PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

Concepts of Governance and Management of Information Systems

1. You are appointed as an Internal Auditor in XYZ enterprise. As an internal auditor, what shall be your perspective while evaluating IT Governance of an enterprise?
2. (a) Discuss Risk Management Strategies in detail.

   (b) What do you understand by "Information Systems Risks"? Discuss broadly the characteristics of risk.
3. (a) Discuss the seven categories of enablers of COBIT 5?

   (b) Discuss various key management practices for assessing and evaluating the system of internal controls in an enterprise.

Information System Concepts

4. "Decision Support Systems (DSS) are widely used as part of an Organization's Accounting Information System". Give examples to support this statement.
5. What is Executive Information Systems (EIS)? Explain major characteristics of an EIS.
6. What do you mean by the term "Information"? Discuss different attributes of it.

Protection of Information Systems

7. Discuss Data Resource Management Controls under Managerial Controls.
8. Why is there an emergence of Quality Assurance Management Controls in organizations?
9. As a senior manager of an organization ABC, what do you think are the major functions performed by you while performing Information Systems (IS) functions in the organization?

Business Continuity Planning and Disaster Recovery Planning

10. (a) Discuss the maintenance tasks undertaken in the development of a Business Continuity Plan (BCP) in brief.

    (b) 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?
11. Discuss Differential Backup, its advantages and disadvantages.

12. An enterprise XYZ implemented a Business Continuity Plan and decided to get its plan audited. What factors should be verified while auditing or self-assessment of the enterprise's Business Continuity Management (BCM) program?

Acquisition, Development and Implementation of Information Systems

13. Discuss various System Changeover Strategies under System Implementation phase of System Development Life Cycle (SDLC).

14. Discuss various issues that should be considered while designing systems input.

15. Discuss the Waterfall Model, its strengths and weaknesses in brief.

Auditing of Information Systems

16. As an auditor, what do you think are the advantages of using Continuous Audit Techniques?

17. Why do we need to perform Audit of Information Systems?

18. What do you understand by the term "Audit Trails"? How Audit Trails can be used to support security objectives?

Information Technology Regulatory Issues

19. ABC Ltd. is a security market intermediary, providing depository services. Briefly explain the relevant requirements with respect to annual systems audit mandated by SEBI (Securities and Exchange Board of India) in this regard.

20. Describe the 'Tampering with Computer Source Documents' in the light of Section 65 of Information Technology Act 2000.

Emerging Technologies

21. Discuss emerging Bring Your Own Devices (BYOD) Threats.

22. Discuss the characteristics and advantages of Community Cloud in Cloud Computing.

Short Note Based Questions

23. Write short notes on following:

    (a) PDCA cyclic process

    (b) Role of IS Auditor in reviewing Physical Access Controls

    (c) Benefits of Governance of Enterprise IT (GEIT)

    (d) Information Technology General Controls (ITGC)

    (e) Business Continuity Plan (BCP) Manual

24. Differentiate between the following:
    (a) Explicit Knowledge and Tacit Knowledge
    (b) Program Debugging and Program Documentation
    (c) Manual Logging and Electronic Logging
    (d) Identity as a Service (IDaaS) and Security as a Service(SECaaS)
    (e) Control Risk and Detection Risk

Questions based on the Case Studies

25. 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) 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?

SUGGESTED ANSWERS/HINTS

1. As an Internal Auditor in XYZ enterprise, the perspective while evaluating IT governance of an enterprise are as follows:

- **Leadership:** The following aspects need to be verified by the auditor:
    - Evaluate the relationship between IT objectives and the current/strategic needs of the organization and the ability of IT leadership to effectively communicate this relationship to IT and organizational personnel.
    - Assess the involvement of IT leadership in the development and on-going execution of the organization's strategic goals.
    - Determine how IT will be measured in helping the organization achieve these

goals.

- Review how roles and responsibilities are assigned within the IT organization and how they are executed.
- Review the role of senior management and the board in helping establish and maintain strong IT governance.

