PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

Concepts of Governance and Management of Information Systems

1. "The success of the process of ensuring business value from the 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 risks is implemented." Explain some of the key metrics which can be used for such evaluation.
2. Discuss the seven enablers of COBIT 5.
3. Write short note on Internal Controls as per Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Information System Concepts

4. What is Executive Information System (EIS)? Explain the major characteristics of an EIS.
5. "Decision Support Systems are widely used as part of an Organization's Accounting Information system". Give examples to support this statement.
6. Discuss some major characteristics of Computer based Information Systems in brief.

Protection of Information Systems

7. Discuss in detail the following:
   (a) "Data Resource Management Controls" under Managerial Controls.
   (b) "Systems Development Management Controls" under Managerial Controls.
8. Discuss Logical Access Controls across the system in brief.
9. Discuss the arrangements a company XYZ should emphasize in order to tighten its Physical Security for protecting its IT assets.

Business Continuity Planning and Disaster Recovery Planning

10. Discuss broadly the administrative procedures that need to be considered during any BCP Audit.
11. 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?
12. Discuss the major areas that form a part of Disaster Recovery Planning (DRP) Document.

Acquisition, Development and Implementation of Information Systems

13. What are the characteristics of a good coded application and program?
14. (a) Mention different functions of steering Committee under SDLC.

(b) "Maintaining the system is an important aspect of SDLC". Considering this statement; list out various categories of System Maintenance in SDLC.

15. Discuss various areas that should be considered while designing systems input.

Auditing of Information Systems

16. What do you understand by Control Risk? Mention different types of information which auditors may collect using System Control Audit Review File (SCARF)?

17. Discuss the Accounting and Operations Audit Trails with respect to Communication Controls.

Information Technology Regulatory Issues

18. Discuss the provision given in IT (Amendment) Act 2008, that gives power to issue directions for blocking for public access of any information through any computer resource?

19. Discuss Information Technology Infrastructure Library (ITIL) Service Lifecycle.

Emerging Technologies

20. Discuss the similarities and differences between Cloud Computing and Grid Computing.

Short Note Based Questions

21. Write short notes on following:
    (a) Phishing, Hacking and Cracking
    (b) Auditor's Selection Norms
    (c) Mobile Computing and Buy Your Own Devices (BYOD)
    (d) General Controls
    (e) Data Flow Diagram (DFD)

22. Differentiate between the following:
    (a) Cold Site and Hot Site
    (b) Phased Changeover and Pilot Changeover
    (c) Structured English and Flowchart
    (d) Inherent Risk and Detection Risk
    (e) Emergency Plan and Recovery Plan

Questions based on the Case Studies

23. A manufacturing company ABC having information flow within departments, operating with in-house developed software till now. Its profit margins are very low due to inefficiency and disorganized work culture. To survive in the competitive market, it has to

improve the efficiency of its internal processes and synchronize onto streamlined business processes so that work culture is improved. Hence it has decided by the top management to purchase and implement real time software. In order to improve its margin, it is decided to transact with suppliers and customer electronically and maintain all records in electronic form. They furnish all books of accounts and report to the controller. Security of information is a key activity of this process which must be taken care of from the beginning. As a member of implementation team, you are required to answer the following:

(a) Explain the major points for evaluation of effectives Management Information System (MIS).

(b) Explain the advantages of Business Continuity Management (BCM).

(c) Explain the penalty for failure to furnish information return under Section 44 of IT Act, 2000.

(d) Explain the various user related issues in achieving the system development objectives.

24. XYZ Technical University, a newly formed university, decided to launch a web based knowledge portal to facilitate their students of distance education for different courses. It proposed to upload the course materials, e - lectures and e-reference books. It is expected to provide various resources easily on anytime and anywhere basis. Therefore, an initial study or investigation under all dimensions was done. As a part of this, the management of the university invited various technical experts for a capable and good solution as per the requirements and guidelines of the university. Also the University decided to encourage people to collaborate and share information online through social networks.

(a) According to you as an IS Auditor, what are the validation methods for approving the vendors' proposals?

(b) If you consider Web 2.0 as an ideal platform for implementing and helping social networks to grow, what are the major components of Web 2.0?

(c) The university will facilitate the communication system to interact with their students effectively and economically by using Electronic Mail systems. What are the features of the Electronic Mail System?

(d) What are the important backup options that should be considered by security administrators?

25. ASK International proposes to launch a new subsidiary to provide e-consultancy services for organizations throughout the world, to assist them in system development, strategic planning and e-governance areas. The fundamental guidelines, programmes modules and draft agreements are all preserved and administered in the e-form only.

