ISCA MAY 2018

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.

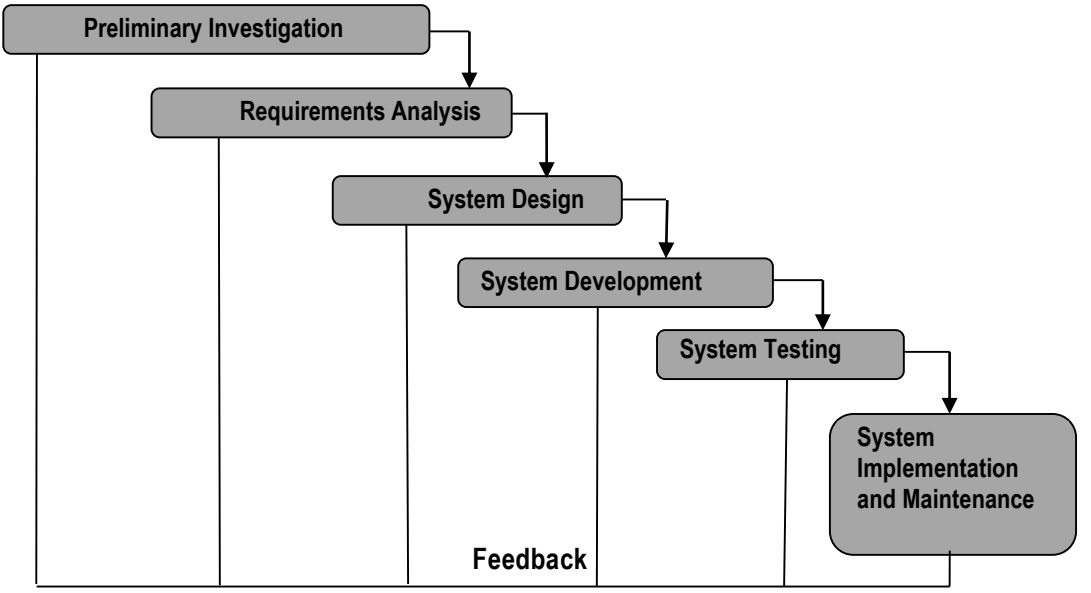
(v) Input Volume: Input volume refers to the amount of data that has to be entered in the computer system at any one time. For example, in some decision-support systems and many real-time transaction processing systems, input volume is light which involves data entry department using key-to-tape or key-to-disk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

ISCA RTP NOV 2017

PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

Concepts of Governance and Management of Information Systems

1. What are the three levels of managerial activity in an enterprise during IT Strategy Planning.
2. Discuss the key Governance practices for evaluating Risk Management.
3. (a) What are the benefits of COBIT 5?
   (b) Discuss various key management practices for assessing and evaluating the system of internal controls in an enterprise.

Information Systems Concepts

4. Discuss the benefits of Enterprise Resource Planning (ERP).
5. What are the major characteristics of an effective Management Information System (MIS)?
6. "Information is considered as a key business Asset". Discuss the statement.

Protection of Information Systems

7. What do you understand by the term "Segregation of Duties"?
8. Categorize and explain various Information systems resources from the perspective of environmental exposures and controls.
9. Discuss Application and Monitoring System Access Controls, in brief.

Business Continuity Planning and Disaster Recovery Planning

10. While developing a Business Continuity Plan, what are the key tasks that should be covered under the second phase 'Vulnerability Assessment and General definition of Requirement'?
11. An enterprise ABC 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?
12. Discuss the major areas that are included as a part of Disaster Recovery Planning (DRP) Document.

Acquisition, Development and Implementation of Information Systems

13. "Feasibility Study is the considered as a backbone of System Development Life Cycle (SDLC)." Considering this statement; list out various dimensions of Feasibility Study in SDLC.

14. Explain two primary methods, which are used for the analysis of the scope of a project in System Development Life Cycle (SDLC).
15. Discuss major strengths and weaknesses of Agile Model.

Auditing of Information Systems

16. (i) PQR Ltd. is looking for a suitable IS Auditor. Please send an introductory note to PQR Ltd. explaining your suitability by describing the skill set and the competence you possess for the job other that your qualification.
    (ii) Let Mr. X is appointed as an IS auditor of PQR Ltd. and is assigned a task to perform preliminary review of audit environment. What are the legal considerations and Audit Standards that he should consider as a part of his preliminary investigation?
17. Discuss the Accounting and Operations Audit Trails of Input Controls under Application Controls.
18. Discuss the System Control Audit Review File (SCARF) technique used in the audit of Information Systems.

Information Technology Regulatory Issues

19. Discuss IT Infrastructure Library (ITIL), in detail.

Emerging Technologies

20. Discuss major limitations of Mobile Computing.
21. What do you understand by the term "Web 3.0"? Discuss its components, in brief.

Short Note Based Questions

22. Write short notes on following:
    (a) BCP Manual
    (b) Data Dictionary
    (c) Audit Hooks
    (d) Operational Level Systems
    (e) Emergency Plan
23. Differentiate between the following:
    (a) Tacit Knowledge and Explicit Knowledge
    (b) Inherent Risk and Detection Risk
    (c) Physical Controls and Logical Controls
    (d) Scheduled Maintenance and Rescue Maintenance
    (e) Data as a Service (DaaS) and Security as a Service(SECaaS)

Questions based on Case Studies/Scenario based

24. (i) XYZ Group is in the process of launching a new business unit to provide various technical consultancy services to the organizations worldwide to assist them in the computerization of their business modules. It involves a number of activities starting from capturing of requirements to maintenance. Business Continuity and Disaster Recovery Planning are two key activities which must be taken care of right from the beginning. Business continuity focuses on maintaining the operations of an organization, especially the IT infrastructure in face of a threat that has materialized. Disaster recovery, on the other hand, arises mostly when business continuity plan fails to maintain operations and there is a service disruption. This plan focuses on restarting the operations using a prioritized resumption list. But both the plans must be assessed regarding their performance on a periodic basis.

Read the above carefully and answer the following:

(a) What are the issues, which are emphasized by the methodology for developing a business continuity plan?