- **Organizational Structure:** The following aspects need to be assessed by the auditor:
  - Review how organization management and IT personnel are interacting and communicating current and future needs across the organization.
  - This should include the existence of necessary roles and reporting relationships to allow IT to meet the needs of the organization, while providing the opportunity to have requirements addressed via formal evaluation and prioritization. In addition, how IT mirrors the organization structure in its enterprise architecture should also be included.
- **Processes:** The following aspects need to be checked by the auditor:
  - Evaluate IT process activities and the controls in place to mitigate risks to the organization and whether they provide the necessary assurance regarding processes and underlying systems.
  - What processes are used by the IT organization to support the IT environment and consistent delivery of expected services?
- **Risks:** The following aspects need to be reviewed by the auditor:
  - Review the processes used by the IT organization to identify, assess, and monitor/mitigate risks within the IT environment.
  - Additionally, determine the accountability that personnel have within risk management and how well these expectations are being met.
- **Controls:** The following aspects need to be verified by the auditor:
  - Assess key controls that are defined by IT to manage its activities and the support of the overall organization.
  - Ownership, documentation, and reporting of self-validation aspects should be reviewed by the internal audit activity.
  - Additionally, the control set should be robust enough to address identified risks based on the organization's risk appetite and tolerance levels, as well as any compliance requirements.

- **Performance Measurement/Monitoring:** The following aspects need to be verified by the auditor:
  - Evaluate the framework and systems in place to measure and monitor organizational outcomes where support from IT plays an important part in the internal outputs in IT operations and developments.

2. (a) The Risk Management Strategies are as follows:

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

(b) Information Systems Risks: 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. Risk management involves identifying, measuring, and minimizing uncertain events affecting resources. Any Information system based on IT has its inherent risks. These risks cannot be eliminated but they can be mitigated by appropriate security. If controls are unavailable or inadequate or inappropriate, then there would be a control weakness, which must be reported to auditee management with appropriate recommendations to mitigate them.

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

Some of the common sources of risk are Commercial and Legal Relationships; Economic Circumstances; Human Behavior; Natural Events; Political Circumstances; Technology and Technical Issues; Management Activities and Controls, and Individual Activities.

Broadly, Risk has the following characteristics:

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

3. (a) The COBIT 5 framework describes seven categories of enablers, which are as follows:

- **Principles, Policies and Frameworks** are the vehicle to translate the desired behavior into practical guidance for day-to-day management.
- **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.
- **Organizational structures** are the key decision-making entities in an enterprise.
- **Culture, Ethics and Behavior** of individuals and of the enterprise is very often underestimated as a success factor in governance and management activities.
- **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.
- **Services, Infrastructure and Applications** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.

- **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.

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

- **Monitor Internal Controls:** Continuously monitor, benchmark and improve the IT control environment and control framework to meet organizational objectives.
- **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. It also includes activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing of controls, continuous controls monitoring, independent assessments, command and control centers, and network operations centers. This provides the business with the assurance of control effectiveness to meet requirements related to business, regulatory and social responsibilities.
- **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.
- **Identify and Report Control Deficiencies:** Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.
- **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.
- **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.

- **Scope assurance initiatives:** Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.
- **Execute assurance initiatives:** Execute the planned assurance initiative. Report on identified findings. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control system residual risks.

4. Decision Support Systems (DSS) 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.

5. **Executive Information Systems (EIS):** It is also referred to as an Executive Support System (ESS) that serves at 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.

   Major characteristics of an EIS are as follows:

   - It 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.
   - It 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.

6. **Information:** Technically, Information means processed data. Information relates to description, definition, or perspective (what, who, when, where) and may be represented in the form of text, graph, pictures, voice, videos etc.

   Information is essential because it adds knowledge, helps in decision making, analyzing the future and taking action in time. Information products produced by an

information system can be represented by number of ways e.g. paper reports, visual displays, multimedia documents, electronic messages, graphics images, and audio responses.