The company intends to utilize the services of a professional analyst to conduct a preliminary investigation and present a report on smooth implementation of the ideas of

the new subsidiary. Based on the report submitted by the analyst, the company decides to proceed further with three specific objectives (i) reduce operational risk, (ii) increase business efficiency and (iii) ensure that information security is being rationally applied.

(a) What are the two primary methods through which the analyst would have collected the data?

(b) To retain their electronic records for specified period, what are the conditions laid down by Section 7, Chapter III of Information Technology Act, 2000?

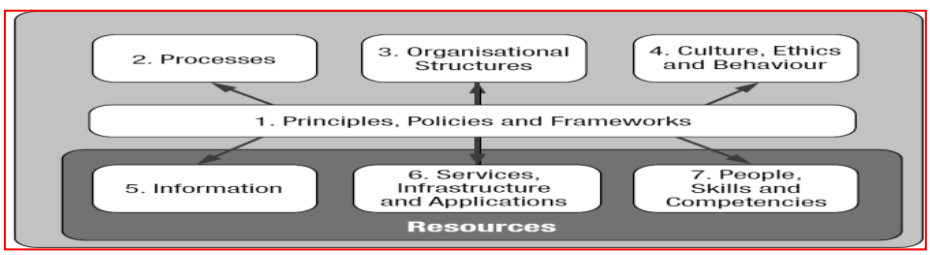
SUGGESTED ANSWERS/HINTS

1. "The success of the process of ensuring business value from the 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 risks is implemented." Some of the key metrics, which can be used for such evaluation, are as follows:

- Percentage of IT enabled investments where benefit realization monitored through full economic life cycle;
- Percentage of IT services where expected benefits realized;
- Percentage of IT enabled investments where claimed benefits met or exceeded;
- Percentage of investment business cases with clearly defined and approved expected IT related costs and benefits;
- Percentage of IT services with clearly defined and approved operational costs and expected benefits; and
- Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of IT financial information.

2. **Enablers of COBIT 5:** Enablers are factors that individually and collectively, influence whether something will work; in case of COBIT 5, Governance and Management over enterprise IT. The COBIT 5 framework describes seven categories of enablers, which are shown in Figure and discussed as below:

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



Seven Enablers of COBIT 5

(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 Behaviour** of individuals and of the enterprise are 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.

3. As per Committee of Sponsoring Organizations of the Treadway Commission (COSO), Internal Control is comprised of five interrelated components:

- **Control Environment:** 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.
- **Risk Assessment:** Each business process comes with various risks. A control environment must include an assessment of the risks associated with each business process.
- **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.
- **Information and Communication:** Associated with control activities are information and communication systems. These enable an organization to capture and exchange the information needed to conduct, manage, and control its business processes.
- **Monitoring:** The internal control process must be continuously monitored with modifications made as warranted by changing conditions.

4. **Executive Information Systems (EIS) –** It is sometimes referred to as an Executive Support System (ESS). It serves the strategic level i.e. top level managers of the organization. ESS creates a generalized computing and communications environment rather than providing any preset applications or specific competence.

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

- EIS is a Computer-based-information system that serves the information need of top executives.
- EIS enables users to extract summary data and model complex, problems without the need to learn query languages statistical formulas or high computing skills.
- EIS provides rapid access to timely information and direct access to management reports.
- EIS is capable of accessing both internal and external data.
- EIS provides extensive online analysis tool like trend analysis, market conditions etc.
- EIS can easily be given as a DSS support for decision making.

5. Decision Support Systems are widely used as a part of an organization's Accounting Information System. The complexity and nature of decision support systems vary. Many are developed in-house using either a general type of decision support program or a spreadsheet program to solve specific problems. Below are several illustrations:

- **Cost Accounting System:** The health care industry is well known for its cost complexity. Managing costs in this industry requires controlling costs of supplies, expensive machinery, technology, and a variety of personnel. Cost accounting applications help health care organizations calculate product costs for individual procedures or services. Decision support systems can accumulate these product costs to calculate total costs per patient. Health care managers may combine cost accounting decision support systems with other applications, such as productivity systems. Combining these applications allows managers to measure the effectiveness of specific operating processes
- **Capital Budgeting System:** Companies require new tools to evaluate high-technology investment decisions. Decision makers need to supplement analytical techniques, such as net present value and internal rate of return, with decision support tools that consider some benefits of new technology not captured in strict financial analysis. Example- Auto Man is a DSS designed to support decisions about investments in automated manufacturing technology that allows decision makers to consider financial, nonfinancial, quantitative, and qualitative factors in their decision-making processes.
- **Budget Variance Analysis System:** Financial institutions rely heavily on their budgeting systems for controlling costs and evaluating managerial performance. One institution uses a computerized decision support system to generate monthly variance reports for division comptrollers. The system allows these comptrollers to graph, view, analyze, and annotate budget variances, as well as create additional one-and five-year budget projections using the forecasting tools provided in the

system. The decision support system thus helps the comptrollers create and control budgets for the cost-center managers reporting to them.

