passwords, user ids, operating system security, antimalware, maker-checker, segregation of duties, physical security, review of exception reports or audit trails, BCP policy and or testing.

f) IS Auditors should review the following additional areas that are critical and high risk such as:

i) IT Governance and information security governance structures and practices implemented by the Bank.

ii) Testing the controls on new development systems before implementing them in live environment.

Q.No.64. What is SEBI? What are the Requirements of SEBI for System Controls & Audit? (A)

The **Securities and Exchange Board of India (SEBI)** is the regulator for the securities market in India. SEBI has to be responsive to the needs of three groups, which constitute the market:

a) The issuers of securities,

b) The investors, and

c) The market intermediaries.

Mandatory audits of systems and processes bring transparency in the complex workings of SEBI, prove integrity of the transactions and build confidence among the stakeholders.

1. **Systems Audit:** SEBI (Securities and Exchange Board of India) mandated that exchanges shall conduct an annual system audit by a reputed independent auditor. **(PM, RTP M16)**

a) The Audit shall be conducted according to the Norms, Terms of References (TOR) and Guidelines issued by SEBI.

b) Stock Exchange/Depository (Auditee) may negotiate and the board of the Stock Exchange / Depository shall appoint the Auditors based on the prescribed Auditor Selection Norms and TOR. The Auditors can perform a maximum of 3 successive audits.

The proposal from Auditor must be submitted to SEBI for records.

c) Audit schedule shall be submitted to SEBI at-least 2 months in advance, along with scope of current audit & previous audit.

d) The scope of the Audit may be extended by SEBI, considering the changes which have taken place during last year or post previous audit report.

e) Audit has to be conducted and the Audit report be submitted to the Auditee. The report should have specific compliance/non-compliance issues, observations for minor deviations as well as qualitative comments for scope for improvement. The report should also take previous audit reports in consideration and cover any open items therein.

f) The Auditee management provides their comment about the Non-Conformities (NCs) and observations. For each NC, specific time-bound (within 3 months) corrective action must be taken and reported to SEBI. The auditor should indicate if a follow-on audit is required to review the status of NCs. The report along with Management Comments shall be submitted to SEBI within 1 month of completion of the audit.

(**ABC Ltd. is a security market intermediary, providing depository services. Briefly explain the relevant requirements with respect to annual systems audit mandated by SEBI in this regard.)**

2. **Audit Report Norms:** These are given as follows: **(RTP M17, N16)**

a) The Systems Audit Reports and Compliance Status should be placed before the Governing Board of the Stock Exchanges/Depositories and the system audit report along with comments of Stock Exchanges / Depositories should be communicated to SEBI.

b) The Audit report should have explicit coverage of each Major Area mentioned in the TOR, indicating any Nonconformity (NCs) or Observations (or lack of it). For each section, auditors should also provide qualitative input about ways to improve the process, based upon the best practices observed.

3. **Auditor Selection Norms:** There are various norms for selection of Auditors, which are given as follows: **(PM, M15 – 4M, MTP – M2 – 6M)**

a) Auditor must have minimum 3 years of experience in IT audit of Securities Industry participants e.g. stock exchanges, clearing houses, depositories etc. The audit experience should have covered all the major Areas mentioned under SEBI's Audit Terms of Reference (TOR).

b) The Auditor must have experience in/direct access to experienced resources in the areas covered under TOR. It is recommended that resources employed shall have relevant industry recognized certifications e.g. CISA (Certified Information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium (ISC)².

c) The Auditor should have IT audit/governance frameworks and processes conforming to industry leading practices like COBIT.

d) The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the Exchange/Depository. He should not have been engaged over the last three years in any consulting engagement with any departments/units of the entity being audited.

e) The Auditor may not have any cases pending against its previous auditees, which fall under SEBI's jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.

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

4. **System Controls:** These are given as follows:
   - **a)** Further, along with the audit report, Stock Exchanges/Depositories are advised to submit a declaration from the MD/CEO certifying the security and integrity of their IT Systems.
   - **b)** A proper audit trail for upload/modifications/downloads of KYC data to be maintained Department of Electronics & IT, Ministry of Communication and IT, Government of India, maintains a panel of systems auditors, which are used by government enterprises for getting system audit done. This provides information on scope of different types of systems audit which is used as reference by auditee firms for getting systems audit done.

Q.NO.65. What is Cyber Forensic and Cyber Fraud Investigation? Explain? (B)

a) Cyber forensics is one of the latest scientific techniques that have emerged due to the effect of increasing computer frauds. To understand the term better, an understanding of the independent words will be useful.

b) Cyber, means on 'The Net' that is online. Forensics is a scientific method of investigation and analysis techniques to gather, process, interpret, and to use evidence to provide a conclusive description of activities in a way that is suitable for presentation in a court of law.

c) Considering 'Cyber' and 'Investigation' together will lead us to conclude that 'Cyber Investigation' is an investigation method gathering digital evidences to be produced in court of law.

d) To ensure that the above objectives are achieved, the experts of the fields use standard processes and globally accept methods so that same result shall always be obtained if the same evidences are checked by another expert, that is why cyber forensic experts follow standard methods for investigation.

e) Increasing frauds across the cyber space, the sheer size, speed and value of the frauds has surprised the law keeper's. Fraudsters are always on the look-out to misuse any loop hole or weaknesses in the computer systems.

f) Cyber Frauds across the world as withdrawal of an amount equal to USD45 Million, by using ATM cards of banks, sent shock waves across the IT security agencies

Q.NO.66. Write something about Security Standards? (C)

Information security is essential in the day-to-day operations of enterprises. Breaches in information security can lead to a substantial impact within the enterprise through, for example, financial or operational damages.

The ever-increasing need for the enterprise to implement security is highlighted here:

a) Maintain information risk at an acceptable level and to protect information against unauthorised disclosure, unauthorised or inadvertent modifications, and possible intrusions;

b) Ensure that services and systems are continuously available to internal and external stakeholders, leading to user satisfaction with IT engagement and services;

c) Comply with the growing number of relevant laws and regulations as well as contractual requirements and internal policies on information and systems security and protection, and provide transparency on the level of compliance; and

d) Achieve all of the above while containing the cost of IT services and technology protection.

Considering the importance of security, Government of India recently published the National Cyber Security Policy 2013 with the vision: **"To build a secure and resilient cyberspace for citizens, business and Government"** and the mission **"To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people processes, technology and cooperation".**

Q.No.67. What is the vision of National Cyber Security Policy 2013? Also explain its major objectives. (A) (PM)

Vision of the National Cyber Security Policy 2013 is: "To build a secure and resilient cyberspace for citizens, business and Government" and the mission "To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people processes, technology and cooperation".

Major objectives of this policy are given as follows:

a) To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy;

b) To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology, & people);

c) To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem;

d) To enhance and create National and Sectorial level 24*7 mechanisms for obtaining strategic information regarding threats of ICT infrastructure creating scenarios for response, resolution and crisis management through effective predicative, protective, response and recovery actions;

e) To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24*7 National Critical Information Infrastructure Protection Center(NCIIPC) and mandating security practices related to the design, acquisition, development and operation of information resources;

f) To improve visibility of the integrity of ICT products & services and establishing infrastructure for testing & validation of security of such products;

g) To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training;

h) To provide fiscal benefits to businesses for adoption of standard security practices and processes;

i) To enable protection of information while in process, handling, storage & transit so as to Safeguard privacy of citizen's data and for reducing economic losses due to cybercrime or data theft;

j) To create a culture of cyber security and privacy enabling responsible user behavior & actions through an effective communication and promotion strategy;

Q.NO.68. What is ISO 27001 standard? Explain? (A) (M17 – 4M, MTP M1- 4M)

a) ISO/IEC 27001 (International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC)) defines how to organize information security in any kind of organization, profit or non-profit, private or state-owned, small or large. \

b) It is safe to say that this standard is the foundation of Information Security Management. ISO 27001 is for information security;

c) The same thing that ISO 9001 is for quality – it is a standard written by the world's best experts in the field of information security and aims to provide a methodology for the implementation of information security in an organization.

d) It also enables an organization to get certified, which means that an independent certification body has confirmed that information security has been implemented in the best possible way in the organization.

How the standard works?

ISO 27001 requires that management:

a) Systematically examines the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;

b) Designs and implements a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and

c) Adopts an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

Q.NO.69. XYZ is a government agency that had been developing and adopting office automation systems at random and in isolated pockets of its departments. At the same time, it was felt that the organisation needs to follow some specification for their Information Security Management System (ISMS). As an IT consultant, explain to the management to why they should follow ISO 27001:2013 standard? (A) (PM)

A company XYZ should adopt ISO 27001 for the following reasons:

a) It is suitable for protecting critical and sensitive information.

b) It provides a holistic, risk-based approach to secure information and compliance.

c) Demonstrates credibility, trust, satisfaction and confidence with stakeholders, partners, citizens and customers.

d) Demonstrates security status according to internationally accepted criteria.

e) Creates a market differentiation due to prestige, image and external goodwill.

f) If a company is certified once, it is accepted globally.

Q.NO.70. Discuss PDCA cyclic process under ISO27001. (A) (PM, MTP - N16 M1- 4M, M16 M1 – 4M, N15 M2 - 4M)

The Plan-Do-Check-Act (PDCA) cycle

ISO27001 prescribes 'How to manage information security through a system of information security management'. Such a management system consists of four phases that should be continuously implemented to minimize risks to the Confidentiality, Integrity and Availability (CIA) of information.

The PDCA cyclic process is explained below:

a) **The Plan Phase (Establishing the ISMS) –** This phase serves to plan the basic organization of information security, set objectives for information security and choose the appropriate security controls (the standard contains a catalogue of 133 possible controls).

b) **The Do Phase (Implementing and Working of ISMS) –** This phase includes carrying out everything that was planned during the previous phase.

c) **The Check Phase (Monitoring and Review of the ISMS) –** The purpose of this phase is to monitor the functioning of the ISMS through various "channels", and check whether the results meet the set objectives.

d) **The Act Phase (Update and Improvement of the ISMS) –** The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase.

The cycle of these four phases never ends, and all the activities must be implemented cyclically to keep the ISMS effective. ISO/IEC 27001:2005 applies this to all the processes in ISMS.

Q.No.71. What are the Benefits of ISO 27001? (B)

Benefits of ISO 27001

The key benefits of ISO 27001 are given as follows:

a) It can act as the extension of the current quality system to include security.

b) It provides an opportunity to identify and manage risks to key information and systems assets.

c) Provides confidence and assurance to trading partners and clients; acts as a marketing tool.

d) Allows an independent review and assurance to you on information security practices. A company may adopt ISO 27001 for the following reasons:

e) It is suitable for protecting critical and sensitive information.

f) It provides a holistic, risk-based approach to secure information and compliance.

g) Demonstrates credibility, trust, satisfaction and confidence with stakeholders, partners, citizens and customers.

h) Demonstrates security status according to internationally accepted criteria.

i) Creates a market differentiation due to prestige, image and external goodwill.

j) If a company is certified once, it is accepted globally.