(b) Explain the objectives of performing Business Continuity Planning tests.

(c) Out of various backup options available, explain incremental backup in brief?

25. (i) As per the article of Aryan Ltd. it was mentioned that the *financial* statements of the company shall be maintained for 8 years in electronic form as records. Mr. X, a person to collect back ground history of well-being of the company, went to the company to get the information of financial condition of past 5 years, so that he may subscribe for the shares of the company. Company denied to access the past accounts of the company as the maintained records have been corrupted.

Discuss in the light of the given situation, the legal position of Aryan Ltd. with respect to the maintenance of records in electronic form as per the IT Act, 2000.

(ii) ABC, is a Database company, funded by the Government, to maintain public documents of the various bodies electronically. If suppose Aryan Ltd. conferred a right on the ABC Database company, to maintain its public documents. Aryan Ltd. demanded of the past maintained records from the database company to maintain the records as they were corrupted. However, Database Company ABC also failed to deliver the past e- records of the financial statements of the company Aryan Ltd. State the liability of Database Company ABC in the given situation.

SUGGESTED ANSWERS/HINTS

1. The three levels of managerial activity in an enterprise during IT Strategy Planning are as follows:

- **Strategic Planning:** Strategic Planning is defined as the process of deciding on objectives of the enterprise, on changes in these objectives, on the resources used to attain these objectives, and on the policies, that are to govern the acquisition, use, and disposition of these resources. Strategic planning is the process by which top management determines overall organizational purposes and objectives and how they are to be achieved.
- **Management Control:** Management Control is defined as the process by which managers assure that resources are obtained and used effectively and efficiently in the accomplishment of the enterprise's objectives.
- **Operational Control:** Operational Control is defined as the process of assuring that specific tasks are carried out effectively and efficiently.

2. The key Governance practices for evaluating risk management are given as follows:

- **Evaluate Risk Management:** Continually examine and make judgment on the effect of risk on the current and future use of IT in the enterprise. Consider whether the enterprise's risk appetite is appropriate and that risks to enterprise value related to the use of IT are identified and managed;
- **Direct Risk Management:** Direct the establishment of risk management practices to provide reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite; and
- **Monitor Risk Management:** Monitor the key goals and metrics of the risk management processes and establish how deviations or problems will be identified, tracked and reported on for remediation.

3. (a) Benefits of COBIT 5 are as follows:

- A comprehensive framework such as COBIT 5 enables enterprises in achieving their objectives for the governance and management of enterprise IT.
- The best practices of COBIT 5 help enterprises to create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use.
- Further, COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT related interests of internal and external stakeholders.
- COBIT 5 helps enterprises to manage IT related risk and ensures compliance, continuity, security and privacy.

- COBIT 5 enables clear policy development and good practice for IT management including increased business user satisfaction.
- The key advantage in using a generic framework such as COBIT 5 is that it is useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.
- COBIT 5 supports compliance with relevant laws, regulations, contractual agreements and policies.

(b) The key management practices for assessing and evaluating the system of internal controls in an enterprise are given 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. The benefits of Enterprise Resource Planning (ERP) are as follows:

- Streamlining processes and workflows with a single integrated system.
- Reduce redundant data entry and processes and in other hand it shares information across the department.
- Establish uniform processes that are based on recognized best business practices.
- Improved workflow and efficiency.
- Improved customer satisfaction based on improved on-time delivery, increased quality, shortened delivery times.
- Reduced inventory costs resulting from better planning, tracking and forecasting of requirements.
- Turn collections faster based on better visibility into accounts and fewer billing and/or delivery errors.
- Decrease in vendor pricing by taking better advantage of quantity breaks and tracking vendor performance.
- Track actual costs of activities and perform activity based costing.
- Provide a consolidated picture of sales, inventory and receivables.

5. Major characteristics of an effective Management Information Systems (MIS) are as follows:

- **Management Oriented –** It means that efforts for the development of the information system should start from an appraisal of management needs and overall business objectives. Such a system is not necessarily for top management only but may also meet the information requirements of middle level or operating levels of management as well.
- **Management Directed –** Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts. For system's effectiveness, it is necessary for management to devote their sufficient time not only at the stage of designing the system but for its review as well to ensure that the implemented system meets the specifications of the designed system.
- **Integrated –** The best approach for developing information systems is the integrated approach as all the functional and operational information sub-systems are tied together into one entity. An integrated Information system has the capability of

generating more meaningful information to management as it takes a comprehensive view or a complete look at the interlocking sub-systems that operate within a company.

- **Common Data Flows –** It means the use of common input, processing and output procedures and media whenever required. Data is captured by the system analysts only once and as close to its original source as possible. Afterwards, they try to utilize a minimum of data processing procedures and sub-systems to process the data and strive to minimize the number of output documents and reports produced by the system. This eliminates duplication in data collections, simplifies operations and produces an efficient information system.
- **Heavy Planning Element –** An MIS usually takes one to three years and sometimes even longer period to get established firmly within a company. Therefore, a MIS designer must be present in MIS development and should consider future enterprise objectives and requirements of information as per the organization structure of the enterprise as per requirements.
- **Sub System Concept –** Even though the information system is viewed as a single entity, it must be broken down into digestible sub-systems, which can be implemented one at a time by developing a phased plan. The breaking down of MIS into meaningful sub-systems sets the stage for this phasing plan.
- **Common Database –** Database is the mortar that holds the functional systems together. It is defined as a "super-file", which consolidates and integrates data records formerly stored in many separate data files. The organization of a database allows it to be accessed by several information sub-systems and thus, eliminates the necessity of duplication in data storage, updating, deletion and protection.
- **Computerized -** Though MIS can be implemented without using a computer; the use of computers increases the effectiveness of the system. In fact, its use equips the system to handle a wide variety of applications by providing their information requirements quickly. Other necessary attributes of the computer to MIS are accuracy and consistency in processing data and reduction in clerical staff. These attributes make computer a prime requirement in management information system.

6. Information is a strategic resource that helps enterprises in achieving long term objectives and goals. In today's dynamic business environment, it becomes mandatory to have complete information and knowledge of customer buying habits and market strategy for any enterprise. Timeliness, accurate, meaningful and action oriented information enhances an organization ability and capacity to deal with and develop in mission, competition, performance and change. The information can be categorized based on its requirement by the top, middle and lower level management.