Some of the important attributes of useful and effective information are as follows:

- **Availability -** Information is useless if it is not available at the time of need. Database is a collection of files which is collection of records and data from where the required information is derived for useful purpose.
- **Purpose/Objective -** Information must have purpose/objective at the time it is transmitted to a person or machine, otherwise it is simple data. The basic objective of information is to inform, evaluate, persuade, and organize. This indeed helps in decision making, generating new concepts and ideas, identify and solve problems, planning, and controlling which are needed to direct human activity in business enterprises.
- **Mode and format -** The mode of communicating information to humans should be in such a way that it is easily understandable by the people. The mode may be in the form of voice, text and combination of these two. Format should also be designed in such a way that it assists in decision making, solving problems, initiating planning, controlling and searching.
- **Current/Updated -** The information should be refreshed from time to time as it usually rots with time and usage. For example, the running score sheet of a cricket match available in Internet sites should be refreshed at fixed interval of time so that the current score will be available.
- **Rate -** The rate of transmission/reception of information may be represented by the time required to understand a particular situation. Useful information is the one which is transmitted at a rate which matches with the rate at which the recipient wants to receive. For example - the information available from internet site should be available at a click of mouse.
- **Frequency -** The frequency with which information is transmitted or received affects its value. For example - the weekly report of sales shows little change as compared to the quarterly and contribute less for accessing salesman capability.
- **Completeness and Adequacy -** The information provided should be complete and adequate in itself because only complete information can be used in policy making. For example - the position of student in a class can be find out only after having the information of the marks of all students and the total number of students in a class.

- **Reliability -** It is a measure of failure or success of using information for decision-making. If information leads to correct decision on many occasions, we say the information is reliable.
- **Validity -** It measures how close the information is to the purpose for which it asserts to serve. For example, the experience of employee supports in evaluating his performance.
- **Quality -** It means the correctness of information. For example, an over-optimistic manager may give too high estimates of the profit of product which may create problem in inventory and marketing.
- **Transparency -** It is essential in decision and policy making. For example, total amount of advance does not give true picture of utilization of fund for decision about future course of action; rather deposit-advance ratio is perhaps more transparent information in this matter.
- **Value of Information -** It is defined as the difference between the value of the change in decision behavior caused by the information and the cost of the information. In other words, given a set of possible decisions, a decision-maker may select one on basis of the information at hand. If new information causes a different decision to be made, the value of the new information is the difference in value between the outcome of the old decision and that of the new decision, less the cost of obtaining the information.

7. **Data Resource Management Controls:** Many organizations now recognize that 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; 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. 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.

   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. Backup controls 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. Various backup strategies are Dual recording of data; Periodic dumping of data; Logging input transactions; and Logging changes to the data.

(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:

- User Access Controls through passwords, tokens and biometric Controls; and
- 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:

- By permitting only addition of data to the database; and
- 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.

8. The reasons for the emergence of Quality Assurance Management Controls in many organizations are as follows:

- Organizations are increasingly producing safety-critical systems and users are becoming more demanding in terms of the quality of the software they employ to undertake their work;
- Organizations are undertaking more ambitious projects when they build software;
- 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;
- 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; and
- 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.

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 –

- Quality goals are established and understood clearly by all stakeholders; and
- Compliance occurs with the standards that are in place to attain quality information systems.

9. The major functions that a senior manager must perform while performing Information Systems (IS) functions in the organization are as follows:

(a) Planning – This includes determining the goals of the information systems function and the means of achieving these goals. To achieve this – the plan is to be prepared with different types of Plans and the Role of a Steering Committee should be defined clearly.

(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.

(c) Leading – This includes motivating, guiding, and communicating with personnel. The purpose of leading is to achieve the harmony of objectives; ie.. a person's or group's objectives must not conflict with the organization's objectives. The process of leading requires managers to motivate subordinates, direct them and communicate with them.

(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.

10. (a) The maintenance tasks undertaken in Development of Business Continuity Plan (BCP) are as follows:

- Determine the ownership and responsibility for maintaining the various BCP strategies within the enterprise;
- 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;
- Determine the maintenance regime to ensure the plan remains up-to-date;
- Determine the maintenance processes to update the plan; and
- Implement version control procedures to ensure that the plan is maintained up-to-date.

(b) If a third-party site is to be used for backup and recovery purposes, security administrators must ensure that a contract is written to cover issues such as

- how soon the site will be made available subsequent to a disaster;
- the number of organizations that will be allowed to use the site concurrently in the event of a disaster;
- the priority to be given to concurrent users of the site in the event of a common disaster;
- the period during which the site can be used;
- the conditions under which the site can be used;
- the facilities and services the site provider agrees to make available; and
- what controls will be in place and working at the off-site facility.