- **General Decision Support System:** Some planning languages used in decision support systems are general purpose and therefore have the ability to analyze many different types of problems. In a sense, these types of decision support systems are a decision-maker's tools. The user needs to input data and answer questions about a specific problem domain to make use of this type of decision support system. An example is a program called Expert Choice that supports a variety of problems requiring decisions. The user works interactively with the computer to develop a hierarchical model of the decision problem. The decision support system then asks the user to compare decision variables with each other. For instance, the system might ask the user how important cash inflows are versus initial investment amount to a capital budgeting decision. The decision maker also makes judgments about which investment is best with respect to these cash flows and which requires the smallest initial investment. Expert Choice analyzes these judgments and presents the decision maker with the best alternative.

6. Major characteristics of Computer based Information Systems (CBIS) are as follows:

- All systems work for predetermined objectives and the system is designed and developed accordingly.
- In general, a system has a number of interrelated and interdependent subsystems or components. No subsystem can function in isolation; it depends on other subsystems for its inputs.
- If one subsystem or component of a system fails; in most of the cases, the whole system does not work. However, it depends on 'how the subsystems are interrelated'.
- The way a subsystem works with another subsystem is called interaction. The different subsystems interact with each other to achieve the goal of the system.
- The work done by individual subsystems is integrated to achieve the central goal of the system. The goal of individual subsystem is of lower priority than the goal of the entire system.

7. (a) **Data Resource Management Controls:** Data is a critical resource that must be managed properly and therefore, accordingly, centralized planning and control are implemented. For data to be managed better; users must be able to share data that 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. Further it must be possible to modify data fairly easily and the integrity of the data be preserved. If data repository system is used properly, it can enhance data and application system reliability. It must be controlled carefully, however, because the consequences are serious if the data definition is compromised or destroyed. 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.

These Controls fall in two categories:

- **Access Controls:** These are designed to prevent unauthorized individual from viewing, retrieving, computing or destroying the entity's data. User Access Controls are established through passwords, tokens and biometric Controls; and through Data Encryption that keeps the data in database in encrypted form.
- **Back-up Controls:** These ensure the availability of system in the event of data loss due to unauthorized access, equipment failure or physical disaster; the organization can retrieve its files and databases. 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:
    - **Dual recording of data:** Under this strategy, two complete copies of the database are maintained and are concurrently updated.
    - **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. The dump may be scheduled.
    - **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.
    - **Logging changes to the data:** This involves copying a record each time it is changed by an update action. The changed record can be logged immediately before the update action changes the record, immediately after, or both.

(b) Systems Development Management Controls: System Development controls are targeted to ensure that proper documentations and authorizations are available for each phase of the system development process. It includes controls at controlling new system development activities which are as follows:

- **System Authorization Activities:** All systems must be properly authorized to ensure their economic justification and feasibility. As with any transaction, system's authorization should be formal.
- **User Specification Activities:** The user can create a detailed written description of the logical needs that must be satisfied by the system. The creation of a user specification document often involves the joint efforts of the user and systems professionals.
- **Technical Design Activities:** The technical design activities in the System Development Life Cycle (SDLC) translate the user specifications into a set of

detailed technical specifications of a system that meets the user's needs. The scope of these activities includes systems analysis, general systems design, feasibility analysis, and detailed systems design.

- **Internal Auditor's Participation:** The auditor should become involved at the inception of the SDLC process to make conceptual suggestions regarding system requirements and controls. Auditor's involvement should be continued throughout all phases of the development process and into the maintenance phase.
- **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.
- **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).

To conclude, we can say that the Systems Development Management has responsibility for the functions concerned with analyzing, designing, building, implementing, and maintaining information systems. Three different types of audits that may be conducted during system development process are discussed below.

- **Concurrent Audit:** Auditors are members of the system development team and assist the team in improving the quality of systems development for the specific system.
- **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.
- **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 or systems effectiveness and efficiency.

Note: *Referring to the relevant January 2015 edition; students are advised to read the "**Section 3.9.6 Data Management Controls**" subsequent to the "**Section 3.7.4 Data Resource Management Controls**" under the topic "**Data Resource Management Controls**" and "**Section 3.9.7 System Development Controls**" subsequent to "**Section 3.7.2 System Development Management Controls**" under the topic "**System Development Management Controls**". Both the controls are to be considered as a part of "**Section 3.7 Managerial Controls and their Categories**".*

8. **Logical Access Controls:** Logical Access Controls serve as one of the means of information security. 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:

   - Used by an application (Data at Process);
   - Stored in some medium (Back up) (Data at Rest); or
   - It may be in transit (being transferred from one location to another).