Q.No.72. Explain the Standard on Auditing (SA) 402? (B) (MTP N16 M2 - 4M)

a) Audit Considerations Relating to an Entity using Service Organization, Standard on Auditing (SA) 402 is a revised version of the erstwhile Auditing and Assurance Standard (AAS) 24, "Audit Considerations Relating to Entities Using Service Organizations" issued by the ICAI in 2002.

b) The revised Standard deals with the user auditors responsibility to obtain sufficient appropriate audit evidence when a user entity uses the services of one or more service organizations.

c) SA 402 also deals with the aspects like obtaining an understanding of the services provided by a service organization, including internal control, responding to the assessed risks of material misstatement, Type 1 and Type 2 reports, fraud, non-compliance with laws and regulations and uncorrected misstatements in relation to activities at the service organization and reporting by the user auditor. This SA is effective for audits of financial statements w.e.f. April 1, 2010.

Q.NO.73. Discuss the 'Service Strategy' of IT Infrastructure Library (ITIL) Framework. (A) (PM, N15 - 4M, RTP N15, MTPN16 M2 - 6M)

Service Strategy: The center and origin point of the ITIL Service Lifecycle, the ITIL Service Strategy (SS) volume, provides guidance on clarification and prioritization of service-provider investments in services. It provides guidance on leveraging service management capabilities to effectively deliver value to customers and illustrate value for service providers.

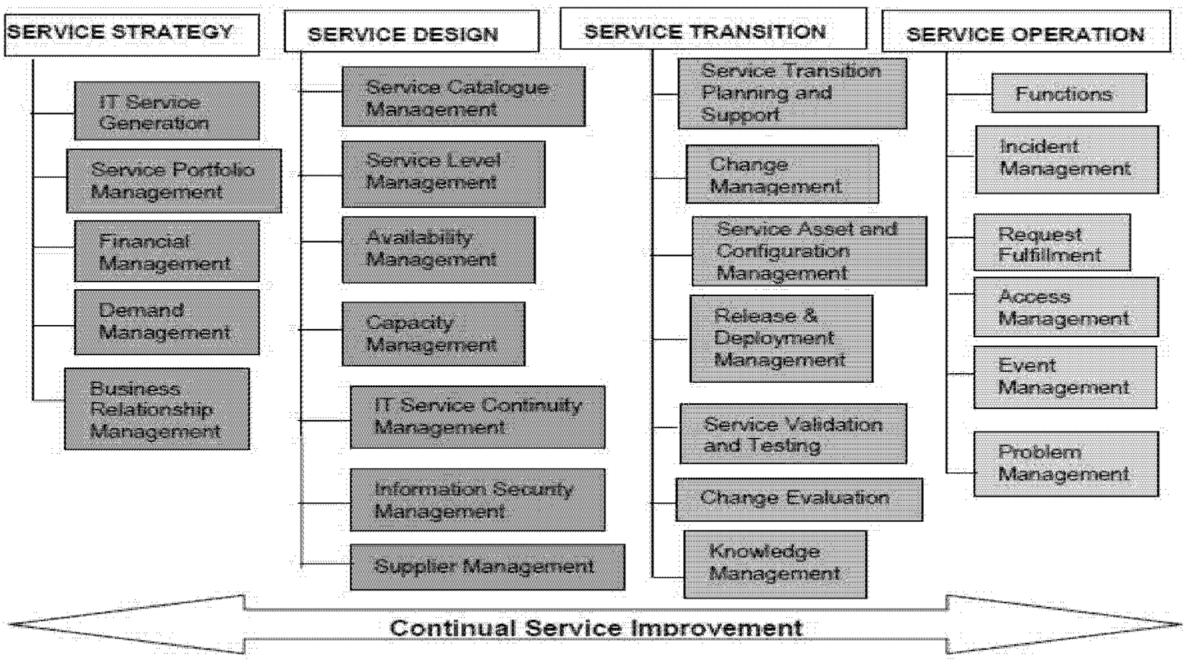
a) IT Service Generation: IT Service Management (ITSM) refers to the implementation and management of quality information technology services and is performed by IT service providers through People, Process and Information Technology.

b) Service Portfolio Management: IT portfolio management is the application of systematic management to the investments, projects and activities of enterprise Information Technology (IT) departments.

c) Financial Management: Financial Management for IT Services' aim is to give accurate and cost effective stewardship of IT assets and resources used in providing IT Services.

d) Demand Management: Demand management is a planning methodology used to manage and forecast the demand of products and services.

e) **Business Relationship Management:** Business Relationship Management is a formal approach to understanding, defining, and supporting a broad spectrum of inter –business activities related to providing and consuming knowledge and services via networks.



Q.NO.74. Discuss the 'Service Design' of IT Infrastructure Library (ITIL) Framework. (A) (N16 – 6M, MTPN16 M2 – 6M)

<u>**Service Design:**</u> Service Design translates strategic plans and objectives and creates the designs and specifications for execution through service transition and operations. It provides guidance on combining infrastructure, applications, systems, and processes, along with suppliers and partners, to present feasible service offerings. It includes design principles and methods for converting strategic objectives into portfolios of services and service assets.

It also provides guidance on the development of design capabilities for service management.

a) **Service Catalogue Management:** Service Catalogue management maintains and produces the Service Catalogue and ensures that it contains accurate details, dependencies and interfaces of all services made available to customers. Service Catalogue information includes ordering and requesting processes, prices, deliverables and contract points.

b) **Service Level Management:** Service-level management provides for continual identification, monitoring and review of the levels of IT services specified in the Service-Level Agreements (SLAs). Service-Level Management is the primary interface with the customer and is responsible for ensuring that the agreed IT services are delivered when and where they are supposed to be.

c) **Availability Management:** Availability management targets allow organizations to sustain the IT service-availability to support the business at a justifiable cost. The high-level activities comprise of realizing availability requirements, compiling availability plan, monitoring availability and maintenance obligations.

d) **Capacity Management:** Capacity management supports the optimum and cost-effective provision of IT services by helping organizations match their IT resources to business demands. The high-level activities include application sizing; workload management; demand management; modelling; capacity planning; resource management and performance management.

e) **IT Service Continuity Management:** IT Service Continuity Management (ITSCM) covers the processes by which plans are put in place and managed to ensure that IT services can recover and continue even after a serious incident occurs.

f) **Information Security Management:** A basic goal of security management is to ensure adequate information security, which in turn, is to protect information assets against risks, and thus to maintain their value to the organization. This is commonly expressed in terms of ensuring their confidentiality, integrity and availability, along with related properties or goals such as authenticity, accountability, non-repudiation and reliability.

g) **Supplier Management:** The purpose of Supplier Management is to obtain value for money from suppliers and contracts. It ensures that underpinning contracts and agreements align with business needs, Service Level Agreements and Service Level Requirements. Supplier Management oversees process of identification of business needs, evaluation of suppliers, establishing contracts, their categorization, management and termination.

Q.No.75. Discuss the 'Service Transition' of IT Infrastructure Library (ITIL) Framework. (A)

<u>Service Transition:</u> Service Transition provides guidance on the service design and implementation ensuring that the service delivers the intended strategy and that it can be operated and maintained effectively. Service Transition planning provides guidance on managing the complexity of changes to services and service management processes to prevent undesired consequences whilst permitting for innovation. It provides guidance on the support mechanism on transferring the control of services between customers and service providers.

a) **Service Transition Planning and Support:** The service transition planning and support process ensures the orderly transition of a new or modified service into production, together with the necessary adaptations to the service management processes. The service transition planning and support process must incorporate the service design and operational requirements within the transition planning.

b) **Change management and Evaluation:** This aims to ensure that standardized methods and procedures are used for efficient handling of all changes. A change is an event that results in a new status of one or more configuration items (CIs), and which is approved by management, is cost-effective, enhances business process changes (fixes) – all with a minimum risk to IT infrastructure.

c) **Service Asset and Configuration Management:** Service Asset and Configuration Management is primarily focused on maintaining information (i.e., configurations) about Configuration Items (i.e., assets) required to deliver an IT service, including their relationships. Configuration management is the management and traceability of every aspect of a configuration from beginning to end.

d) **Release and Deployment Management:** Release and deployment management is used by the software migration team for platform-independent and automated distribution of software and hardware, including license controls across the entire IT infrastructure. Proper software and hardware control ensures the availability of licensed, tested, and version-certified software and hardware, which functions as intended when introduced into existing infrastructure.

e) **Service Validation and Testing:** The objective of ITIL Service Validation and Testing is to ensure that deployed Releases and the resulting services meet customer expectations, and to verify that IT operations are able to support the new service.

f) **Knowledge Management:** Knowledge Management (KM) is the process of capturing, developing, sharing, and effectively using organisational knowledge. It refers to a multidisciplined approach to achieving organisational objectives by making the best use of knowledge.

Q.No.76. Discuss the functions of 'Service operation' of IT Infrastructure Library (ITIL) Framework. (A)

<u>Functions:</u> The major functions are as follows:

i) **Service Desk:** The service desk is one of four ITIL functions and is primarily associated with the Service Operation lifecycle stage. Tasks include handling incidents and requests, and providing an interface for other ITSM processes. Features include Single Point of Contact (SPOC); Single Point of Entry and Exit; easier for customers and streamlined communication channel.

ii) **Application management**: ITIL application management encompasses a set of best practices proposed to improve the overall quality of IT software development and support through the life-cycle of software development projects, with particular attention to gathering and defining requirements that meet business objectives.

iii) **IT Operations:** IT Operations primarily work from documented processes and procedures and should be concerned with a number of specific sub-processes, such as: output management, job scheduling, backup and restore, network monitoring/management, system monitoring/management, database monitoring/management storage monitoring/management.

iv) **IT Technical Support**: IT technical support provides a number of specialist functions: research and evaluation, market intelligence, proof of concept and pilot engineering, specialist technical expertise, and creation of documentation.

Q.No.77 Discuss the 'Service operation' of IT Infrastructure Library (ITIL) Framework. (A)

Service Operation: Service Operation provides guidance on the management of a service through its day-to-day production life. It also provides guidance on supporting operations by means of new models and architectures such as shared services, utility computing, web services, and mobile commerce.

IT Technical Support: IT technical support provides a number of specialist functions: research and evaluation, market intelligence, proof of concept and pilot engineering, specialist technical expertise, and creation of documentation.

a) **Incident Management:** Incident management aims to restore normal service operation as quickly as possible and minimize the adverse effect on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

b) **Request fulfillment:** Request fulfillment (or request management) focuses on fulfilling Service Requests, which are often minor changes (e.g., requests to change a password) or requests for information.

c) **Access Management:** It is a process that focuses on granting authorized users the right to use a service, while preventing access to non-authorized users.

d) **Event Management:** An event may indicate that something is not functioning correctly, leading to an incident being logged. Event management generates and detects notifications, while monitoring checks the status of components even when no events are occurring.

e) **Problem Management:** Problem management aims to resolve the root causes of incidents and thus to minimize the adverse impact of incidents caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors.

Q.No.78. Discuss the 'Continual Service Improvement' of IT Infrastructure Library (ITIL) Framework. (A)

Continual Service Improvement:

a) Continual Service Improvement provides guidance on the measurement of service performance through the service life-cycle, suggesting improvements to ensure that a service delivers the maximum benefit.

b) This volume provides guidance on creating and maintaining value for customers through improved design, introduction, and operation of services.

c) It combines principles, practices, and methods from change management, quality management, and capability improvement to achieve incremental and significant improvements in service quality, operational efficiency, and business continuity.