- Top level management strives for the information that can help them in major policy decisions such as establishment of new plant, launching of new product etc. In other

words, we can say that the top management requires strategic information that helps them in making strategy of an enterprise in terms of scope of products, targets of products i.e. customers, competition with market i.e. price, quality, long term planning etc.

- Middle management requires tactical information that helps in implementing decisions taken by the top management. For example - information of customers likely to purchase certain product in a particular location can help sales managers to fulfill their sales target efficiently. Tactical information is used for short term planning whereas strategy information is used for long term planning. For example, the offers of companies during festive seasons are a short-term planning, which is done by having information about the customers buying capacity in that location.
- The lower management requires operational information, which is required in day-to-day activities. The operational information mainly comprises of information about stock on hand, information about customer order pending, information about bill payable by customer etc. These are essential for smooth running of the daily activities of a business at primary level. For example, if a regular customer demands for a product other than the daily purchase then this information is important for salesman because it will help him in providing better service.

7. **Segregation of Duties:** Segregation of Duties (SoD) refers to the concept of distribution of work responsibilities such that individual employees are performing only the duties stipulated for their respective jobs and positions. The main purpose is to prevent or detect errors or irregularities by applying suitable controls. It reduces the likelihood of errors and wrongful acts going undetected because the activities of one group or individual will serve as a check on the activities of the other. The irregularities are frauds due to various facts like Theft of assets like funds, IT equipment, the data and programs; Modification of the data leading to misstated and inaccurate financial statements; and Modification of programs in order to perpetrate irregularities like rounding down, salami etc.

   Examples of Segregation of Duties are as follows:

   - Systems software programming group from the application programming group;
   - Database administration group from other data processing activities;
   - Computer hardware operations from the other groups;
   - Systems analyst function from the programming function;
   - Physical, data, and online security group(s) from the other IS functions; and
   - IS Audit from business operations groups.

   From a functional perspective, segregation of duties should be maintained between the Information systems use; Data entry; Computer operation; Network management; System administration; Systems development and maintenance; Change management; Security administration, and Security audit.

8. From the perspective of environmental exposures and controls, Information systems resources may be categorized as follows (with the primarily focus on facilities):

- **Hardware and Media:** This includes Computing Equipment, Communication equipment, and Storage Media.
- **Information Systems Supporting Infrastructure or Facilities:** This typically includes Physical Premises like Computer Rooms, Cabins, Server Rooms, Data Centre premises, Printer Rooms, Remote facilities; Staging Room, and Storage Areas; Communication Closets; Cabling ducts; Power Source, and Heating, Ventilation and Air Conditioning (HVAC).
- **Documentation:** Physical and geographical documentation of computing facilities with emergency excavation plans and incident planning procedures.
- **Supplies:** The third-party maintenance procedures viz. air-conditioning, fire safety, and civil contractors whose entry and assess with respect to their scope of work assigned are to be monitored and logged.
- **People:** The employees, contract employees, visitors, supervisors and third party maintenance personnel are to be made responsible and accountable for environmental controls in their respective Information Processing Facility (IPF). Training of employees and other stake holders on control procedures is a critical component.

9. Some of the Application and Monitoring System Access Controls are as follows:

- **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. Controls are implemented on the access rights of users. For example, read, write, delete, and execute. And ensure that sensitive output is sent only to authorized terminals and locations.
- **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. Monitoring system access and use is a detective control, to check if preventive controls discussed so far are working. If not, this control will detect and report any unauthorized activities.
- **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. An intruder may penetrate the system by trying different passwords and user ID combinations. All incoming and outgoing requests along with attempted access should be recorded in a transaction log. The log should record the user ID, the time of the access and the terminal location from where the request has been originated.

- **Monitor system use:** Based on the risk assessment, a constant monitoring of some critical systems is essential. Define the details of types of accesses, operations, events and alerts that will be monitored. The extent of detail and the frequency of the review would be based on criticality of operation and risk factors. The log files are to be reviewed periodically and attention should be given to any gaps in these logs.
- **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.

10. While developing a Business Continuity Plan, the key tasks that should be covered in the second phase 'Vulnerability Assessment and General definition of Requirement' are given as follows:

- A thorough Security Assessment of the computing and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security; insurance; security planning and administration; application controls; and personal computers.
- The Security Assessment will enable the project team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.
- Present findings and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.
- Define the scope of the planning effort.
- Analyze, recommend and purchase recovery planning and maintenance software required to support the development of the plans and to maintain the plans current following implementation.
- Develop a Plan Framework.
- Assemble Project Team and conduct awareness sessions.

11. The following factors should be verified while auditing or self-assessment of the enterprise's Business Continuity Management (BCM) program:

- 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.

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 center 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 Feasibility Study is carried out by the system analysts, which refers to a process of evaluating alternative systems through cost/benefit analysis so that the most feasible and desirable system can be selected for development. The Feasibility Study of a system is evaluated under following dimensions described briefly as follows:

- **Technical Feasibility:** It may try to answer, whether implementation of the project viable using current technology? It is concerned with issues pertaining to hardware and software. Essentially, an analyst ascertains whether the proposed system is feasible with existing or expected computer hardware and software technology.
- **Financial Feasibility:** The solution proposed may be prohibitively costly for the user organization. For example, Monitoring the stock through VSAT network connecting multiple locations may be acceptable for an organization with high turnover. But this may not be a viable solution for smaller ones.
- **Economic Feasibility:** It includes an evaluation of all the incremental costs and benefits expected if the proposed system is implemented. After problems or opportunities are identified, the analysts must determine the scale of response needed to meet the user's requests for a new system as well as the approximate amount of time and money that will be required in the effort.