11. Differential Backup: Differential backups fall in the middle between full backups and incremental backup. A Differential Backup stores files that have changed since the last full backup. With differential backups, one full backup is done first and subsequent backup runs are the changes made 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.

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.

Advantages of Differential Backup are as follows:

- 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.

Disadvantages of Differential Backup are as follows:

- 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.

12. An audit or self-assessment of the enterprise's Business Continuity Management (BCM) program should verify the following factors:

- All key products and services and their supporting critical activities and resources have been identified and included in the enterprise's BCM strategy;
- The enterprise's BCM policy, strategies, framework and plans accurately reflect its priorities and requirements (the enterprise's objectives);
- 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;
- The enterprise's BCM solutions are effective, up-to-date and fit-for-purpose, and appropriate to the level of risk faced by the enterprise;
- The enterprise's BCM maintenance and exercising programs have been effectively implemented;
- BCM strategies and plans incorporate improvements identified during incidents and exercises and in the maintenance program;
- The enterprise has an ongoing program for BCM training and awareness;

- BCM procedures have been effectively communicated to relevant staff, and that those staff understand their roles and responsibilities; and
- Change control processes are in place and operate effectively.

13. System Change-Over Strategies: Conversion or changeover is the process of changing over or shifting over from the old system (may be the manual system) to the new system. It requires careful planning to establish the basic approach to be used in the actual changeover, as it may put many resources/assets/operations at risk. The Four types of popular implementation strategies are described as follows:

- **Direct Implementation / Abrupt Change-Over:** This is achieved through an abrupt takeover – an all or no approach. With this strategy, the changeover is done in one operation, completely replacing the old system in one go. 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.
- **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.
- **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.
- **Parallel Changeover:** This is considered the most secure method with both systems running in parallel over an introductory period. The old system remains fully operational while the new systems come online. With this strategy, the old and the new system are both used alongside each other, both being able to operate independently. If all goes well, the old system is stopped and new system carries on as the only system.

14. 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.

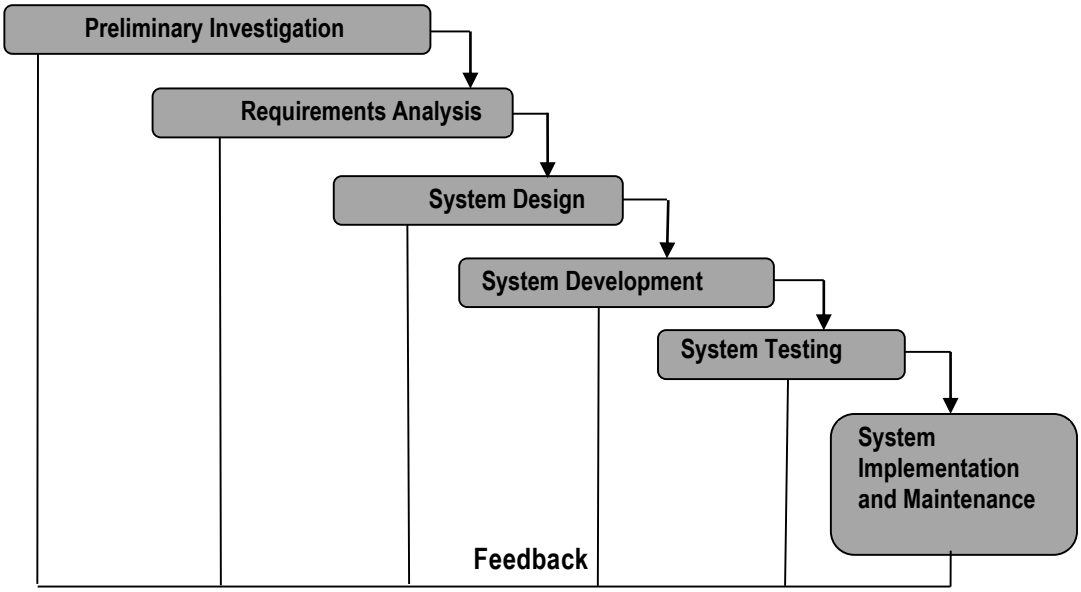
(v) **Input Volume:** Input volume refers to the amount of data that has to be entered in the computer system at any one time. For example, in some decision-support systems and many real-time transaction processing systems, input volume is light which involves data entry department using key-to-tape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

15. **Waterfall Model:** The waterfall approach is a traditional development approach in which each phase is carried in sequence or linear fashion. These phases include requirements analysis, specifications and design requirements, coding, final testing, and release. In this traditional approach of system development, activities are performed in sequence. The tasks that are performed during each phase of the traditional approach is shown in the Fig. below. When the traditional approach is applied, an activity is undertaken only when the prior step is fully completed.