Q.No.79. ABC Ltd.is not aware of the importance and requirement relating to 'Retention of Electronic Records' as per IT Act, 2008. Please enlighten them on this. (A)

ABC Ltd. is looking for a suitable IS auditor. I hereby explain my suitability for the same, as I hereby announce that I possess the desired skill set that is generally expected to be with an IS auditor which includes the following:

a) Sound knowledge of business operations, practices and compliance requirements;

b) Possess the requisite professional technical qualification and certifications;

c) A good understanding of information Risks and Controls;

d) Knowledge of IT strategies, policy and procedural controls;

e) Ability to understand technical and manual controls relating to business continuity; and

f) Good knowledge of Professional Standards and Best Practices of IT controls and security.

THE END

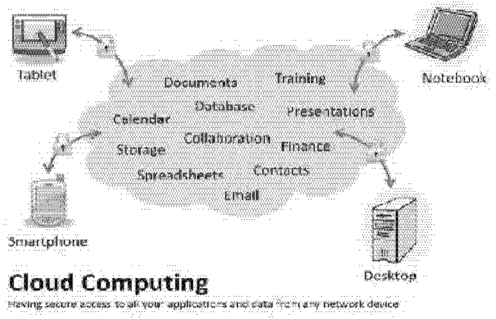
8. EMERGING TECHNOLOGIES

Q.No.1. What is Grid Computing? (A)

1. The idea of Grid computing is to make use of non-utilized or underutilized computing resources or power by the needy organizations, and thereby the Return On Investment (ROI) on computing investments can be increased.
2. Grid computing is a network of computing or processor machines managed with a kind of software such as middleware, in order to access and use the resources remotely. The managing activity of grid resources through the middleware is called Grid Services.
3. Grid Services provide access control, security, access to data including digital libraries and databases, and access to large-scale interactive and long-term storage facilities.
4. Grid Computing is more popular due to the following reasons:
   a) It has the ability to make use of unused computing power, and thus, it is a cost-effective solution (reducing investments, only recurring costs).
   b) This enables heterogeneous resources of computers to work cooperatively and collaboratively to solve a scientific problem.
5. Grid computing requires the use of software that can divide and carve out pieces of a program as one large system image to several thousand computers.
6. *One concern about grid is that if one piece of the software on a node fails, other pieces of the software on other nodes may fail.*

Q.No.2. Explain Cloud Computing in detail. (A) (PM)

1. Cloud computing is nothing but use of computing resources as a service through networks, typically the Internet.
2. A cloud is a collection of servers, applications, databases, documents, agreements, spreadsheets, storage capacity etc which allows organizations to share these resources from anywhere.
3. With Cloud Computing, users can access database resources via the Internet from anywhere without worrying about any maintenance or management of actual resources.
4. Databases in cloud may be highly dynamic and scalable.
5. The best example of cloud computing is Google Apps where any application can be accessed using a browser and it can be deployed on thousands of computer through the Internet.
6. *Cloud computing is both, a combination of software and hardware based computing resources delivered as a networked service.*
7. Cloud computing provides the facility to access shared resources and common infrastructure offering services on demand over the internetwork.



8. The location of physical resources and devices being accessed are typically not known to the end user.
9. It also provides facilities for users to develop, deploy and manage their applications 'on the cloud', which entails virtualization of resources that maintains and manages itself.

10. With cloud computing, companies can scale up to massive capacities in an instant without having to invest in new infrastructure, train new personnel or license new software.
11. Cloud computing is of particular benefit to small and medium-sized business systems.

Q.No.3. What are the Pertinent similarities & difference between Cloud Computing and Grid computing? (OR) what are the significant differences between Cloud Computing & Grid computing. (OR) cloud vs Grid computing (B) (PM, N15 RTP, N15 MTP2, M17 – 4M)

1. Grid and Cloud are two terms used in computing to refer to two types of resource sharing techniques where multiple computing devices and usually the Internet are involved.
2. Cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive and it provides on demand services over the Internet.
3. Grid computing is a form of distributed computing where a virtual computing system is compiled by using many loosely connected computing devices to perform a large computing task.

PERTINENT SIMILARITIES:

1. **Scalability:** Cloud computing and grid computing both are scalable. Scalability is accomplished through load balancing of application instances running separately on a variety of operating systems and connected through Web services.
2. **Multitenancy and multitasking:** Both computing types involve multitenancy and multitasking, meaning that many customers can perform different tasks, accessing a single or multiple application instances.
3. **Reduced cost:** Sharing of resources among large pool of users help to reduce infrastructure costs.
4. **High uptime availability:** Service level agreement (SLA) ensures that high uptime availability in the terms of 99%.

PERTINENT DIFFERENCES:

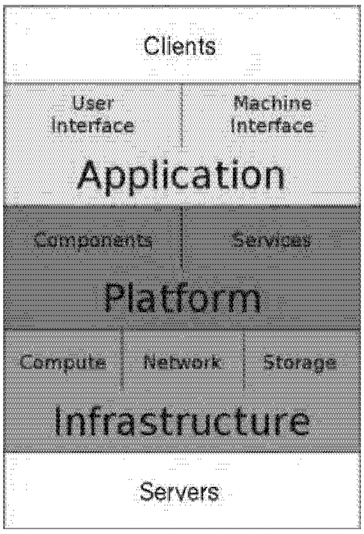
1) **Data storage:** While the storage computing in the grid is well suited for data-intensive storage, it is not economically suited for storing objects as small as 1 byte. While in cloud computing, we can store an object as low as 1 byte and as large as 5 GB or even several terabytes.
2) **Computation:** A computational grid focuses on computationally intensive operations, while cloud computing offers two types of instances: standard and high process oriented CPUs.

Q.No.4. Discuss the major goals of Cloud computing. (PM, N14-6M, N14 RTP, M16 MTP1) (A)
(OR)
Discuss some of the pertinent objectives in order to achieve the goals of cloud computing?

The key goals of a cloud computing are as follows:

a) To create a highly efficient IT eco system, where resources are pooled together
b) Costs are aligned with what resources are actually used, i.e. pay only for resources what actually used.
c) Access services and data from anywhere at any time
d) Scale the IT system quickly, easily and cost-effectively based on the business needs
e) Consolidate IT infrastructure into a more integrated and manageable environment
f) Reduce costs related to IT energy/power consumption
g) Improve "Anywhere Access" (AA) for ever increasing users
h) Enable rapidly provision resources as needed.

Q.No.5. Write about Cloud computing architecture (CCA)? (or) Describe Frontend and Backend architectures with reference to cloud computing? (OR) cloud computing architecture comprises of two parts. Briefly describe these two parts. (A) (PM, M15 RTP, M17-4M)



1. The Cloud Computing Architecture (CCA) of a cloud solution is the structure of the system, which comprises of on-premise and cloud resources, services, middleware, and software components, their geo-location, their externally visible properties and the relationships between them.
2. In the context of cloud computing, protection depends on having the Right Architecture for the Right Application (RARA).
3. A cloud computing architecture consists of a Front end and a Back end connected to each other through a network, usually the Internet.
4. The front end is interface for the user and the backend is the cloud section for the whole system which facilitates the cloud services.
5. **Front End Architecture:**

   a) The Front end of the cloud computing system comprises of the client's devices (or computer network) and some applications needed for accessing the cloud computing system.

   b) All the cloud computing systems do not give the same interface to users.

   c) Web services like electronic mail programs use some existing web browsers such as Firefox, Microsoft's internet explorer or Apple's Safari.
6. **Back End Architecture:**

   a) Back end refers to some service facilitating peripherals.

   b) In cloud computing, the back end is cloud itself, which may include various computer machines, data storage systems and servers.

   c) Groups of these clouds make up a whole cloud computing system. Usually, every application would have its individual dedicated server for services.

   Central Server:

   a) A central server is established to be used for administering the whole system.

   b) It is also used for monitoring client's demand as well as traffic to ensure that everything of system runs without any problem.

   Protocol: There are some set of rules, technically referred as protocols, are followed by server.

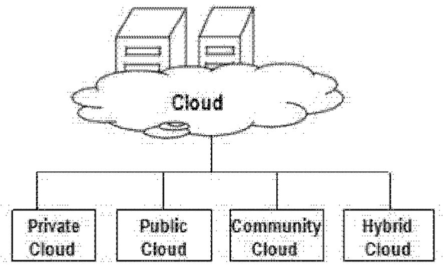
   Middleware:

   a) Cloud uses a special type of software known as middleware. Middleware allows computers that are connected on networks to communicate with each other.

   b) The cloud computing system must have a redundant back-up copy of all the data of its client's.

Q.No.6. Explain Cloud Computing Environment or Deployment models (OR) Explain different types of clouds? (B)

The cloud computing environment can consist of multiple types of clouds based on their deployment and usage. They are



a) Private Cloud.

b) Public Cloud.

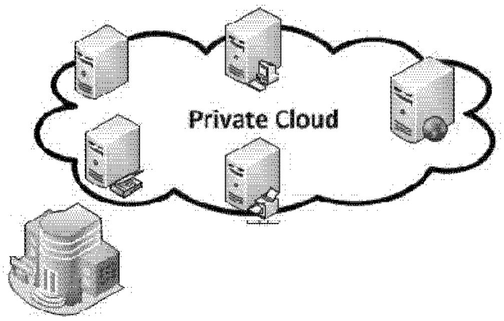
c) Hybrid Cloud.

d) Community Cloud.

Q.No.7. What is a Private Cloud? Explain its characteristics? (A)

Private Cloud:

a) It resides within the boundaries of an organization and is used exclusively for the organization's benefits.



b) These are also called internal clouds or corporate clouds.

c) Private Clouds can either be private to the organization and managed by the single organization (On-Premise Private Cloud) or can be managed by third party (Outsourced Private Cloud).

d) They are built primarily by IT departments within enterprises, who seek to optimize utilization of infrastructure resources within the enterprise by provisioning the infrastructure with applications using the concepts of grid and virtualization.

Characteristics of Private Cloud:

a) Secure: The private cloud is secure as it is deployed and managed by the organization itself, and hence there is least chance of data leakage from the private cloud.

b) Central Control: The private cloud is managed and controlled by the organization itself, there is no need for the organization to rely on anybody.

c) Weak Service Level Agreements (SLAs): SLA is defined as agreements between the user and the service provider. In private cloud, either Formal SLAs do not exist or are weak.

Q.No.8. Mention the advantages and limitations of Private Cloud? (B) (PM)

Advantages:

a) Improves average server utilization;

b) Allow usage of low-cost servers and hardware thus improve efficiencies;

c) Reducing the costs, compared to individual infrastructure by an organization.

d) Provides a high level of security and privacy to the user.

e) It is small in size, easy to controlled and maintained by the organization.

Limitations:

a) IT teams in the organization may have to invest in buying, building and managing the clouds independently, hence it is expensive compared to public cloud.

b) Budget is a constraint in private clouds and they also have loose SLAs.

c) It supports only limited number of users, hence less scalable.