- **Schedule or Time Feasibility:** Schedule feasibility involves the design team's estimating how long it will take a new or revised system to become operational and communicating this information to the steering committee. For example, if a design team projects that it will take 16 months for a particular system design to become fully functional, the steering committee may reject the proposal in favor of a simpler alternative that the company can implement in a shorter time frame.
- **Resources Feasibility:** This focuses on human resources. Implementing sophisticated software solutions becomes difficult at specific locations because of the reluctance of skilled personnel to move to such locations.
- **Operational Feasibility:** It is concerned with ascertaining the views of workers, employees, customers and suppliers about the use of computer facility. A system can be highly feasible in all respects except the operational and fails miserably because of human problems.
- **Behavioral Feasibility:** It refers to the systems, which is to be designed to process data and produce the desired outputs. However, if the data input for the system is not readily available or collectable, then the system may not be successful.
- **Legal Feasibility:** Legal feasibility is largely concerned with whether there will be any conflict between a newly proposed system and the organization's legal obligations. Any system, which is liable to violate the local legal requirements, should also be rejected. For example, a revised system should comply with all applicable statutes about financial and statuary reporting requirements, as well as the company's contractual obligations.

14. Two primary methods which are used for the analysis of the scope of a project in System Development Life Cycle (SDLC) are as follows:

- **Reviewing Internal Documents:** The analysts conducting the investigation first try to learn about the organization involved in, or affected by, the project. For example, to review an inventory system proposal, an analyst may try to know how the inventory department operates and who are the managers and supervisors. Analysts can usually learn these details by examining organization charts and studying written operating procedures.
- **Conducting Interviews:** Written documents tell the analyst how the systems should operate, but they may not include enough details to allow a decision to be made about the merits of a systems proposal, nor do they present users' views about current operations. To learn these details, analysts use interviews. Interviews allow analysts to know more about the nature of the project request and the reasons for submitting it. Usually, preliminary investigation interviews involve only management and supervisory personnel.

15. Some strengths of Agile Model, identified by the experts and practitioners include the following:

- Agile methodology has the concept of an adaptive team, which enables to respond to the changing requirements.
- The team does not have to invest time and efforts and finally find that by the time they delivered the product, the requirement of the customer has changed.
- Face to face communication and continuous inputs from customer representative leaves a little space for guesswork.
- The documentation is crisp and to the point to save time.
- The end result is generally the high-quality software in least possible time duration and satisfied customer.

Some of the weaknesses of Agile Model, identified by the experts and practitioners include the following:

- In case of some software deliverables, especially the large ones, it is difficult to assess the efforts required at the beginning of the software development life cycle.
- There is lack of emphasis on necessary designing and documentation.
- Agile increases potential threats to business continuity and knowledge transfer. By nature, Agile projects are extremely light on documentation because the team focuses on verbal communication with the customer rather than on documents or manuals.
- Agile requires more re-work and due to the lack of long-term planning and the lightweight approach to architecture, re-work is often required on Agile projects when the various components of the software are combined and forced to interact.
- The project can easily get taken off track if the customer representative is not clear about the final outcome.
- Agile lacks the attention to outside integration.

16. (i) PQR Ltd. is looking for a suitable IS auditor. I hereby explain my suitability for the same, as I hereby announce that I possess the desired skill set that is generally expected to be with an IS auditor which includes the following:

- Sound knowledge of business operations, practices and compliance requirements;
- Possess the requisite professional technical qualification and certifications;
- A good understanding of information Risks and Controls;
- Knowledge of IT strategies, policy and procedural controls;
- Ability to understand technical and manual controls relating to business continuity; and

- Good knowledge of Professional Standards and Best Practices of IT controls and security.

Note

On Page No. 7.16 of January 2017 edition of Practice Manual, Question No. 19 and corresponding answer provided are erroneously misprinted. You are advised to refer to the Question no 16(i) to obtain the clarity on the same.

(ii) Some of the legal considerations and Audit Standards that Mr. X must consider as a part of his preliminary investigation are as follows:

- The auditor should carefully evaluate the legal as well as statutory implications on his/her audit work.
- The Information Systems audit work could be required as part of a statutory requirement in which case he should take into consideration the related stipulations, regulations and guidelines for conduct of his audit.
- The statutes or regulatory framework may impose stipulations as regards minimum set of control objectives to be achieved by the subject organization. Sometimes, this may also include restrictions on the use of certain types of technologies e.g. freeware, shareware etc.
- The IS Auditor should also consider the Audit Standards applicable to his conduct and performance of audit work. Non-compliance with the mandatory audit standards would not only impact on the violation of the code of professional ethics but also have an adverse impact on the auditor's work.

17. Accounting Audit Trail of Input Controls is as follows:

- The identity of the person(organization) who was the source of the data;
- The identity of the person(organization) who entered the data into the system;
- The time and date when the data was captured;
- The identifier of the physical device used to enter the data into the system;
- The account or record to be updated by the transaction;
- The standing data to be updated by the transaction;
- The details of the transaction; and
- The number of the physical or logical batch to which the transaction belongs.

Operations Audit Trail of Input Controls is as follows:

- Time to key in a source document or an instrument at a terminal;

- Number of read errors made by an optical scanning device;
- Number of keying errors identified during verification;
- Frequency with which an instruction in a command language is used; and
- Time taken to invoke an instruction using a light pen versus a mouse.

18. **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. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities. 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.

19. Details of the IT Infrastructure Library (ITIL) Framework are as follows:

(a) **Service Strategy:** The centre and origin point of the ITIL Service Lifecycle, the ITIL Service Strategy (SS) volume, provides guidance on clarification and prioritization of service-provider investments in services. It provides guidance on leveraging service

management capabilities to effectively deliver value to customers and illustrate value for service providers. The Service Strategy volume provides guidance on the design, development, and implementation of service management, not only as an organizational capability, but also as a strategic asset. It provides guidance on the principles underpinning the practice of service management to aid the development of service management policies, guidelines, and processes across the ITIL Service Lifecycle.

(b) Service Design: Service Design translates strategic plans and objectives and creates the designs and specifications for execution through service transition and operations. It provides guidance on combining infrastructure, applications, systems, and processes, along with suppliers and partners, to present feasible service offerings. It includes design principles and methods for converting strategic objectives into portfolios of services and service assets. The Service Design volume provides guidance on the design and development of services and service management processes. It includes design principles and methods for converting strategic objectives into portfolios of services and service assets.