Major strengths of Waterfall Model are as follows:

- It is ideal for supporting less experienced project teams and project managers or project teams, whose composition fluctuates.
- The orderly sequence of development steps and design reviews help to ensure the quality, reliability, adequacy and maintainability of the developed software.

- Progress of system development is measurable.
- It enables to conserve resources.



Some of the weaknesses of the Waterfall Model are as follows:

- It is criticized to be inflexible, slow, costly, and cumbersome due to significant structure and tight controls.
- Project progresses forward, with only slight movement backward.
- There is a little to iterate, which may be essential in situations.
- It depends upon early identification and specification of requirements, even if the users may not be able to clearly define 'what they need early in the project'.
- Requirement inconsistencies, missing system components and unexpected development needs are often discovered during design and coding.
- Problems are often not discovered until system testing.
- System performance cannot be tested until the system is almost fully coded, and under capacity may be difficult to correct.
- It is difficult to respond to changes, which may occur later in the life cycle, and if undertaken it proves costly and are thus discouraged.
- It leads to excessive documentation, whose updation to assure integrity is an uphill task and often time-consuming.
- Written specifications are often difficult for users to read and thoroughly appreciate.

- It promotes the gap between users and developers with clear vision of responsibility.

16. Some of the advantages of using Continuous Audit Techniques are given as under:

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

17. Audit of Information Systems is required due to following reasons:

- **Organisational Costs of Data Loss:** Data is a critical resource of an organisation for its present and future process and its ability to adapt and survive in a changing environment.
- **Cost of Incorrect Decision Making:** Management and operational controls taken by managers involve detection, investigations and correction of the processes. These high level decisions require accurate data to make quality decision rules.
- **Costs of Computer Abuse:** Unauthorised access to computer systems, malwares, unauthorised physical access to computer facilities and unauthorised copies of sensitive data can lead to destruction of assets (hardware, software, data, information etc.)
- **Value of Computer Hardware, Software and Personnel***:* These are critical resources of an organisation, which has a credible impact on its infrastructure and business competitiveness.
- **High Costs of Computer Error:** In a computerised enterprise environment where many critical business processes are performed, a data error during entry or process would cause great damage.

- **Maintenance of Privacy:** Today, data collected in a business process contains private information about an individual too. These data were also collected before computers but now, there is a fear that privacy has eroded beyond acceptable levels.
- **Controlled evolution of computer Use:** Use of Technology and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.

18. Audit Trails: Audit trails are the logs that can be designed to record activity at the system, application, and user level. When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives. Many operating systems allow management to select the level of auditing to be provided by the system. This determines 'which events will be recorded in the log'. An effective audit policy will capture all significant events without cluttering the log with trivial activity.

Audit trail controls attempt to ensure that a chronological record of all events that have occurred in a system is maintained. This record is needed to answer queries, fulfill statutory requirements, detect the consequences of error and allow system monitoring and tuning. The accounting audit trail shows the source and nature of data and processes that update the database. The operations audit trail maintains a record of attempted or actual resource consumption within a system.

Audit trails can be used to support security objectives in three ways:

- **Detecting Unauthorized Access*:*** The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls. 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. 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.
- **Reconstructing Events*:*** 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. 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. Audit trail analysis also plays an important role in accounting control.
- **Personal Accountability*:*** Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behavior. Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log.

19. SEBI (Securities and Exchange Board of India) mandated that exchanges shall conduct an annual system audit by a reputed independent auditor.

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

20. Section 65 of Information Technology Act, 2000 is about "Tampering with Computer Source Documents". The section is -

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.