Q.No.9. Explain the major differences between On-Premise Private Cloud and Outsourced Private cloud. (B)

	On-Premise Private Cloud	**Outsourced Private Cloud**
Management	Managed by the organization itself.	Managed by the third party Everything is same as usual private cloud except that here the cloud is outsourced
Service Level Agreements(SLAs)	SLAs are defined between the organization and its users. Users have broader access rights than general public cloud users and service providers are able to efficiently provide the service because of small user base and mostly efficient network.	These are usually followed strictly as it is a third party organization.
Network	Network management and network issue resolving are easier. The networks usually have high bandwidth and low latency.	The cloud is fully deployed at the third party site and organizations connect to the third party by means of either a dedicated connection or through internet.
Security and Data Privacy	Comparatively it is more resistant to attacks than any other cloud and the security attacks are possible from an internal users only.	Cloud is relatively less secure and the security threat is from the third party and the internal employee.
Location	The data is usually stored in the same geographical location where the cloud users are present. In case of several physical locations, the cloud is distributed over several places and is accessed using the internet.	The cloud is located off site and when there is a change of location the data need to be transmitted through long distances.
Performance	The performance depends on the network and resources and can be controlled by the network management team.	The performance of the cloud depends on the third party that is outsources the cloud.

Q.No.10. What is public cloud? Explain its characteristics? (A)

Public Clouds: **(N14 – RTP)**

a) The public cloud is the cloud infrastructure that is provisioned for open use by the general public.

b) It may be owned, managed, and operated by a business, academic, or government organizations, or some combination of them.

c) Typically, public clouds are administrated by third parties or vendors over the Internet, and the services are offered on pay – per - use basis.

d) These are also called Provider Clouds or external cloud.

e) Public cloud consists of users from all over the world wherein a user can simply purchase resources on an hourly basis and work with the resources which are available in the cloud provider's premises.

Characteristics:

a) **Highly Scalable:** The resources in the public cloud are large in number and the service providers make sure that all requests are granted. Hence public clouds are considered to be scalable.

b) **Affordable:** The cloud is offered to the public on a pay-as-you-go basis. So the user has to pay only for what he or she is using (using on a per-hour basis).

c) **Less Secure:** Since it is offered by a third party and they have full control over the cloud, the public cloud is less secure out of all the other deployment models.

d) **Highly Available:** It is highly available because anybody from any part of the world can access the public cloud with proper permissions.

e) **Stringent SLAs:** As the service provider's business reputation and customer strength are totally dependent on the cloud services, they follow the SLAs strictly and violations are avoided.

Q.No.11. Mention the advantages and limitations of Public Cloud? (B) (PM, N14 RTP)

Advantages of Public Cloud:

a) It is widely used in the development, deployment and management of enterprise applications, at affordable costs.

b) It allows the organizations to deliver highly scalable and reliable applications rapidly and at more affordable costs.

c) No need for establishing infrastructure for setting up and maintaining the cloud.

d) Strict SLAs are followed

e) No limit for the number of users.

Limitations:

a) Security assurance and building trust among the clients is far from desired.

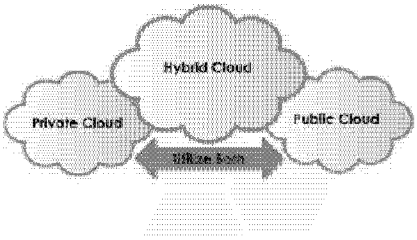
b) Privacy and organizational autonomy (independence) are not possible.

Q.No.12. What is Hybrid Cloud? Explain its characteristics? (B) (PM)

1. This is a combination of both at least one private (internal) and at least one public (external) cloud computing environments.

2. The usual method of using the hybrid cloud is to have a private cloud initially, and then for additional resources, the public cloud is used.

3. The hybrid cloud can be regarded as a private cloud extended to the public cloud and aims at utilizing the power of the public cloud by retaining the properties of the private cloud.



Characteristics:

a) **Scalable:** The hybrid cloud has the property of public cloud with a private cloud environment and as the public cloud is scalable; the hybrid cloud with the help of its public counterpart is also scalable.

b) **Partially Secure:** The private cloud is considered as secured and public cloud has high risk of security breach(violation) thus it is partially secure.

c) **Stringent SLAs:** Overall the SLAs are more strict than the private cloud and might be as per the public cloud service providers.

d) **Complex Cloud Management:** Cloud management is complex as it involves more than one type of deployment models and also the number of users is high.

Q.No.13. Mention the advantages and limitations of Hybrid cloud? (B) (PM)

Advantages:

a) It is highly scalable and gives the power of both private and public clouds.

b) It provides better security than the public cloud.

Limitation: The security features are not as good as the private cloud and complex to manage.

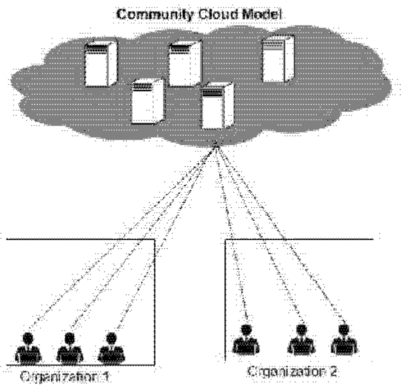
Q.No.14. What is Community Cloud? Explain its characteristics? (B) (PM, RTP M17 N16, MTP1 M17-4M)

1. The community cloud is the cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns. (eg. mission security requirements, policy, and compliance considerations).

2. It may be owned, managed, and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises.

3. In this, a private cloud is shared between several organizations.

4. This model is suitable for organizations that cannot afford a private cloud and cannot rely on the public cloud either.



Characteristics:

a) Collaborative and Distributive Maintenance: In this, no single company has full control over the whole cloud. This is usually distributive and hence better cooperation provides better results.

b) Partially Secure: Some organizations share the cloud, so there is a possibility that the data can be leaked from one organization to another, though it is safe from the external world.

c) Cost Effective: Cloud is being shared by several organizations community, not only the responsibility gets shared, the community cloud becomes cost effective.

Q.No.15. Mention the advantages and limitations of community Cloud? (PM)

Advantages:

a) It allows establishing a low-cost private cloud.

b) It allows collaborative work on the cloud.

c) It allows sharing of responsibilities among the organizations.

d) It has better security than the public cloud.

Limitations:

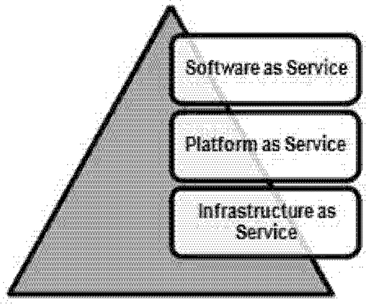
a) The autonomy of the organization is lost.

b) Some of the security features are not as good as the private cloud.

c) It is not suitable in the cases where there is no collaboration.

Q.No.16. Write about various Cloud computing service models? (Or) Cloud computing service providers offers their services on the lines of several fundamental models. Describe the various types of cloud computing models. (A) (M16 - 6M)

1. Cloud computing is a model that enables the end users to access the shared pool of resources such as computing, network, storage, database and application as an on-demand service without the need to buy or own it.
2. The services are provided and managed by the service provider.
3. The essential characteristics of the cloud include on-demand, self service, broad network access, resource pooling, rapid elasticity, and measured service.
4. The National Institute of Standards and Technology (NIST) define three basic service models -
   - **a)** Infrastructure as a Service (IaaS)
   - **b)** Platform as a Service (PaaS)
   - **c)** Software as a Service (SaaS)



Q.No.17. What is Infrastructure as a Service (IaaS)? Explain its services? (A)

1. IaaS, a hardware-level service, provides computing resources such as processing power, memory, storage, and networks for cloud users to run their application on-demand.
2. It allows users to maximize the utilization of computing capacities without having to own and manage their own resources.
3. IaaS changes the computing from a physical infrastructure to a virtual infrastructure through virtual computing; storage; and network resources by abstracting the physical resources.
4. In order to deploy applications, cloud clients install operating -system images and their application software on the cloud infrastructure.
5. The end-users or IT architects will use the infrastructure resources in the form of Virtual machines (VMs) and design virtual infrastructure, network load balancers etc., based on their needs.
6. The IT architects need not maintain the physical servers as it is maintained by the service providers.
7. Examples of IaaS providers include Amazon Web Services (AWS), Google Compute Engine, OpenStack and Eucalyptus.
8. **A typical IaaS provider may provide the following services:**
   - **a) Compute:** Computing as a Service includes virtual Central Processing Inputs (CPUs) and virtual main memory for the Virtual Machines (VMs) that are provisioned to the end users.
   - **b) Storage:** STaaS provides back-end storage for the VM images. Some of the IaaS providers also provide the back end for storing files.
   - **c) Network:** Network as a Service (NaaS) provides virtual networking components such as virtual router, switch, and bridge for the VMs.
   - **d) Load Balancers:** Load balancing as a Service may provide load balancing capability at the infrastructure layer.

Q. No.18. Explain the characteristics of IaaS? (A) (PM)

1) **Web access to the resources:** The IaaS model enables the IT users to access infrastructure resources over the Internet. When accessing a huge computing power, the IT user need not get physical access to the servers.
2) **Centralized management:** The resources distributed across different parts are controlled from any management console that ensures effective resource management and effective resource utilization.
3) **Elasticity and Dynamic Scaling:** IaaS resources and services can be increased or decreased according to the requirements.
4) **Shared infrastructure:** IaaS follows a one-to-many delivery model and allows multiple IT users to share the same physical infrastructure and increases resource utilization.
5) **Metered Services:** IaaS allows the IT users to rent the computing resources instead of buying it. The services consumed by the IT user will be measured, and the users will be charged based on the usage.

Q.No.19. Explain different Instances of IaaS? (B)

1. **Network as a Service (NaaS):**
   - **a)** NaaS provides users with needed data communication capacity to accommodate bursts in data traffic during data-intensive activities such as video conferencing or large file downloads.
   - **b)** It is an ability given to the end-users to access virtual network services that are provided by the service provider over the Internet on pay-per-use basis.
   - **c)** NaaS allows network architects to create virtual networks; virtual network interface cards (NICs), virtual routers, virtual switches, and other networking components.
   - **d)** NaaS providers operate using three common service models:
     - **i)** Virtual Private Network (VPN)
     - **ii)** Bandwidth on Demand (BoD)
     - **iii)** Mobile Virtual Network (MVN).
2. **Storage as a Service (STaaS): (RTP N16)**
   - **a)** STaaS provides storage infrastructure on a subscription basis to users.
   - **b)** It is a low-cost and convenient way to store data, synchronize data across multiple devices, manage off-site backups, mitigate risks of disaster recovery, and preserve records for the long-term.
   - **c)** STaaS allows the end users to access the files at any time from any place.
   - **d)** STaaS provider provides the virtual storage that is abstracted from the physical storage of any cloud data center.
3. **Database as a Service (DBaaS):**
   - **a)** It provides users with seamless mechanisms to create, store, and access databases at a host site on demand.
   - **b)** It is an ability given to the end users to access the database service without the need to install and maintain it on the pay-per-use basis.
   - **c)** The end users can access the database services through any Application Programming Interfaces (APIs) or Web User Interfaces provided by the service provider.

4. **Backend as a Service (BaaS):**
   - a) It provides web and mobile app developers a way to connect their applications to backend cloud storage.
   - b) It also provides added services such as user management, push notifications, social network services integration using custom software development kits and application programming interfaces.