   Logical access controls is all about protection of these assets wherever they reside. The details are given below:

   (i) User Access Management

   - **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.
   - **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.
   - **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.
   - **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.

   (ii) User Responsibilities: User awareness and responsibility is also an important factor:

   - **Password use:** Mandatory use of strong passwords to maintain confidentiality.
   - **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.

   (iii) 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:

- **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.
- **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.
- **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
- **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.
- **Security of network services:** The techniques of authentication and authorization policy should be implemented across the organization's network.

(iv) Operating System Access Control: Operating System provides the platform for an application to use various Information System resources and perform the specific business function. 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.

Automated terminal identification; Terminal log-on procedures, User identification and authentication; Password management system; Use of system utilities; Duress alarm to safeguard users; Terminal time out and limitation of connection time are some of vital steps to control unlimited access.

(v) Application and Monitoring System Access Control:

- **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.
- **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.
- **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.
- **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.

- **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.

(vi) Mobile Computing: 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.

9. 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. Similarly, unauthorized access to secret records of the organization can cause leakage of vital information. Hence, there is a great need for physical security of the computer system. Physical security includes arrangements that are discussed below:
- **Fire Damage:** 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 given below:
  - Both automatic and manual fire alarms are placed at strategic locations;
  - A control panel may be installed which shows where in the location an automatic or manual alarm has been triggered;
  - Besides the control panel, master switches may be installed for power and automatic fire suppression system;
  - Manual fire extinguishers can be placed at strategic locations;
  - Fire exits should be clearly marked. When a fire alarm is activated, a signal may be sent automatically to permanently manned station;
  - All staff members should know how to use the systems Like - Fire Alarms, Extinguishers, Sprinklers, Instructions / Fire Brigade Nos., Smoke detectors, and Carbon dioxide based fire extinguishers; and
  - Less Wood and plastic should be in computer rooms.

- **Water Damage:** Some of the major ways of protecting the installation against water damage are as follows:
  - Wherever possible have waterproof ceilings, walls and floors;
  - Ensure an adequate positive drainage system exists;
  - Install alarms at strategic points within the installation;
  - In flood areas have the installation above the upper floors but not at the top floor;
  - Use a gas based fire suppression system;
  - Water proofing; and
  - Water leakage Alarms.
- **Power Supply Variation:** Voltage regulators and circuit breakers protect the hardware from temporary increase or decrease of power. 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.
- **Pollution Damage:** The major pollutant 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 essential.
- **Unauthorized Intrusion:** Physical entry may be restricted to the computer room by various means so that unauthorized intrusion does not take place. A badge system may be used to identify the status of personnel inside the computer room. Various devices are available to detect the presence of bugs by the intruder, that are physically or electronically logging; Guard, dogs; Entry in computer area restricted; Log books; Alarms; Preventing wire tapping; Physical Intrusion detectors; and Security of Documents, data & storage media.

10. The Administrative Procedures that need to be considered during any Business Continuity Planning (BCP) Audit are as follows:

- 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 building is denied or limited for an extended period of time?
- Is there a designated emergency operations center where incident management teams can coordinate response and recovery?
- Determine if the disaster recovery/ business resumption plan covers procedures for disaster declaration, general shutdown and migration of operations to the backup facility.
- 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?

11. If a third-party site is to be used for recovery purposes, security administrators must ensure that a contract is written to cover the following issues:

- How soon the site will be made available subsequent to a disaster;
- The number of organizations that will be allowed to use the site concurrently in the event of a disaster;
- The priority to be given to concurrent users of the site in the event of a common disaster;
- The period during which the site can be used;
- The conditions under which the site can be used;
- The facilities and services the site provider agrees to make available;
- Procedures to ensure security of company's data from being accessed/damaged by other users of the facility; and
- What controls will be in place for working at the off-site facility.

12. The Disaster Recovery Planning (DRP) document may include the following major areas:

- The conditions for activating the plans, which describe the process to be followed before each plan, are activated.
- 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.
- 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.
- Resumption procedures, which describe the actions to be taken to return to normal business operations.
- A maintenance schedule, which specifies 'how and when the plan will be tested', and the process for maintaining the plan.
- 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.
- The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
- Contingency plan document distribution list.