(c) Service Transition: Service Transition provides guidance on the service design and implementation ensuring that the service delivers the intended strategy and that it can be operated and maintained effectively. Service Transition planning provides guidance on managing the complexity of changes to services and service management processes to prevent undesired consequences whilst permitting for innovation. It provides guidance on the support mechanism on transferring the control of services between customers and service providers. The Service Transition volume provides guidance on the development and improvement of capabilities for transitioning new and changed services into operations.

(d) Service Operation: Service Operation provides guidance on the management of a service through its day-to-day production life. It also provides guidance on supporting operations by means of new models and architectures such as shared services, utility computing, web services, and mobile commerce.

(e) Continual Service Improvement: Continual Service Improvement provides guidance on the measurement of service performance through the service life-cycle, suggesting improvements to ensure that a service delivers the maximum benefit. This volume provides guidance on creating and maintaining value for customers through improved design, introduction, and operation of services. It combines principles, practices, and methods from change management, quality management, and capability improvement to achieve incremental and significant improvements in service quality, operational efficiency, and business continuity.

20. Limitations of Mobile Computing are as follows:

- **Insufficient Bandwidth:** Mobile Internet access is generally slower than direct cable connections using technologies such as General Packet Radio Service (GPRS) and

Enhanced Data for GSM (Global System for Mobile Communication) Evolution (EDGE), and more recently 3G networks. These networks are usually available within range of commercial cell phone towers. Higher speed wireless LANs are inexpensive but have very limited range.

- **Security Standards:** When working mobile, one is dependent on public networks, requiring careful use of Virtual Private Network (VPN). Security is a major concern while concerning the mobile computing standards on the fleet. One can easily attack the VPN through a huge number of networks interconnected through the line.
- **Power consumption:** When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power. Combined with the compact size of many mobile devices, this often means unusually expensive batteries must be used to obtain the necessary battery life. Mobile computing should also look into Greener IT in such a way that it saves the power or increases the battery life.
- **Transmission interferences:** Weather, terrain, and the range from the nearest signal point can all interfere with signal reception. Reception in tunnels, some buildings, and rural areas is often poor.
- **Potential health hazards:** People who use mobile devices while driving are often distracted from driving are thus assumed more likely to be involved in traffic accidents. Cell phones may interfere with sensitive medical devices. There are allegations that cell phone signals may cause health problems.
- **Human interface with device:** Screens and keyboards tend to be small, which may make them hard to use. Alternate input methods such as speech or handwriting recognition require training.

21. Web 3.0: The term Web 3.0, also known as the Semantic Web, describes sites wherein the computers will be generated raw data on their own without direct user interaction. Web 3.0 standard uses semantic web technology, drag and drop mash-ups, widgets, user behavior, user engagement, and consolidation of dynamic web contents depending on the interest of the individual users. Web 3.0 technology uses the "Data Web" Technology, which features the data records that are publishable and reusable on the web through query-able formats. The Web 3.0 standard also incorporates the latest researches in the field of artificial intelligence.

An example of typical Web 3.0 application is the one that uses content management systems along with artificial intelligence. These systems are capable of answering the questions posed by the users, because the application is able to think on its own and find the most probable answer, depending on the context, to the query submitted by the user. In this way, Web 3.0 can also be described as a "machine to user" standard in the internet.

The two major components of Web 3.0 are as follows:

- **Semantic Web:** This provides the web user a common framework that could be used

to share and reuse the data across various applications, enterprises, and community boundaries. This allows the data and information to be readily intercepted by machines, so that the machines can take contextual decisions on their own by finding, combining and acting upon relevant information on the web.

- **Web Services:** It is a software system that supports computer-to-computer interaction over the Internet. For example - the popular photo-sharing website Flickr provides a web service that could be utilized and the developers to programmatically interface with Flickr in order to search for images.

22. (a) 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.

(b) Data Dictionary: A Data Dictionary contains descriptive information about the data items in the files of a business information system. Thus, a data dictionary is a computer file about data. Each computer record of a data dictionary contains information about a single data item used in a business information system. This information may include - the identity of the source document(s) used to create the data item; the names of the computer files that store the data item; the names of the computer programs that modify the data item; the identity of the computer programs or individuals permitted to access the data item for the purpose of file maintenance, upkeep, or inquiry; the identity of the computer programs or individuals not permitted to access the data item etc.

Accountants and auditors can also make good use of a data dictionary. For example, a data dictionary can help to establish an audit trail because it can identify the input sources of data items, the computer programs that modify particular data items, and the managerial reports on which the data items are output. When an accountant participates in the design of a new system, a data dictionary can also be used to plan the flow of transaction data through the system.

(c) Audit Hooks: There are audit routines that flag suspicious transactions. For example, internal auditors at Insurance Company determined that their policyholder system was vulnerable to fraud every time a policyholder changed his or her name or address and then subsequently withdrew funds from the policy. They devised a system of audit hooks to tag records with a name or address change. The internal audit department will investigate these tagged records for detecting fraud. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they

occur. This approach of real-time notification displays a message on the auditor's terminal.

(d) **Operational-Level Systems:** These support operational managers in tracking elementary activities. These can include tracking customer orders, invoice tracking, etc. Operational-level systems or Operational Support Systems (OSS) ensure that business procedures are followed. Information systems are required to process the data generated and used in business operations. OSS produces a variety of information for internal and external use. Its role is to effectively process business transactions, control industrial processes, support enterprise communications and collaborations and update corporate database. The main objective of OSS is to improve the operational efficiency of the enterprise. For example- Transaction Processing System (TPS).

(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. If an enterprise undertakes a comprehensive security review program, the threat identification and exposure analysis phases involve identifying those situations that require the emergency plan to be invoked.

23. **(a)** **Tacit knowledge:** Tacit knowledge 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.

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

(b) **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, if 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. ATM in an example of the same.

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.

(c) **Physical Controls:** These controls are groups of transactions that constitute a physical unit. For example – source documents might be obtained via the email, assembled into batches, spiked and tied together, and then given to a data-entry clerk to be entered an application system at a terminal.

Logical Controls: These are group of transactions bound together on some logical basis, rather than being physically contiguous. For example - different clerks might use the same terminal to enter transaction into an application system. Clerks keep control totals of the transactions into an application system.