5. **Desktop as a Service (DTaaS):**
   - a) It that provides ability to the end users to use desktop virtualization without buying and managing their own infrastructure.
   - b) DTaaS is a pay-per-use cloud service delivery model in which the service provider manages the back-end responsibilities of data storage, backup, security and upgrades.

Q.No.20. Explain PaaS? (B) (RTP M15, MTP M17, N16)

1. PaaS provides the users the ability to develop and deploy an application on the development platform provided by the service provider.
2. In traditional application development, the application will be developed locally and will be hosted in the central location.
3. PaaS changes the application development from local machine to online.
4. For example- Google AppEngine, Windows Azure Compute etc.
5. **Typical PaaS providers may provide:**
   - a) **Programming Languages:** PaaS providers provide a wide variety of programming languages like Java, PHP, Python, Ruby etc. for the developers to develop applications.
   - b) **Application Frameworks:** PaaS vendors provide application development framework like Joomla, WordPress, Sinatra etc. for application development.
   - c) **Database:** Along with PaaS platforms, PaaS providers provide some of the popular databases like ClearDB, Cloudant, Redis etc. so that application can communicate with the databases.
   - d) **Other Tools:** PaaS providers provide all the tools that are required to develop, test, and deploy an application.

Q.No.21. Explain the characteristics of PaaS? (B) (PM)

1. **All in One:** Most of the PaaS providers offer services like programming languages to develop, test, deploy, host and maintain applications in the same Integrated Development Environment (IDE).
2. **Web access to the development platform:** It provides web access to the development platform that helps the developers to create, modify, test, and deploy different applications on the same platform.
3. **Offline Access:** The developers can develop an application locally (offline) and deploy it online whenever they are connected to the Internet.
4. **Built-in Scalability:** PaaS services provide built-in scalability to an application. It ensures that the application is capable of handling varying loads efficiently.
5. **Collaborative Platform:** To enable collaboration among developers, PaaS providers provide tools for project planning and communication.
6. **Diverse Client Tools:** PaaS providers offer a wide variety of client tools like Web User Interface (UI), Application Programming Interface (API) etc. to help the developers to choose the tool of their choice.

Q.No.22. Explain the SaaS? Explain Services provided by SaaS? (A) (RTPM15) (OR) Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) are two of the three main categories of cloud computing. What's the third category? Explain in brief.

1. SaaS provides ability to the end users to access an application over the Internet that is hosted and managed by the service provider.
2. SaaS changes the way the software is delivered to the customers.
3. In the traditional software model, the software is delivered as a license-based product that needs to be installed in the end user device.
4. SaaS is delivered as an on-demand service over the Internet, there is no need to install the software to the end-user's devices and these services can be accessed or disconnected at any time based on the end user's needs.

SERVICES PROVIDED BY SAAS:

a) **Business Services:** SaaS providers provide a variety of business services to startup companies that includes ERP, CRM, billing, sales, and human resources.

b) **Social Networks:** Since the number of users of the social networking sites is increasing exponentially, loud computing is the perfect match for handling the variable load.

c) **Document Management:** Most of the SaaS providers provide services to create, manage, and track electronic documents as most of the enterprises extensively use electronic documents.

d) **Mail Services:** To handle the unpredictable number of users and the load on e-mail services, most of the email providers offer their services as SaaS services.

Q.No.23. Explain the Characteristics of SaaS? (B) (PM)

1. **One to Many:** SaaS services are delivered as one-to-many models where a single instance of the application can be shared by multiple customers.
2. **Web Access:** SaaS services allow the end users to access the application from any location, from any device that is connected to the Internet.
3. **Centralized Management:** Since SaaS services are hosted and managed from the central location, the SaaS providers perform the automatic updates to ensure that each customer is accessing the most recent version of the application without any user-side updates.
4. **Multi-device Support:** SaaS services can be accessed from any end user devices such as desktops, laptops, tablets, smart phones, and thin clients.
5. **Better Scalability:** Most of the SaaS services leverage PaaS and IaaS for its development and deployment and ensure a better scalability than traditional software.
6. **High Availability:** SaaS services ensure 99.99% availability of user data as proper backup and recovery mechanisms are implemented.
7. **API Integration:** SaaS services have the capability of integrating with other software or service through standard APIs.

Q.No.24. Explain the various Instances of SaaS? (B)

1. **Testing as a Service (TaaS):** This provides users with software testing capabilities such as generation of test data, generation of test cases, execution of test cases and test result evaluation on a pay-per-use basis.

2. **API as a Service (APIaaS):** This allows users to explore functionality of Web services such as Google Maps, Payroll processing, and credit card processing services etc.
3. **Email as a Service (EaaS):** This provides users with an integrated system of emailing, office automation, records management, migration, and integration services with archiving, spam blocking, malware protection, and compliance features.

Q.No.25. Explain various other cloud service models. (B)

1. **Communication as a Service (CaaS):** **(M16 MTP1)**
   - **a)** CaaS has evolved in the same lines as SaaS.
   - **b)** CaaS is an outsourced enterprise communication solution that can be leased from a single vender/seller.
   - **c)** The CaaS vendor is responsible for all hardware and software management and offers guaranteed Quality of Service (QoS).
   - **d)** It allows businesses to selectively deploy communication devices and modes on a pay -as-you-go, as-needed basis by eliminating the large capital investments.
   - **e)** Examples are: Voice over IP (VoIP), Instant Messaging (IM), Collaboration and Videoconferencing application using fixed and mobile devices.
2. **Data as a Service (DaaS):**
   - **a)** DaaS provides data on demand to a diverse set of users, systems or application.
   - **b)** The data may include text, images, sounds, and videos.
   - **c)** Data encryption and operating system authentication are commonly provided for security.
   - **d)** DaaS users have access to high-quality data in a centralized place and pay by volume or data type, as needed.
   - **e)** However, as the data is owned by the providers, users can only perform read operations on the data.
   - **f)** DaaS is highly used in geography data services and financial data services
3. **Security as a Service (SECaaS):**
   - **a)** It is an ability given to the end user to access the security service provided by the service provider on a pay-per-use basis.
   - **b)** It is a new approach to security in which cloud security is moved into the cloud itself whereby cloud service users will be protected from within the cloud using a unified approach to threats.
   - **c)** Four mechanisms of Cloud security that are currently provided are Email filtering, Web content filtering, Vulnerability management and Identity management
4. **Identity as a Service (IDaaS):**
   - **a)** It is an ability given to the end users; typically an organization or enterprise; to access the authentication infrastructure that is built, hosted, managed and provided by the third party service provider.
   - **b)** Generally, IDaaS includes directory services, authentication services, risk and event monitoring, single sign-on services, and identity and profile management.

Q.No.26. Explain different characteristics of cloud computing? (A) (PM, N16 RTP)

1. **High Scalability:** Cloud environments enable servicing of business requirements for larger audiences, through high scalability, it allows ability to increase or decrease resources according to the requirements.
2. **Agility:** The cloud works in the 'distributed mode 'environment. It shares resources among users and tasks, while improving efficiency and agility (responsiveness).

3. **High Availability and Reliability:** Availability of servers is supposed to be high and more reliable as the chances of infrastructure failure are minimal.
4. **Multi-sharing:** With the cloud working in a distributed and shared mode, multiple users and applications can work more efficiently with cost reductions by sharing common infrastructure.
5. **Virtualization:** This technology allows servers and storage devices to increasingly share and utilize applications, by easy migration from one physical server to another.
6. **Performance:** It is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.
7. **Maintenance:** Cloud computing applications are easier, because they are not to be installed on each user's computer and can be accessed from different places
8. **Services in Pay-Per-Use Mode**: SLAs between the provider and the user must be defined when offering services in pay per use mode. This may be based on the complexity of services offered.

Q.No.27. Briefly discuss the advantages of Cloud computing?

(OR)

What are the advantages of using cloud computing environment? (A)(PM, N15-5M, N16 MTP2)

Cloud computing provides large number of benefits such as cost efficiency, easy access of information and applications and availability of large storage space.

1. **Cost Efficiency:**
   - a) Cloud computing is probably the most cost efficient method to use, maintain and upgrade.
   - b) Traditional desktop software costs companies a lot in terms of finance. Adding up the licensing fees for multiple users can prove to be very expensive for the establishment concerned.
   - c) The cloud, on the other hand, is available at much cheaper rates and hence, can significantly lower the company's IT expenses.
   - d) Besides, there are many one-time-payments, pay-as-you-go and other scalable options available, which make it very reasonable for the company.

2. **Almost Unlimited Storage:**
   - a) Storing information in the cloud gives us almost unlimited storage capacity.
   - b) Hence, one no more need to worry about running out of storage space or increasing the current storage space availability.
3. **Backup and Recovery:**
   - a) Since all the data is stored in the cloud, backing it up and restoring the same is relatively much easier than storing the same on a physical device.
   - b) Furthermore, most cloud service providers are usually competent enough to handle recovery of information.
   - c) Hence, this makes the entire process of backup and recovery much simpler than other traditional methods of data storage.
4. **Automatic Software Integration:**
   - a) In the cloud, software integration is usually something that occurs automatically.
   - b) This means that we do not need to take additional efforts to customize and integrate the applications as per our preferences.
   - c) This aspect usually taken care of service provider.
   - d) Cloud computing allows us to customize the options with great ease

5. **<u>Easy Access to Information:</u>** Once registered in the cloud, one can access the information from anywhere, where there is an Internet connection. This convenient feature lets one move beyond time zone and geographic location issues.

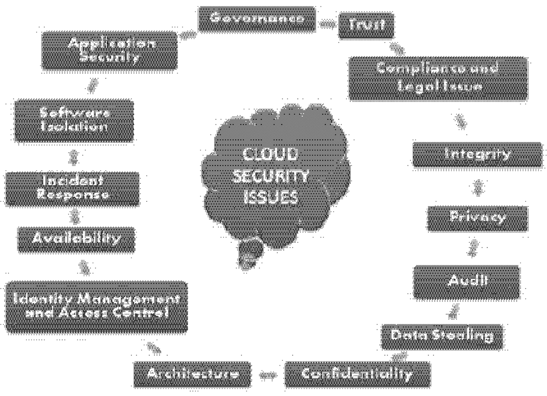
6. **<u>Quick Deployment:</u>**

   a) Cloud computing gives us the advantage of quick deployment and use of services.

   b) Once we opt for this method of functioning, the entire system can be fully functional in a matter of a few minutes.