- Detailed description of the purpose and scope of the plan.
- Contingency plan testing and recovery procedure.
- List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
- Checklist for inventory taking and updating the contingency plan on a regular basis.
- List of phone numbers of employees in the event of an emergency.
- Emergency phone list for fire, police, hardware, software, suppliers, customers, back-up location, etc.
- Medical procedure to be followed in case of injury.
- Back-up location contractual agreement, correspondences.
- Insurance papers and claim forms.
- Primary computer centre hardware, software, peripheral equipment and software configuration.
- Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
- Alternate manual procedures to be followed such as preparation of invoices.
- Names of employees trained for emergency situation, first aid and life saving techniques.
- Details of airlines, hotels and transport arrangements.

13. A good coded application and program should have the following characteristics:

- **Reliability:** It refers to the consistency with which a program operates over a period of time. However, poor setting of parameters and hard coding of some data subsequently could result in the failure of a program after some time.
- **Robustness:** It refers to the applications' strength to uphold its operations in adverse situations by taking into account all possible inputs and outputs of a program in case of least likely situations.
- **Accuracy:** It refers not only to 'what program is supposed to do', but should also take care of 'what it should not do'. The second part becomes more challenging for quality control personnel and auditors.
- **Efficiency:** It refers to the performance per unit cost with respect to relevant parameters and it should not be unduly affected with the increase in input values.
- **Usability:** It refers to a user-friendly interface and easy-to-understand internal/ external documentation.

- **Readability:** It refers to the ease of maintenance of program even in the absence of the program developer.

14. (a) Some of the functions of Steering Committee are given as follows:

- To provide overall directions and ensures appropriate representation of affected parties;
- To be responsible for all cost and timetables;
- To conduct a regular review of progress of the project in the meetings of steering committee, which may involve co-ordination and advisory functions; and
- To undertake corrective actions like rescheduling, re-staffing, change in the project objectives and need for redesigning.

(b) "Maintaining the system is an important aspect of SDLC". To achieve this objective, System Maintenance can be categorized in the following ways:

- **Scheduled Maintenance:** Scheduled maintenance is anticipated and can be planned for operational continuity and avoidance of anticipated risks. For example, the implementation of a new inventory coding scheme can be planned in advance, security checks may be promulgated etc.
- **Rescue Maintenance:** Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate troubleshooting solution. A system that is properly developed and tested should have few occasions of rescue maintenance.
- **Corrective Maintenance:** Corrective maintenance deals with fixing bugs in the code or defects found during the executions. A defect can result from design errors, logic errors coding errors, data processing and system performance errors. The need for corrective maintenance is usually initiated by bug reports drawn up by the end users. Examples of corrective maintenance include correcting a failure to test for all possible conditions or a failure to process the last record in a file.
- **Adaptive Maintenance:** Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system. The term environment 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.
- **Perfective Maintenance:** Perfective maintenance mainly deals with accommodating to the new or changed user requirements and concerns functional enhancements to the system and activities to increase the system's performance or to enhance its user interface.

- **Preventive Maintenance:** Preventive maintenance concerns with the activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system.

15. Input design consists of developing specifications and procedures for data preparation, developing steps which are necessary to put transactions data into a usable form for processing, and data-entry, i.e., the activity of putting the data into the computer for processing. Major areas that should be considered while designing systems input are as follows:

(i) **Content:** The analyst is required to consider the types of data that are needed to be gathered to generate the desired user outputs. Sometimes, the data needed for a new system are not available within the organization. Hence, the system designer has to prepare new documents for collecting such information.

(ii) **Timeliness:** In data processing, it is very important that data is inputted to computer in time because outputs cannot be produced until certain inputs are available. Hence, a plan must be established regarding when different types of inputs will enter the system.

(iii) **Media:** Various user input alternatives are available in the market such as workstations, magnetic disc, OCR, pen-based computers and voice input etc. A suitable medium may be selected depending on the application to be computerized.

(iv) **Format:** After the data contents and media requirements are determined, input formats are considered. While specifying the record formats, for instance, the type and length of each data field as well as any other special characteristics must be defined. Designing input formats often requires the assistance of a professional programmer or database administrator.

(v) **Input Volume:** Input volume refers to the amount of data that has to be entered in the computer system at any one time. For example, in some decision-support systems and many real-time transaction processing systems, input volume is light which involves data entry department using key-to-tape or key-to-disk systems.

16. **Control Risk:** 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. 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. 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.