(d) **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.

(e) **Data as a Service (DaaS):** DaaS provides data on demand to a diverse set of users, systems or application. The data may include text, images, sounds, and videos. Data encryption and operating system authentication are commonly provided for security. DaaS users have access to high-quality data in a centralized place and pay by volume or data type, as needed. However, as the data is owned by the providers, users can only perform read operations on the data. DaaS is highly used in geography data services and financial data services.

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.

24. **(a)** The methodology for developing a Business Continuity Plan emphasizes the following:

(i) Providing management with a comprehensive understanding of the total efforts

required to develop and maintain an effective recovery plan;

(ii) Obtaining commitment from appropriate management to support and participate in the effort;

(iii) Defining recovery requirements from the perspective of business functions;

(iv) Documenting the impact of an extended loss to operations and key business functions;

(v) Focusing appropriately on disaster prevention and impact minimization, as well as orderly recovery;

(vi) Selecting business continuity teams that ensure the proper balance required for plan development;

(vii) Developing a business continuity plan that is understandable, easy to use and maintain;

(viii) Planning the testing of plans in a systematic manner and measuring results of such tests; and

(ix) Defining how business continuity considerations must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.

(b) The objectives of performing Business Continuity Planning (BCP) tests are to ensure that:

- the recovery procedures are complete and workable.
- the competence of personnel in their performance of recovery procedures can be evaluated.
- the resources such as business processes, IS systems, personnel, facilities and data are obtainable and operational to perform recovery processes.
- manual recovery procedures and IT backup system/s are current and can either be operational or restored.
- the success or failure of business continuity training program is monitored.

(c) **Incremental Backup:** Incremental Backup: An Incremental Backup captures files that were created or changed since the last backup, regardless of backup type. The last backup can be a full backup or simply the last incremental backup. With incremental backups, one full backup is done first and subsequent backup runs are just the changed files and new files added since the last backup.

Advantages of incremental Backup are as follows:

- Much faster backups.
- Efficient use of storage space as files is not duplicated. Much less storage space used compared to running full backups and even differential backups.

Disadvantages of Incremental Backup are as follows:

- Restores are slower than with a full backup and differential backups.
- Restores are a little more complicated. All backup sets (first full backup and all incremental backups) are needed to perform a restore.

25. (i) As per Section 7 of the IT Act, 2000, 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.

According to the given facts, Article of the company provides that the *financial* statements of the company shall be maintained for 8 years in electronic form as records. It was the responsibility of the Company to maintain the records in e-form with proper back up. However, its denial from providing of information of past financial statements due to corruption of file is not sufficient ground. In fact, as per the above provision that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if the information contained therein remains accessible so as to be usable for a subsequent reference.

So, Aryan Ltd. failed to comply with the said provision.

(ii) As per Section 9 of the IT Act, 2000, nothing contained in section 7 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

So, accordingly, Aryan Ltd. cannot compel ABC Database Company to retain and preserve any documents in e-form records.

ISCA RTP MAY 2017

PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

Concepts of Governance and Management of Information Systems

1. (a) Discuss Risk Management Strategies in detail.
   (b) What do you understand by "Information Systems Risks"? Discuss broadly the characteristics of risk.
2. Discuss the components of Internal Controls as per COSO (Committee of Sponsoring Organizations).
3. Explain the term "Corporate Governance".

Information Systems Concepts

4. Discuss the system classification 'Based on the Interactive behaviour'.
5. Discuss important characteristics of Computer based Information Systems.
6. Distinguish between Operational Level Systems and Management Level Systems.

Protection of Information Systems

7. What are Detective Controls? Discuss their characteristics.
8. Discuss major ways of protecting the hardware installation against the fire damage.
9. Why is there a need for Quality Assurance Management Controls in enterprises?

Business Continuity Planning and Disaster Recovery Planning

10. Discuss advantages and disadvantages of Differential Backup.
11. Discuss various components of Business Continuity Management (BCM) process.
12. Discuss BCP audit steps with regards to Building, Utilities and Transportation.

Acquisition, Development and Implementation of Information Systems

13. What are the various cost factors that are involved in software development.
14. Discuss the sections of Systems Requirement Specifications (SRS) document.
15. Discuss important factors that should be considered by the system analyst while designing user input/output forms of a user-interface.

Auditing of Information Systems

16. What are the various functions performed by an Information Systems' Auditor?
17. Discuss the major concerns that an auditor should address in evaluating the implementation of Programming Management Controls.

Information Technology Regulatory Issues

18. (a) Discuss the provision given in IT (Amendment) Act, 2008 that gives "Penalty for failure to furnish information return, etc."

    (b) Discuss the Audit Report norms set up by SEBI for System Controls and Audit.

Emerging Technologies

19. Discuss Green Computing Best Practices, in brief.

20. Discuss "Community Cloud" and its characteristics under Cloud Computing environment.

Short Note Based Questions

21. Write short notes on following:

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

    (b) Information Technology General Controls (ITGC)

    (c) Program Debugging

    (d) Data Integrity

    (e) Components of Web 3.0

22. Differentiate between the following:

    (a) Behavioral Feasibility and Legal Feasibility

    (b) Control Risk and Detection Risk

    (c) Manual Logging and Electronic Logging

    (d) Device Risks and Application Risks

Questions based on the Case Studies

23. (a) The enterprise XYZ limited establishes an IT Steering Committee and expects the committee to perform certain role. Can you explain the role of IT Steering committee?

    (b) Furthermore, the management of XYZ limited wants to design an Operating System Access Control mechanism for achieving security policy objective in its computerized environment. Discuss some of the major such control mechanisms.

24. (a) A leading enterprise ABC appoints you to assess and evaluate their system of IT internal controls. What are the key management practices that you would follow to carry out the assignment complying with COBIT 5?

    (b) An owner of a small local store is currently using manual system for his day to day business activities viz. purchase, sales, billing, payments receipts etc. In the last few years, turnover of the store is increased manifold and now it has become increasingly difficult to handle all these activities manually. You being an IT expert and his auditor, are requested to suggest which operation support system will be the most suitable for

him. Also, advise him what activities can be performed by the proposed system and what are the major limitations of it?