Q.No.28. Explain key challenges relating to cloud computing? (OR)
Explain various security issues of cloud computing? (OR)
Management wants to know the major challenges in using cloud computing technology for running the new web application. Write any five challenges. (OR)
Explain the Major challenges in cloud computing issues in cloud computing technology for running the new web application. (A) (PM, M15-5M, N14 RTP)

Maintaining <u>security and confidentiality</u> of data is one of the key challenges for cloud computing.



a) <u>Confidentiality:</u>

   i) Cloud works on public networks thus Prevention of the <u>unauthorized disclosure</u> of the data is referred as Confidentiality.

   ii) With the use of <u>encryption and physical isolation</u>, data can be kept secret.

   iii) *The basic approaches to attain confidentiality are the encrypting the data before placing it in a Cloud with the use of <u>TC3 (Total Claim Capture & Control)</u>.*

b) <u>Integrity:</u>

   i) Integrity refers to the <u>prevention of unauthorized</u> modification of data and it ensures that data is of <u>high quality, correct, consistent and accessible</u>.

   ii) Data integrity ensures that data is error free and represent the <u>actual facts</u>.

   iii) The data owners need to be ensured that data after moving to cloud <u>not changed</u>, tampered<u>, or deleted</u>.

   iv) Strong <u>data integrity</u> controls such as digital signature and authorization control for data access and use should be <u>maintained</u> to deal with issue of <u>data loss and deletion</u>.

c) <u>Availability:</u>

   i) It refers to data is available when needed. It also meets the organization's continuity and contingency <u>planning requirements</u>

   ii) *Availability refers to the <u>prevention of unauthorized withholding</u> of data and it ensures the data backup through Business Continuity Planning (BCP) and <u>Disaster Recovery Planning (DRP).</u>*

   iii) *Availability can be affected <u>temporarily or permanently</u>, and a loss can be partial or complete from Temporary breakdowns, sustained and Permanent Outages, Denial of Service (DoS) attacks, <u>equipment failure</u>, and natural calamities are all threats to availability.*

d) <u>Privacy:</u>

   i) Privacy refers to the <u>personal information</u> should not be disclosed intentionally or accidentally. *It is also considered as one of the <u>important issues in Cloud</u>.*

   ii) *It should include both the <u>legal compliance</u> and <u>trusting maturity</u>.*

   iii) *The Cloud should be designed in such a way that it <u>decreases the privacy</u> risk.*

e) **Data Stealing or data loss:**

- **i)** In a Cloud, data stored anywhere, In such cases, an issue arises as data stealing.
- **ii)** Some of the Cloud providers do not use their own server, instead. They use servers from other service providers. So, there is a probability that the data is less secure and is more prone to the loss from external server.
- ***iii)*** *Back up policies such as Continuous Data Protection (CDP) should be implemented in order to avoid issues with data recovery in case of a sudden attack.*

f) **Application Security:** In cloud computing, the applications for data processing are stored on cloud thus face the issues of application security because cloud is accessible by large number of users.

g) **Software Isolation:**. Software isolation is to understand virtualization and other logical isolation techniques that the Cloud provider employs in its multi –tenant software architecture and evaluate the risks required for the organization.

h) **Identity Management and Access control:**

- **i)** Every organization normally uses its own rules for identity management and access controls.
- **ii)** The identity management provides a trust and shares the digital attributes between the Cloud provider and organization ensuring the protection against attackers.

i) **Cloud Architecture:** In the architecture of Cloud computing models, there should be a control over the security and privacy of the system.

j) **Governance:**

- **i)** Every organization has their own governance rules and policies to meet their business objectives.
- **ii)** It system of organization is normally designed to meet business objectives and employees of organizations are governed by rules and policies.
- **iii)** Extending these governing rules, policies and business objectives to cloud service provides system is also an issue or big challenge.

k) **Trust:**

- **i)** An organization will have direct control over IT resource and employees who are using these resources.
- **ii)** However extending these direct controls for cloud service providers employees and resource is not possible. Therefore, establishing trust between organizations and cloud service provides is also a big challenge.

l) **Legal Issues and Compliance:**

- **i)** One of the major challenge of cloud computing. There are various requirements relating to legal and regulatory compliance for information system, data protection and security.
- **ii)** The biggest issue is these laws vary from location to location and in cloud computing it is not known where data is physically stored and from where it will be accessed and used.
- **iii)** This requires a thorough knowledge of laws and compliance requirement from all perspectives.

m) **Audit:**

- **i)** Auditing is type of checking that ‘what is happening in the Cloud environment’.
- **ii)** It is an additional layer before the virtualized application environment, which is being hosted on the virtual machine to watch ‘what is happening in the system’.

n) **Incident Response:**

- **i)** It ensures to meet the requirements of the organization during an incident.
- **ii)** It ensures that the Cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident.

Q.No.29. Explain some pertinent issues in Cloud Computing? (OR) Explain various Implementation / Adaptation Issues in cloud computing (A) (PM, N14 - 6M)

SOME OF THE WELL-IDENTIFIED ISSUES STAND OUT WITH CLOUD COMPUTING:

1. **Threshold Policy:** This is a policy which defines cyclic use of any application e.g. use of credit card will rise sharply during the festival seasons and use will decrease significantly after the festival or buying season is over. The program processing the credit card should be having the capability to provide more instances or processing capabilities during buying seasons and deallocate these instances for other work when buying season is over. The threshold policy helps to detect sudden increase in the demand and results in the creation of additional instances to fill in the demand. It also determines how unused resources are to be deallocated and turned over to other work. Developing and implanting an appropriate threshold policy in the cloud program is a key issue with cloud computing.
2. **Interoperability:** There are no industry wide standards for interoperability of application and data between different cloud computing vendors. If a company outsources or creates applications with one cloud computing vendor, the company may find it difficult to change to another computing vendor that has proprietary Application Programming Interfaces (APIs) and different formats for importing and exporting data. It requires change of the format/logic in applications.
3. **Hidden Costs:** Cloud computing services providers do not reveals hidden costs such as higher chargers for data storage and use of applications during peak time and companies could experience slow services or latency in services particularly during heavy traffic.
4. **Unexpected Behavior:**_Companies may get unexpected results or outputs while using cloud services. Therefore, it is necessary that before migrating to cloud the companies should test the cloud services for correct output particularly during the heavy traffic or peak loads.
5. **Software Development in Cloud**: To develop software using high-end databases, the most likely choice is to use cloud server pools at the internal data corporate centre and extend resources temporarily for testing purposes. This allows project managers to control costs, manage security and allocate resources to clouds for a project. The project managers can also assign individual hardware resources to different cloud types: Web development cloud, testing cloud, and production cloud.
6. **Environment Friendly Cloud Computing:** One reason for cloud computing is that it may be more environment friendly. *It reduces the number of hardware components needed to run applications on the company's internal data centre and replacing them with cloud computing systems*

Q.No.30. What is Mobile computing? Explain the components of Mobile computing? (A) (PM, N15 RTP, N14, N16 MTP1)

1. Mobile Computing refers to the technology that allows transmission of data via a computer without having to be connected to a fixed physical link.
2. Mobile voice communication is widely established throughout the world and has a rapid increase in the number of subscribers to the various cellular networks over the last few years.
3. An extension of this technology is the ability to send and receive data across these cellular networks. This is the fundamental principle of mobile computing.
4. Mobile data communication has become a very important and rapidly evolving technology as it allows users to transmit data from remote locations to others either in remote or fixed locations.

Components of Mobile Computing: The key components of Mobile Computing are as follows:

a) **Mobile Communication:** This refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. This would include communication properties, protocols, data formats and concrete technologies.

b) **Mobile Hardware:** This includes mobile devices or device components that receive or access the service of mobility. They would range from Portable laptops, Smart Phones, Tablet PCs, and Personal Digital Assistants (PDA) that use an existing and established network to operate on. *The characteristics of mobile computing hardware are defined by the size and form factor, weight, microprocessor, primary storage, secondary storage, screen size and type, means of input, means of output, battery life, communications capabilities, expandability and durability of the device.*

c) **Mobile Software:** Mobile Software is the actual program that runs on the mobile hardware and deals with the characteristics and requirements of mobile applications. It is the operating system of that appliance and is the essential component that makes the mobile device operates.

Q.No.31. Explain the working of Mobile computing? (B) (MTP M17)

1. The user enters or access data using the application on handheld computing device.
2. Using one of several connecting technologies, the new data are transmitted from handheld to site's information system where files are updated and the new data are accessible to other system user.
3. Now both systems (handheld and site's computer) have the same information and are in sync.
4. The process work the same way starting from the other direction.
5. The process is similar to the way a worker's desktop PC access the organization's applications, except that user's device is not physically connected to the organization's system.
6. The communication between the user device and site's information systems uses different methods for transferring and synchronizing data, some involving the use of Radio Frequency (RF) technology.

Q.No.32. Explain the benefits of Mobile Computing? (A) (PM, M16 - 6M, N15 MTP2)

a) It provides mobile workforce with remote access to work order details, such as work order location, contact information, required completion date, asset history relevant warranties/service contracts.

b) It enables mobile sales personnel to update work order status in real-time, facilitating excellent communication.

c) It facilitates access to corporate services and information at any time, from anywhere.

d) It provides remote access to the corporate Knowledgebase at the job location.

e) It enables to improve management effectiveness by enhancing information quality, information flow, and ability to control a mobile workforce.

Q.No.33. Explain the Limitations of Mobile computing? (B) (N16-5M)

1. **Insufficient Bandwidth:** Mobile Internet access is generally slower than direct cable connections using technologies.
2. **Security Standards:** One can easily attack the VPN through a huge number of networks interconnected through the line.
3. **Power consumption:** When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power.
4. **Transmission interferences:** Weather, terrain, and the range from the nearest signal point can all interfere with signal reception. Reception in tunnels, some buildings, and rural areas is often poor.

5. **Potential health hazards:** People who use mobile devices while driving are often distracted from driving **are** thus assumed to be more likely involved in traffic accidents. Cell phones may interfere with sensitive medical devices.

6. **Human interface with device:** Screens and keyboards tend to be small, which may make them hard to use. Alternate input methods such as speech or handwriting recognition require training.

Q.No.34. Explain various issues in Mobile computing? (B) (PM)

1. **Security Issues**: Wireless networks have relatively more security requirements than wired network. A number of approaches have been suggested and also the use of encryption has been proposed.

   a) **Confidentiality:** Preventing unauthorized users from gaining access to critical information of any particular user.

   b) **Integrity:** Ensures unauthorized modification, destruction or creation of information cannot take place.

   c) **Availability:** Ensuring authorized users getting the access they require.

   d) **Legitimate:** Ensuring that only authorized users have access to services.

   e) **Accountability:** Ensuring that the users are held responsible for their security related activities by arranging the user and his/her activities are linked if and when necessary.

2. **Bandwidth**: Bandwidth utilization can be improved by logging and compression of data before transmission. The technique of caching frequently accessed data items can play an important role in reducing contention in narrow bandwidth wireless networks. The cached data can help improve query response time. .

3. **Location Intelligence**: A mobile computer must be able to switch from infrared mode to radio mode as it moves from indoors to outdoors. A small movement may result in a much longer path if cell or network boundaries are crossed. It will also lead to updating of the location dependent information.

4. **Power Consumption**: Mobile Computers will rely on their batteries as the primary power source. Batteries should be ideally as light as possible but at the same time they should be capable of longer operation times. Power consumption should be minimized to increase battery life.

5. **Revising the technical architecture**: Mobile users are demanding and are important to the business world. To provide complete connectivity among users; the current communication technology must be revised to incorporate mobile connectivity.

6. **Reliability, coverage, capacity, and cost**: At present; wireless network is less reliable, have less geographic coverage and reduced bandwidth, are slower, and cost more than the wired-line network services. It is important to find ways to use this new resource more efficiently by designing innovative applications.