System Control Audit Review File (SCARF): The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written onto a special audit file- the

SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up. Auditors might use SCARF to collect the following types of information:

- **Application System Errors** - SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.
- **Policy and Procedural Variances** - Organizations have to adhere to the policies, procedures and standards of the organization and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.
- **System Exception** - SCARF can be used to monitor different types of application system exceptions. For example, salespersons might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.
- **Statistical Sample** - Some embedded audit routines might be statistical sampling routines, SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.
- **Snapshots and Extended Records** - Snapshots and extended records can be written into the SCARF file and printed when required.
- **Profiling Data** - Auditors can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.
- **Performance Measurement** - Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.

17. **Communication Controls:** Communication Controls maintain a chronology of the events from the time a sender dispatches a message to the time a receiver obtains the message.

Accounting Audit Trail

- Unique identifier of the source/sink node;
- 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;
- Time and date at which the message was received by the sink node;
- Time and date at which node in the network was traversed by the message; and
- Message sequence number; and the image of the message received at each node traversed in the network.

Operations Audit Trail

- Number of messages that have traversed each link and each node;
- 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;
- Log of system restarts; and
- Message transit times between nodes and at nodes.

18. Section 69A is the provision in IT (Amendment) Act 2008 that gives power to issue directions for blocking for public access of any information through any computer resource and is discussed below:

***[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 or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

(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 direction 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.

19. Information Technology Infrastructure Library (ITIL) Service Lifecycle involves the following:

- **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.
- **Service Portfolio Management:** IT portfolio management is the application of systematic management to the investments, projects and activities of enterprise Information Technology (IT) departments.

- **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.
- **Demand Management:** Demand management is a planning methodology used to manage and forecast the demand of products and services.
- **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.

20. Some pertinent similarities between Grid Computing and Cloud Computing are as follows:

- 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. CPU and network bandwidth is allocated and de-allocated on demand. The system's storage capacity goes up and down depending on the number of users, instances, and the amount of data transferred at a given time.
- Both computing types involve multi-tenancy and multitasking, meaning that many customers can perform different tasks, accessing a single or multiple application instances. Sharing resources among a large pool of users assists in reducing infrastructure costs and peak load capacity. Cloud and grid computing provide Service-Level Agreements (SLAs) for guaranteed uptime availability of, say, 99 percent. If the service slides below the level of the guaranteed uptime service, the consumer will get service credit for receiving data not in stipulated time.

Some pertinent differences between Grid Computing and Cloud Computing are as follows:

- 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. In a data grid, the amounts of distributed data must be large for maximum benefit. While in cloud computing, we can store an object as low as 1 byte and as large as 5 GB or even several terabytes.
- A computational grid focuses on computationally intensive operations, while cloud computing offers two types of instances: standard and high-CPU.

21. (a) Phishing: It is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) 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.

Hacking: It refers to unauthorized access and use of computer systems, usually by means of personal computer and a telecommunication network. Normally, hackers do not intend to cause any damage.

Cracking: Crackers are hackers with malicious intentions, which means, un-authorized entry. Now across the world hacking is a general term, with two nomenclatures namely: Ethical and Un-ethical hacking. Un-ethical hacking is classified as Cracking.

(b) Auditor's Selection Norms: There are various norms for selection of Auditors, which are given as follows:

- 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).
- 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, commonly known as $(ISC)^2$.
- The Auditor should have IT audit/governance frameworks and processes conforming to industry leading practices like CoBIT.
- The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the Exchange/Depository. It should not have been engaged over the last three years in any consulting engagement with any departments/units of the entity being audited.
- 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.

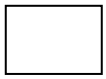
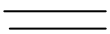
(c) Mobile Computing and Buy Your Own Devices (BYOD): Mobile computing, including BYOD is the single most radical shift in business since the PC revolution of the 1980s. Over the next decade, it will have a huge impact on how people work and live, how companies operate, and on the IT infrastructure. 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. 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. They are optimized for mobility, which means that they have to be light, easy to handle, and maximize battery life. 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.

(d) General Controls: 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. On the whole, General Controls apply to all computerized applications and consist of a combination of system software and manual procedures that create an overall control environment.

(e) Data Flow Diagram (DFD): A Data Flow Diagram uses few simple symbols to illustrate the flow of data among external entities (such as people or organizations, etc.), processing activities and data storage elements. A DFD is composed of four basic elements: Data Sources and Destinations, Data Flows, Transformation processes, and Data stores. These have different symbols that are combined to show how data are processed.

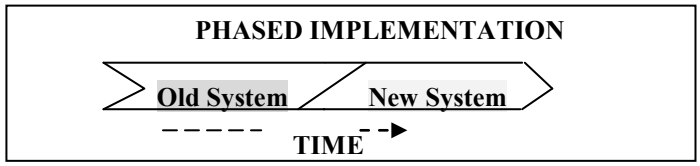
Data Flow Diagram Symbols

Symbol	Name	Explanation
	Data Sources 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 process	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.