25. Mr. A is regularly sending obscene content in electronic form to Ms. B. When Ms. B made a complaint to Police, it was found that all the communications were sent through XYZ network service provider. Police have held both Mr. A and XYZ network service provider as liable for this act. Suggest under what provisions of Information Technology (Amendment) Act, 2008, the XYZ network service provider can get exemption from the liability? Also discuss the relevant provisions of the above section.

SUGGESTED ANSWERS

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

- **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.

2. **Internal Controls as per COSO (Committee of Sponsoring Organizations):** In a computerised environment, the goals of asset safeguarding, data integrity, system efficiency and system effectiveness can be achieved only if an organization's management sets up a system of internal controls. Per COSO, Internal Control is comprised of five interrelated components:

- **Control Environment:** This includes the elements that establish the control context in which specific accounting systems and control procedures must operate. The control environment is manifested in management's operating style, the ways authority and responsibility are assigned, the functional method of the audit committee, the methods used to plan and monitor performance and so on. 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:** This includes the elements that identify and analyze the risks faced by an organisation and the way the risk can be managed. Both external and internal auditors are concerned with errors or irregularities that cause material losses to an organisation. Each business process comes with various risks. A control environment must include an assessment of the risks associated with each business process.

- **Control Activities:** This includes the elements that operate to ensure transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded, and independent checks on performance and valuation of records. These are called accounting controls. Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency objectives. 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:** These are the elements, in which information is identified, captured and exchanged in a timely and appropriate form to allow personnel to discharge their responsibilities. These are associated with control activities regarding information and communication systems of the entity that acts as one of the component of internal accounting system. 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. This includes the elements that ensure internal controls operate reliably over time. The best internal controls are worthless if the company does not monitor them and make changes when they are not working.

3. **Corporate Governance or Conformance:** Corporate Governance is defined as the system by which a company or enterprise is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance. Corporate Governance refers to the structures and processes for the direction and control of companies. Corporate governance concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders. The corporate governance provides a historic view and focuses on regulatory requirements. This covers corporate governance issues such as: Roles of the chairman and CEO, Role and composition of the board of directors, Board committees, Controls assurance and Risk management for compliance.

   (i) Good corporate governance contributes to sustainable economic development by enhancing the performance of companies and increasing their access to outside capital. It is about doing good business to protect shareholders' interest. Corporate Governance drives the corporate information needs to meet business objectives.

   (ii) Good corporate governance requires sound internal control practices such as segregation of incompatible functions, elimination of conflict of interest, establishment of Audit Committee, risk management and compliance with the relevant laws and standards including corporate disclosure requirements. These are intended to guide companies to achieve their business objectives in a manner such that those who are entrusted with the resources or power to run the companies, meet stakeholder needs

without compromising the shareholders' interest. Corporate governance is thus necessary for the purpose of monitoring and measuring the performance of these committees.

(iii) Regulatory requirements and standards generally address corporate governance with compliance being subject to assurance and/or audit. There are established oversight mechanisms for the board to ensure that good corporate governance processes are effective. These might include committees composed mainly or wholly of independent non-executive directors, particularly the audit committee or its equivalent in countries where the two tier board system is the norm.

(iv) Good corporate governance is important and it is critical so that any weakness in this area is addressed properly. However, good corporate governance by itself cannot make an organization successful. There is always a risk that inadequate attention is paid to the need for enterprises to create wealth or stakeholder value. Hence, it is important to remember that strategy and performance are also very important.

4. System Classification based on the Interactive behavior: may be classified as Open Systems or Closed System. The classification is based on 'how the system interacts with environment'.

- An **Open System** interacts with other systems in its environment. For example; Information system is an open system because it takes input from the environment and produces output to the environment, which changes as per the changes in the environment.
- **Closed System** does not interact with the environment and does not change with the changes in environment. Consider a 'throw-away' type sealed digital watch, which is a system, composed of several components that work in a cooperative fashion designed to perform some specific task. This watch is a closed system as it is completely isolated from its environment for its operation.

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

- All systems work for predetermined objectives and the system is designed and developed accordingly.
- In general, a system has several 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.

6. **Operational-Level Systems:** These support operational managers in tracking elementary activities. These can include tracking customer orders, invoice tracking, etc. Operational-level systems or Operational Support Systems (OSS) ensure that business procedures are followed. Information systems are required to process the data generated and used in business operations. OSS produces a variety of information for internal and external use. Its role is to effectively process business transactions, control industrial processes, support enterprise communications and collaborations and update corporate database. The main objective of OSS is to improve the operational efficiency of the enterprise. These are further categorized as follows:

   Management-Level Systems: These support the middle managers in monitoring, decision-making and administrative activities and are helpful in answering questions like - Are things working well and in order? These provide periodic reports rather than instant information on operations. For example - a college control system gives report on the number of leaves availed by the staff, salary paid to the staff, funds generated by the fees, finance planning etc. These types of systems mainly answer "what if" questions. For example - What would be quality of teaching if college must achieve top ranking in academics? These types of questions can be answered only after getting new data from outside the organization, as well as data from inside which cannot be easily obtained from existing operational level systems. Management Information System and Decision Support Systems are types of Management Level systems.

7. **Detective Controls:** These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. An example of a detective control would be a use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend. Examples of detective controls include Hash totals; Check points in production jobs; Echo control in telecommunications; Error message over tape labels; Duplicate checking of calculations; Periodic performance reporting with variances; Past-due accounts report; The internal audit functions; Intrusion detection system; Cash counts and bank reconciliation, and monitoring expenditures against budgeted amount.

   The main characteristics of Detective controls are as follows:

   - Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc.;
   - An established mechanism to refer the reported unlawful activities to the appropriate person or group;
   - Interaction with the preventive control to prevent such acts from occurring; and
   - Surprise checks by supervisor.