21. Every business decision is accompanied with a set of threats and so is Bring Your Own Device (BYOD) program too; it is not immune from them. As outlined in the Gartner survey, 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 as outlined below:

- **Network Risks:** It is normally exemplified and hidden in 'Lack of Device Visibility'. When company-owned devices are used by all employees within an organization, the organization's IT practice has complete visibility of the devices connected to the network. This helps to analyze traffic and data exchanged over the Internet. As BYOD permits employees to carry their own devices (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the network. As network visibility is of high importance, this lack of visibility can be hazardous.
- **Device Risks:** It is normally exemplified and hidden in 'Loss of Devices'. A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information. Data lost from stolen or lost devices ranks as the top security threats as per the rankings released by Cloud Security Alliance. With easy access to company emails as well as corporate intranet, company trade secrets can be easily retrieved from a misplaced device.
- **Application Risks:** It is normally exemplified and hidden in **'**Application Viruses and Malware'. 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. With an increase in mobile usage, mobile vulnerabilities have increased concurrently. Organizations are not clear in deciding that 'who is responsible for device security – the organization or the user'.
- **Implementation Risks:** It is normally exemplified and hidden in 'Weak BYOD Policy'. The effective implementation of the BYOD program should not only cover the technical issues mentioned above but also mandate the development of a robust implementation policy. Because corporate knowledge and data are key assets of an organization, the absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse. In addition to this, a weak policy fails to educate the user, thereby increasing vulnerability to the above-mentioned threats.

22. Characteristics of Community Clouds in Cloud Computing are as follows:

- **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.

- **Partially Secure:** This refers to the property of the community cloud where few 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.
- **Cost Effective:** As the complete cloud if being shared by several organizations or community, not only the responsibility gets shared; the community cloud becomes cost effective too.

Advantages of Community Clouds in Cloud Computing are as follows:

- It allows establishing a low-cost private cloud.
- It allows collaborative work on the cloud.
- It allows sharing of responsibilities among the organizations.
- It has better security than the public cloud.

23. (a) The PDCA cyclic process is explained below:

- **The Plan Phase (Establishing the Information Security Management System (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).
- **The Do Phase (Implementing and Working of ISMS) –** This phase includes carrying out everything that was planned during the previous phase.
- **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.
- **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.

(b) Role of IS Auditor in reviewing Physical Access Controls involves the following:

- **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.
- **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.

- **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.

(c) Benefits of Governance of Enterprise IT (GEIT) are as follows:

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

(d) **Information Technology General Controls (ITGC):** These 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. IT General Controls are the foundation for the overall IT control environment as they provide the assurance that systems operate as intended and that output is reliable.

ITGCs may also be referred to as General Computer Controls (GCC) which are defined as: Controls, other than application controls, which relate to the environment within which computer-based application systems are developed, maintained and operated, and which are therefore applicable to all applications. 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. Like application controls, general controls may be either manual or programmed. 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.

(e) **Business Continuity Plan (BCP) Manual:** 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. 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. 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(s) affected and other departments providing support services.

24. (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.

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.

(b) **Program Debugging:** Debugging is the most primitive form of testing activity, which refers to correcting programming language syntax and diagnostic errors so that the program compiles cleanly. A clean compile means that the program can be successfully converted from the source code written by the programmer into machine language instructions. Debugging can be a tedious task consisting of following four steps:

- Giving input the source program to the compiler,
- Letting the compiler to find errors in the program,
- Correcting lines of code that are erroneous, and
- Resubmitting the corrected source program as input to the compiler.

Program Documentation: The writing of narrative procedures and instructions for people, who will use software is done throughout the program life cycle. Managers and users should carefully review both internal and external documentation to ensure that the software and system behave as the documentation indicates. If they do not, documentation should be revised. 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.

(c) **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. Logging may happen at both fronts - reception and entrance to the computer room. A valid and acceptable identification such as a driver's license, business card or vendor identification tag may also be asked for before allowing entry inside the company.

Electronic Logging: This feature is a combination of electronic and biometric security systems. The users logging can be monitored and the unsuccessful attempts being highlighted.

(d) **Identity as a Service (IDaaS):** 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. Generally, IDaaS includes directory services, authentication services, risk and event monitoring, single sign-on services, and identity and profile management.

Security as a Service(SECaaS): 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. 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. Four mechanisms of Cloud security that are currently provided are Email filtering, Web content filtering, Vulnerability management and Identity management.

(e) **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.

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.

25. (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) 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.