22. (a) Cold Site: If an organisation can tolerate some downtime, cold-site backup might be appropriate. A cold site has all the facilities needed to install a mainframe system-raised floors, air conditioning, power, communication lines, and so on. An organisation can establish its own cold-site facility or enter into an agreement with another organisation to provide a cold-site facility.

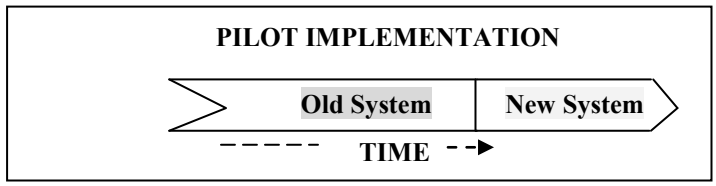
Hot Site: If fast recovery is critical, an organisation might need hot site backup. All hardware and operations facilities will be available at the hot site. In some cases, software, data and supplies might also be stored there. A hot site is expensive to maintain. They are usually shared with other organisations that have hot-site needs.

(b) Phased Changeover: With this strategy, implementation can be staged with conversion to the new system taking place gradually. For example, some new files may be converted and used by employees whilst other files continue to be used on the old system i.e. the new is brought in stages (phases). If a phase is successful then the next phase is started, eventually leading to the final phase when the new system fully replaces the old one as shown in Figure.



Phased Changeover

Pilot Changeover: With this strategy, the new system replaces the old one in one operation but only on a small scale. 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. 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. Figure below depicts Pilot Implementation.



Pilot Changeover

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

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

(d) Inherent Risk: Inherent Risk is the susceptibility of information resources or resources controlled by the information system to material theft, destruction,

disclosure, unauthorized modification, or other impairment, assuming that there are no related internal controls. 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. 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. 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. Example - ATM. Internal controls are ignored in setting inherent risk because they are considered separately in the audit risk model as control risk. It is often an area of professional judgment on the part of an auditor.

Detection Risk: 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. 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. The detection risk associated with lack of identification of disaster recovery plans is ordinarily low since existence is easily verified.

(e) Emergency Plan: The Emergency Plan specifies the actions to be undertaken immediately when a disaster occurs. Management must identify those situations that require the plan to be invoked e.g., major fire, major structural damage and terrorist attack. The actions to be initiated can vary depending on the nature of the disaster that occurs.

When the situations that evoke the plan have been identified, four aspects of the emergency plan must be articulated. 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 (e.g., conditions that must be met before the site is considered safe) must be designated. In all cases, the personnel responsible for the actions must be identified, and the protocols to be followed must be specified clearly.

Recovery Plan: The backup plan is intended to restore operations quickly so that information system function can continue to service an organization, whereas, recovery plans set out procedures to restore full information system capabilities. Recovery plan should identify a recovery committee that will be responsible for working out the specifics of the recovery to be undertaken. The plan should specify the responsibilities of the committee and provide guidelines on priorities to be followed. The plan might also indicate which applications are to be recovered first. Members of a recovery committee must understand their responsibilities. Again, the problem is that they will be required to undertake unfamiliar tasks. Periodically, they

must review and practice executing their responsibilities so they are prepared should a disaster occur. If committee members leave the organization, new members must be appointed immediately and briefed about their responsibilities.

23. (a) The evaluation of effective Management Information System (MIS) should take into account the following major points:

- Examining whether enough flexibility exists in the system to cope with any expected or unexpected information requirement in future.
- Ascertaining the views of users and the designers about the capabilities and deficiencies of the system.
- Guiding the appropriate authority about the steps to be taken to maintain effectiveness of MIS.

(b) The advantages of Business Continuity Management (BCM) are that the enterprise:

- is able to proactively assess the threat scenario and potential risks;
- has planned response to disruptions which can contain the damage and minimize the impact on the enterprise; and
- is able to demonstrate a response through a process of regular testing and trainings.

(c) [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.

(d) User Related Issues: It refers to those issues where user/customer is reckoned as the primary agent. Some of the aspects with regard to this problem are as follows:

- **Shifting User Needs:** User requirements for IT are constantly changing. As these changes accelerate, there will be more requests for Information systems development and more development projects. When these changes occur

during a development process, the development team faces the challenge of developing systems whose very purpose might change since the development process began.

- **Resistance to Change:** People have a natural tendency to resist change, and information systems development projects signal changes - often radical - in the workplace. When personnel perceive that the project will result in personnel cutbacks, threatened personnel will dig in their heels, and the development project is doomed to failure.
- **Lack of User Participation:** Users must participate in the development efforts to define their requirements, feel ownership for project success, and work to resolve development problems. User participation also helps to reduce user resistance to change.
- **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.