7. **Integration with legacy mainframe and emerging client/server applications**: Application development paradigms are changing. As a result of the IT industry's original focus on mainframes, a huge inventory of applications using communications interfaces that are basically incompatible with mobile connectivity have been accumulated.

8. **End-to-end design and performance**: Since mobile computing involves multiple networks (including wired) and multiple application server platforms; end-to-end technical compatibility, server capacity design, and network response time estimates are difficult to achieve.

9. **Business challenges**: Mobile computing also faces business challenges. This is due to the lack of trained professionals to bring the mobile technology to the general people and development of pilot projects for testing its capabilities.

Q.No.35. Write about Green IT or Green Computing? (A) (PM)

1. Green computing or Green IT refers to the study and practice of environmentally sustainable computing or IT.
2. It is the study and practice of establishing / using computers and IT resources in a more efficient and environmentally friendly and responsible way.
3. Computers consume a lot of natural resources, from the raw materials needed to manufacture them, the power used to run them, and the problems of disposing them at the end of their life cycle.
4. This can include "designing, manufacturing, using, and disposing of computers, servers and associated subsystems - such as monitors, printers, storage devices, and networking and communications systems - efficiently and effectively with minimal or no impact on the environment".
5. The objective of Green computing is to reduce the use of hazardous materials, maximize energy efficiency during the product's lifetime, and promote the recyclability or biodegradability of defunct products and factory waste.
6. Such practices include the implementation of energy-efficient Central Processing Units (CPUs), servers and peripherals as well as reduced resource consumption and proper disposal of electronic waste (e-waste).

Q.No.36. Explain the Green Computing best practices? (A) (OR)
What are your recommendations for efficient use of computers and IT resources to achieve the objectives of "Green computing". (OR)
(PM, N14 - 5M, M15-4M, N14, M17, N16 RTP, N15 MTP2)
The work habits of computer users and businesses can be modified to minimize adverse impact on the global environment'. Discuss some of such steps, which can be followed for Green IT.

The work habits of computer users and businesses can be modified to minimize adverse impact on the global environment.

Some of such steps for Green IT include the following:

a) **Develop a sustainable Green Computing plan:**

i) Involve stakeholders to include checklists, recycling policies, recommendations for disposal of used equipment, government guidelines and recommendations for purchasing green computer equipment in organizational policies and plans;

ii) Encourage the IT community for using the best practices and encourage them to consider green computing practices and guidelines.

iii) Include power usage, reduction of paper consumption, as well as recommendations for new equipment and recycling old machines in organizational policies and plans.

iv) Use cloud computing so that multiple organizations share the same computing resources, thus increasing the utilization by making more efficient use of hardware resources.

b) **Recycle**

i) Dispose e-waste according to central, state and local regulations ;

ii) Discard used or unwanted electronic equipment in a convenient and environmentally responsible manner as computers emit harmful emissions;

iii) Manufacturers must offer safe end-of-life management and recycling options when products become unusable; and Recycle computers through manufacturer's recycling services.

c) **Make environmentally sound purchase decisions**

i) Purchase of desktop computers, notebooks and monitors based on environmental attributes;

ii) Provide a clear, consistent set of performance criteria for the design of products;

iii) Recognize manufacturer efforts to reduce the environmental impact of products by reducing or eliminating environmentally sensitive materials, designing for longevity and reducing packaging materials; and

iv) Use Server and storage virtualization that can help to improve resource utilization, reduce energy costs and simplify maintenance.

d) Reduce Paper Consumption

i) Reduce paper consumption by use of e-mail and electronic archiving

ii) Use of "track changes" feature in electronic documents, rather than redline corrections on paper;

iii) Use online marketing rather than paper based marketing because e-mail providers provides online accessing and support.

iv) While printing documents; make sure to use both sides of the paper, recycle regularly, use smaller fonts and margins, and selectively print required pages.

e) Conserve Energy

i) Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors;

ii) Develop a thin-client strategy wherein thin clients are smaller, cheaper, simpler for manufacturers to build than traditional PCs or notebooks and most importantly use about half the power of a traditional desktop PC;

iii) Use notebook computers rather than desktop computers whenever possible.

iv) Use the power-management features to turn off hard drives and displays after several minutes of inactivity;

v) Power-down the CPU and all peripherals during extended periods of inactivity ;

vi) Try to do computer-related tasks during contiguous, intensive blocks of time, leaving hardware off at other times;

vii) Power-up and power-down energy-intensive peripherals such as laser printers according to need;

viii) Employ alternative energy sources for computing workstations, servers, networks and data centers; and

ix) Adapt more of Web conferencing offers instead of travelling to meetings in order to go green and save energy.

Q.No.37. Explain relevant facts about Green IT? (B)

1. All businesses are increasingly dependent on technology, and small business is no exception.
2. We work on our PCs, notebooks and smart phones all day, connected to servers running 24x7.
3. Since the technology refresh cycle is fast, these devices quickly become obsolete, and at some point — more often sooner than later — we dispose of old devices and replace them with new ones.
4. We use massive quantities of paper and ink to print documents, many of which we promptly send to the circular file.
5. In the process, most businesses waste resources, in the form of energy, paper, money and time — resources we could invest to develop new products or services, or to hire and train employees.
6. Even if we aren't a tree hugger, it makes good business sense to green our IT environment and culture.
7. Many IT vendors have major initiatives underway to green their products, services and practices. it include building computers with more environmentally friendly materials, designing them to be consume less energy, providing recycling programs to dispose of old systems, developing virtualization and cloud computing alternatives, and providing tips to businesses that want to go green.

Q.No.38. Explain Green IT security services and challenges? (B)

1. IT solutions providers are offering green security services in many ways.
2. What to look in green security products, the challenges in the security services market and how security services fare in a recession.
3. If administered properly with other green computing technologies, green security can be a cost - efficient and lucrative green IT service for solution providers.
4. The basic aim is to increase the customer's energy savings through green security services and assess that 'how sustainable computing technology can immediately help the environment'.
5. Green IT services present many benefits for clients as well as providers, but knowing 'how to evaluate a client's infrastructure to accommodate green technology is really a vital issue'.
6. Moreover, apart from the common security issues, the green security emphasizes the role of security tools, methods and practices that reduce a company's environmental impact.
7. But to estimate the scope, to cope with the lack of green security services in the market and get advice on conserving power and purchasing switches is very important and needs a high level of sensitivity.
8. Learning about the challenges of implementing green security and the best practices is a major hope, as the artifacts are still evolving.

Q.No.39. Write about BYOD? Explain its advantages? (A) (PM, N15 RTP)

1. BYOD (Bring Your Own Device) refers to business policy that allows employees to use their preferred computing devices, like smart phones and laptops for business purposes.
2. It means employees are welcome to use personal devices (laptops, smart phones, tablets etc.) to connect to the corporate network to access information and application.
3. The BYOD policy has rendered the workspaces flexible, empowering employees to be mobile and giving them the right to work beyond their required hours.
4. The continuous influx of readily improving technological devices has led to the mass adoption of smart phones, tablets and laptops, challenging the long- standing policy of working on company - owned devices.

Advantages of BYOD: **(N16-4M)**

a) **Happy Employees:** Employees love to use their own devices when at work. This also reduces the number of devices an employee has to carry.

b) **Lower IT budgets:** The employees could involve financial savings to the organization since employees would be using the devices they already possess, thus reducing the cost of the organization in providing devices to them.

c) **IT reduces support requirement:** IT department does not have to provide end user support and maintenance for all these devices resulting in cost savings.

d) **Early adoption of new Technologies:** Employees are generally proactive in adoption of new technologies that result in enhanced productivity of employees leading to overall growth of business.

e) **Increased employee efficiency:** The efficiency of employees is more when the employee works on their own device.

Q.No.40. What is BYOD and what are its key threats? (OR) Explain emerging BYOD Threats? (OR) If the employees of the company are allowed to use personal devices such as laptop, smart phones tablets etc. to connect and access the data, what could be the security risks involved? Classify and elaborate such risks. (A) (N15- 5M, M16 RTP, N15 MTP1)

Every business decision is accompanied with a set of threats and so is BYOD program also.

A BYOD program that allows access to corporate network, emails, client data etc. is one of the top security concerns for enterprises.

Overall, these risks can be classified into four areas:

a) **Network Risks:**

- i) It is normally exemplified and hidden in 'Lack of Device Visibility'.
- ii) When company-owned devices are used by all employees within an organization, the organization's IT practice has complete visibility of the devices connected to the network.
- iii) This helps to analyze traffic and data exchanged over the Internet.
- iv) As BYOD permits employees to carry their own devices (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the network.
- v) It is possible that some of the devices may cause the destructive operations such as inserting viruses, although security checks will be there but that may miss some of the destructive operations for outside devices.

b) **Device Risks:**

- i) It is known as 'Loss of Devices'.
- ii) A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information.
- iii) Data lost from stolen or lost devices ranks as the top security threats as per the rankings released by Cloud Security Alliance.
- iv) With easy access to company emails as well as corporate intranet, company trade secrets can be easily retrieved from a misplaced device.

c) **Application Risks:**

- i) It is normally exemplified and hidden in 'Application Viruses and Malware'.
- ii) A related report revealed that a majority of employees' phones and smart devices that were connected to the corporate network weren't protected by security software.
- iii) With an increase in mobile usage, mobile vulnerabilities have increased concurrently.
- iv) Organizations are not clear in deciding that 'who is responsible for device security – the organization or the user'.

d) **Implementation Risks:**

- i) It is known as 'Weak BYOD Policy'.
- ii) It is important that the organization should have a strong BYOS policy, this policy should be effectively implemented as well.
- iii) Any weakness in this implementation may result in big loss to organization.