24. (a) **Methods of Validating the proposal:** Large organizations would naturally tend to adopt a sophisticated and objective approach to validate the vendor's proposal. Some of the validation methods for approving the vendor's proposal are as follows:

- **Checklists:** It is the most simple and a subjective method for validation and evaluation. The various criteria are put in check list in the form of suitable questions against which the responses of the various vendors are validated. For example, Support Service Checklists may have parameters like Performance; System development, Maintenance, Conversion, Training, Back-up, Proximity, Hardware and Software.
- **Point-Scoring Analysis:** Point-scoring analysis provides an objective means of selecting a final system. There are no absolute rules in the selection process, only guidelines for matching user needs with software capabilities. 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.
- **Public Evaluation Reports:** Several consultancy as well as independent agencies compare and contrast the hardware and software performance for various manufacturers and publish their reports in this regard. This method has been frequently and usefully employed by several buyers in the past and is particularly useful where the buying staffs have inadequate knowledge of facts.
- **Benchmarking Problems related Vendor's Solutions:** Benchmarking problems related to vendors' proposals are accomplished by sample programs that represent at least a part of the buyer's primary work load and include considerations and can be current applications that have been designed to

represent planned processing needs. That is, benchmarking problems are oriented towards testing whether a solution offered by the vendor meets the requirements of the job on hand of the buyer.

- **Testing Problems:** Test problems disregard the actual job mix and are devised to test the true capabilities of the hardware, software or system. For example, test problems may be developed to evaluate the time required to translate the source code (program in an assembly or a high level language) into the object code (machine language), response time for two or more jobs in multi-programming environment, overhead requirements of the operating system in executing a user program, length of time required to execute an instruction, etc.

(b) Major components that have been considered in Web 2.0 include the following:

- **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. There are a number of tools available online, now-a-days to create communities, which are very cost efficient as well as easy to use.
- **Blogging:** 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.
- **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.
- **Folksonomy:** Web 2.0 being a people-centric technology has introduced the feature of Folksonomy where users can tag their content online and this enables others to easily find and view other content.
- **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.
- **Mashups:** This is the facility, by using which people on the internet can congregate services from multiple vendors to create a completely new service. An example may be combining the location information from a mobile service provider and the map facility of Google maps in order to find the exact information of a cell phone device from the internet, just by entering the cell number.

(c) Various features of Electronic Mail are stated below:

- **Electronic Transmission -** The transmission of messages with email is electronic and message delivery is very quick, almost instantaneous. The confirmation of transmission is also quick and the reliability is very high.

- **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. It also facilitates the storage of messages on magnetic media, thereby reducing the space required to store the messages.
- **Broadcasting and Rerouting -** Email permits sending a message to a large number of target recipients. Thus, it is easy to send a circular to all branches of a bank using Email resulting in a lot of saving of paper. The email could be rerouted to people having direct interest in the message with or without changing or and appending related information to the message.
- **Integration with other Information Systems -** The E-mail has the advantage of being integrated with the other information systems. Such integration helps in ensuring that the message if accurate and the information required for the message is accesses quickly.
- **Portability -** Email renders the physical location of the recipient and sender irrelevant. The email can be accessed from any Personal computer/tablet/smart phones equipped with the relevant communication hardware, software and link facilities.
- **Economical -** The advancements in communication technologies and competition among the communication service providers have made Email the most economical mode for sending and receiving messages. The email is very helpful for formal communication as well as informal communication within the enterprise.

(d) Various types of back-ups are given as follows:

- **Full Backup:** A Full Backup captures all files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data.
- **Incremental Backup:** An Incremental Backup captures files that were created or changed since the last backup, regardless of backup type. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space.

  Normally, incremental backup are very difficult to restore. One will have to start with recovering the last full backup, and then recovering from every incremental backup taken since.
- **Differential Backup:** A Differential Backup stores files that have changed since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up.

Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

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

25. (a) Two primary methods through which the analyst would have collected the data are given as follows:

(1) **Reviewing internal documents:** The analyst first tries to learn about the organization involved in or affected by the project. For example, to review an inventory system proposal, s/he will try to know 'how the inventory department operates' and 'who are the managers and supervisors'. S/he will examine organization charts and written operating procedures.

(2) **Conducting interviews:** Written documents tell the analyst 'how the system should operate' but they may not include enough details to allow a decision to be made about the merits of a system proposal nor do they present users' views about current operations. To learn these details, analysts use interviews. Preliminary investigation interviews involve only management and supervisory personnel.

(b) [Section 7] Retention of Electronic Records

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, 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.