Q.No.41. Explain Social media? (B)

1. There are two types of networks: physical and logical networks.
2. Physical network is a network of computers and devices.
3. Logical network is network of communities and human beings to exchange ideas and information with each others. These logical networks are known as social networks or social media.
4. Social media refers to the means of interaction among the people in which they create, share, and exchange information and ideas in virtual communities and networks.
5. There are multiple types of social networks due to different human interests and professions. This can range from a network of researchers, to a network of doctors to a network of academics etc.
6. Each type of network has its own focus area, member size, geographical spread, societal impact and objective.
7. Managing such networks is not only complicated but requires lot of collective efforts and collaboration.
8. A social network is usually created by a group of individuals, who have a set of common interests and objectives.
9. There are usually a set of network formulators followed by a broadcast to achieve the network membership.
10. This happens both in public and private groups depending upon the confidentiality of the network.
11. Success of a social network mainly depends on contribution, interest and motivation of its members along with technology backbone or platform support that makes the life easier to communicate and exchange information to fulfill a particular communication need.
12. *Implementing social networks and sustaining them is one of the biggest challenges and people have formulated many mechanisms in the past to keep alive such networks.*

Q.No.42. Write about Web 2.0? (B) (PM)

1. Web 2.0 is the term given to describe a second generation of the World Wide Web that is focused on the ability for people to collaborate and share information online.
2. The two major contributors of Web 2.0 are the technological advances enabled by Ajax (Asynchronous JavaScript and XML) and other applications and other applications such as RSS (Really Simple Syndication) and Eclipse that support the user interaction and their empowerment in dealing with the web.
3. Web 2.0 basically refers to the transition from static HTML Web pages to a more dynamic Web that is more organized and is based on serving Web applications to users.
4. Other improved functionality of Web 2.0 includes open communication with an emphasis on Web-based communities of users, and more open sharing of information.
5. One of the most significant differences between Web 2.0 and the traditional World Wide Web (Web 1.0) is that migration is from the "read-only web" to "read-write web".
6. Blogs, wikis, and Web services are all seen as components of Web 2.0.
7. *Web 2.0 tries to tap the power of humans connected electronically through its new ways at looking at social collaboration.*
8. The main agenda of Web 2.0 is to connect people in numerous new ways and utilize their collective strengths, in a collaborative manner.
9. *In this regard, many new concepts have been created such as Blogging, Social Networking, Communities, Mashups, and Tagging.*

Q.No.43. Explain the components of web 2.0 for Social networks? (OR) Describe the major components of web 2.0 for Social networks. (A) (M16- 4M, N15 RTP)

Major components that have been considered in Web 2.0 include the following:

a) **Communities:** These are an online space formed by a group of individuals to share their thoughts, ideas and have a variety of tools to promote Social Networking.

b) **RSS-generated Syndication:** RSS is a format for syndicating web content that allows feed the freshly published web content to the users through the RSS reader.

c) **Blogging:** A blog is a journal, diary, or a personal website that is maintained on the internet, and it is updated frequently by the user. Blogging allows a user to make a post to a web log or a blog. Blogs give the users of a Social Network the freedom to express their thoughts in a free form basis and help in generation and discussion of topics.

d) **Wikis:** A Wiki is a set of co-related pages on a particular subject and allow users to share content. Wikis replace the complex document management systems and are very easy to create and maintain.

e) **Usage of Ajax and other new technologies:** Ajax is a way of developing web applications that combines XHTML and CSS (Cascading Style Sheets) standards-based presentation that allows the interaction with the web page and data interchange with XML (eXtensible Markup Language) and XSLT (eXtensible Stylesheet Language Transformations).

f) **Folksonomy:** This allows the free classification of information available on the web, which helps the users to classify and find information, using approaches such as tagging.

g) **File Sharing/Podcasting:** This is the facility, which helps users to send their media files and related content online for other people of the network to see and contribute.

h) **Mashups:** This is the facility, by using which people on the internet can congregate services from multiple vendors to create a completely new service.

Q.No.44. Write about types and behavior of Social networks? (OR) Explain various social networks? (A) (M16 MTP1)

1. Social networks exist in various domains-within and outside organizations, within and outside geographical boundaries, within and outside social boundaries and many other areas.

2. **The main categories are:**

   a) **Social Contact Networks:** These most popular types of networks are formed to keep contact with friends and family. They have all components of Web 2.0 like blogging, tagging, wikis, and forums. Examples of these include Orkut, Facebook and Twitter.

   b) **Study Circles:** These are social networks dedicated for students, where they can have areas dedicated to student study topics, placement related queries and advanced research opportunity gathering. These have components like blogging and file sharing. Examples of these include, Fledge Wing and College Tonight.

   c) **Social Networks for Specialist Groups:** These types of social networks are specifically designed for core field workers like doctors, scientists, engineers, members of the corporate industries. A very good example for this type of network is LinkedIn.

   d) **Networks for Fine Arts:** These types of social networks are dedicated to people linked with music, painting and related arts and have lots of useful networking information for all aspiring people of the same line.

   e) **Police and Military Networks:** These types of networks, though not on a public domain, operate much like social networks on a private domain due to the confidentiality of information.

   f) **Sporting Networks:** These types of social networks are dedicated to people of the sporting fraternity and have a gamut of information related to this field. Examples of these include Athlinks.

g) **Mixed Networks:** There are a number of social networks that have a subscription of people from all the above groups and is a heterogeneous social network serving multiple types of social collaboration.

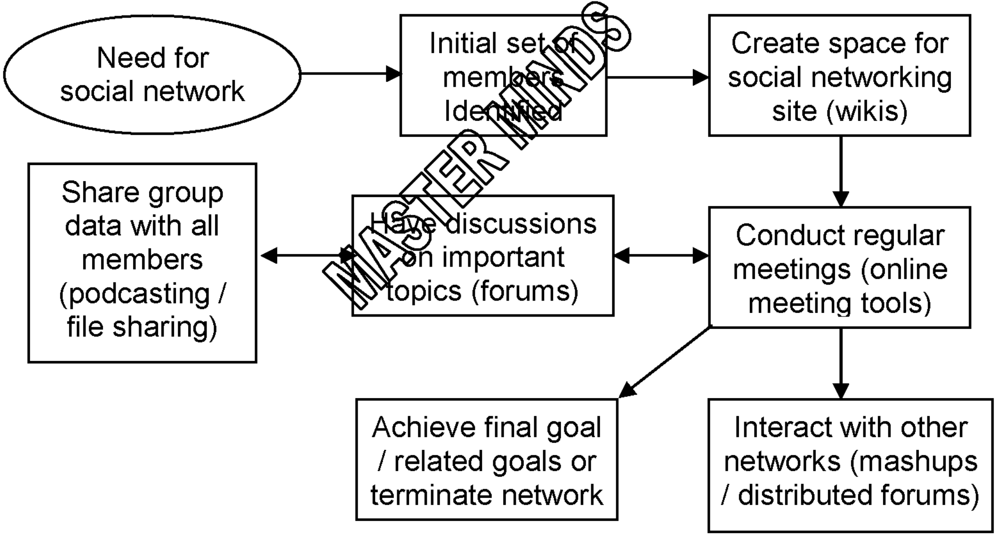
h) **Social Networks for the 'inventors':** These are the social networks for the people who have invented the concept of social networks, the developers and architects that have developed the social networks. Examples include Technical Forums and Mashup centres.

i) **Shopping and Utility Service Networks:** The present world of huge consumerism has triggered people to invest in social networks, which will try to analyze the social behavior and send related information for the same to respective marts and stores.

j) **Others:** Apart from the networks outlined above, there are multiple other social networks, which serve huge number of the internet population in multiple ways.

Q.No.45. Explain the life cycle of social networks? (B) (N15 MTP1)

1. The concept of social net works and the components of Web 2.0, which are significant for social networks.
2. For any social network, there are a number of steps in its life cycle.
3. In each of the life cycle step of an online social network, Web 2.0 concepts have a great influence.
4. Consider the diagram below for social network life cycle.



Need for social network
Initial set of members Identified
Create space for social networking site (wikis)
Share group data with all members (podcasting / file sharing)
Have discussions on important topics (forums)
Conduct regular meetings (online meeting tools)
Achieve final goal / related goals or terminate network
Interact with other networks (mashups / distributed forums)

5. For all the steps in the life cycle, web 2.0 has provided tools and concepts which are not only cost effective and easy to implement but also to achieve desired objectives.
6. Web 2.0 provides excellent communication mechanisms concepts like blogging and individual email filtering too keep everyone in the network involved in the day to day activities of the networks.

Q.No.46. Explain various applications of Web 2.0. (A)

Social networks built on Web 2.0 concepts has become so cost affordable and easy to use that more and more people are migrating to this wave.

Web 2.0 finds applications in different fields, some of them are:

a) **Social Media:** It is an important application of web 2.0. It provides a basic way in which people communicate and share information. It also offers a number of online tools and platforms that can be used by the users to share their data, perspectives, and opinions among other user communities.

b) **Marketing:** It allows the marketers to collaborate with consumers on various aspects such as product development, service enhancement, and promotion. Consumer-oriented companies use networks such as Twitter and Face book as common elements of multichannel promotion of their products.

c) **Education:** Web 2.0 technologies can help the education scenario by providing students and faculty with more opportunities to interact and collaborate with their peers. By utilizing the tools of Web 2.0, the students get the opportunity to share what they learn with other peers by collaborating with them.

Q.No.47. Explain the benefits and challenges for social networks using web 2.0? (A)

Benefits:

a) It provides a platform where users of the network need not to worry about the implementation of underlying technology at a very affordable cost and a very easy pickup time.

b) Concepts of Web 2.0 like blogging are some things that people do on a day -to-day basis and no new knowledge skills are required.

c) Web 2.0 techniques are very people centric activities and its adaptation is very fast.

d) People are coming much closer to another and all social and geographical boundaries are being reduced at lightning speed*, which is one of the biggest sustenance factors for any social network.*

e) Using Web 2.0 also increases the social collaboration to a very high degree and this in turn helps in achieving the goals for a social network.

Challenges:

a) One of the major aspects is data security and privacy and in such public domains, there is a huge chance of data leak and confidentiality loss because there are usually no centrally mandated administrative services to take care of such aspects.

b) Privacy of individual users also arises and can create a huge problem if malicious users somehow manage to perpetuate the social networks.

c) This is more important for public utility networks like doctors and police.

d) A majority of the social networks are offline, and for bringing these under the purview of online social networks, a lot of education and advertising needs to be done, which itself becomes a cost burden, when the people involved are not computer literate.

e) This becomes more viable in the areas of the world that are developing and do not have the basic amenities.

f) The fact is that these areas are the ones that can benefit the most using social networks in an online mode and a huge amount of effort would be needed to help them using the technologies.

Q.No.48. Explain Web 3.0? Explain the major components of Web 3.0. (A)

1. The Web 3.0 also known as Semantic Web, which generated data without direct user interaction.
2. Web 3.0 is considered as the next logical step in the evolution of the Internet and Web technologies.
3. It allows drag and drop mash-ups, widgets, user behavior, user engagement, and consolidation of dynamic web contents depending on the interest of the individual users.
4. It uses the "Data Web" Technology, which features the data records that are publishable and reusable on the web through query-able formats.
5. An example of typical Web 3.0 application is the one that uses content management systems along with artificial intelligence.

6. *These systems are capable of answering the questions posed by the users, because the application is able to think on its own and find the most probable answer, depending on the context, to the query submitted by the user.*

7. Web 3.0 can also be described as a "machine to user" standard in the internet.

Major components of Web 3.0: **(N16-4M, RTP M17)**

a) Semantic Web: It provides the web user a common framework that could be used to share and reuse the data across various applications, enterprises, and community boundaries.

b) Web Services: It is a software system that supports computer-to-computer interaction over the Internet. For example - the popular photo-sharing website Flickr provides a web service that could be utilized and allows searching for images.

Q.No.49. Write short notes on mobile computing and BYOD. (RTP N15)

1. Mobile Computing and Buy Your Own Devices (BYOD): Mobile computing, including BYOD is the single most radical shift in business since the PC revolution of the 1980s.
2. Over the next decade, it will have a huge impact on how people work and live, how companies operate, and on the IT infrastructure.
3. These services will focus on the issues and opportunities surrounding the new way to communicate and consume computing services. Mobile computing is not just PCs on the move.
4. Mobile devices such as smart phones, tablets, and the iPod Touch, the last PDA standing are a radically different kind of devices, designed from the ground up as end points of data networks both internal corporate networks and the Internet rather than primarily as stand-alone devices.
5. They are optimized for mobility, which means that they have to be light, easy to handle, and maximize battery life.
6. Where laptops has a three hour battery life, the tablet and smartphone regularly run 12 hours or more between charging and serve as windows into the Cloud.

THE END