8. Some of the major ways of protecting the hardware installation against fire damage are as follows:

- Both automatic and manual fire alarms may be placed at strategic locations and a control panel may be installed to clearly indicate this;
- Besides the control panel, master switches may be installed for power and automatic fire suppression system. Different fire suppression techniques like Dry-pipe sprinkling systems, water based systems, halon etc., depending upon the situation may be used;
- Manual fire extinguishers can be placed at strategic locations;
- Fireproof Walls; Floors and Ceilings surrounding the Computer Room and Fire Resistant Office Materials such as wastebaskets, curtains, desks, and cabinets should be used;
- 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 system. The procedures to be followed during an emergency should be properly documented are Fire Alarms, Extinguishers, Sprinklers, Instructions / Fire Brigade Nos., Smoke detectors, and Carbon dioxide based fire extinguishers;
- Less Wood and plastic should be in computer rooms;
- Use a gas based fire suppression system;
- To reduce the risk of firing, the location of the computer room should be strategically planned and should not be located in the basement or ground floor of a multi-storey building;
- Regular Inspection by Fire Department should be conducted;
- Fire repression systems should be supplemented and not replaced by smoke detectors;
- **Documented and Tested Emergency Evacuation Plans:** Relocation plans should emphasize human safety, but should not leave information processing facilities physically unsecured. Procedures should exist for a controlled shutdown of the computer in an emergency situation. In all circumstances saving human life should be given paramount importance;
- **Smoke Detectors:** Smoke detectors are positioned at places above and below the ceiling tiles. Upon activation, these detectors should produce an audible alarm and must be linked to a monitored station (for example, a fire station); and
- **Wiring Placed in Electrical Panels and Conduit:** Electrical fires are always a risk. To reduce the risk of such a fire occurring and spreading, wiring should be placed in the fire resistant panels and conduit. This conduit generally lies under the fire-resistant raised floor in the computer room.

9. 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.

10. Advantages of Differential Backup are as follows:

- Restores are fast and easy to manage as the entire list of files and folders are in one backup set.
- Easy to maintain and restore different versions.

Disadvantages of Differential Backup are as follows:

- Backups can take very long as each file is backed up again every time the full backup is run.
- Consumes the most storage space compared to incremental and differential backups. The exact same files are stored repeatedly resulting in inefficient use of storage.

11. Components of Business Continuity Management (BCM) Process are as follows:

- **BCM – Process:** The management process enables the business continuity, capacity and capability to be established and maintained. The capacity and capability are established in accordance to the requirements of the enterprise.

- **BCM – Information Collection Process:** The activities of assessment process do the prioritization of an enterprise's products and services and the urgency of the activities that are required to deliver them. This sets the requirements that will determine the selection of appropriate BCM strategies in the next process.
- **BCM – Strategy Process:** Finalization of business continuity strategy requires assessment of a range of strategies. This requires an appropriate response to be selected at an acceptable level and during and after a disruption within an acceptable timeframe for each product or service, so that the enterprise continues to provide those products and services. The selection of strategy will take into account the processes and technology already present within the enterprise.
- **BCM – Development and Implementation Process:** Development of a management framework and a structure of incident management, business continuity and business recovery and restoration plans.
- **BCM – Testing and Maintenance Process:** BCM testing, maintenance and audit testify the enterprise BCM to prove the extent to which its strategies and plans are complete, current and accurate; and Identifies opportunities for improvement.
- **BCM – Training Process:** Extensive trainings in BCM framework, incident management, business continuity and business recovery and restoration plans enable it to become part of the enterprise's core values and provide confidence in all stakeholders in the ability of the enterprise to cope with minimum disruptions and loss of service.

12. BCP audit steps with regards to Building, Utilities and Transportation are as follows:

- Does the disaster recovery/ business resumption plan have a provision for having a building engineer inspect the building and facilities soon after a disaster so that damage can be identified and repaired to make the premises safe for the return of employees as soon as possible?
- Does the disaster recovery/business resumption plan consider the need for alternative shelter, if needed? Alternatives in the immediate area may be affected by the same disaster.
- Review any agreements for use of backup facilities.
- Verify that the backup facilities are adequate based on projected needs (telecommunications, utilities, etc.). Will the site be secure?
- Does the disaster recovery/ business resumption plan consider the failure of electrical power, natural gas, toxic chemical containers, and pipes?
- Are building safety features regularly inspected and tested?

- Does the plan consider the disruption of transportation systems? This could affect the ability of employees to report to work or return home. It could also affect the ability of vendors to provide the goods needed in the recovery effort.

13. Various cost factors that are involved in software development are as follows:

- **Development Costs:** Development Costs for a computer based information system include costs of the system development process, like salaries of developers.
- **Operating Costs:** Operating Costs of a computer based information system including hardware/software rental or depreciation charges; salaries of computer operators and other data processing personnel, who will operate the new system.
- **Intangible Costs:** Intangible Cost that cannot be easily measured. For example, the development of a new system may disrupt the activities of an organization and cause a loss of employee productivity or morale.

14. **Systems Specification:** At the end of the analysis phase, the systems analyst prepares a document called **Systems Requirement Specifications (SRS)**. A well-documented SRS may normally contains the following sections:

- **Introduction:** Goals, Objectives, software context, Scope and Environment of the computer-based system.
- **Information Description:** Problem description; Information content, flow and structure; Hardware, software, human interfaces for external system elements and internal software functions.
- **Functional Description:** Diagrammatic representation of functions; Processing narrative for each function; Interplay among functions; Design constraints.
- **Behavioral Description:** Response to external events and internal controls.
- **Validation Criteria:** Classes of tests to be performed to validate functions, performance and constraints.
- **Appendices:** Data flow/Object Diagrams; Tabular Data; Detailed description of algorithms charts, graphs and other such material.
- **SRS Review:** The development team makes a presentation and then hands over the SRS document to be reviewed by the user or customer. The review reflects the development team's understanding of the existing processes. Only, after ensuring that the document represents existing processes accurately, the user should sign the document. This is a technical requirement of the contract between users and development team/organization.

15. Important factors which should be considered by the system analyst while designing user input/ output forms of a user-interface are as follows:

Characteristic	Definition	Input Design	Output Design
Content	Refers to the actual pieces of data to be gathered to produce the required output to be provided to users.	The analyst is required to consider the types of data that are needed to be gathered to generate the desired user outputs. New documents for collecting such information may be designed.	The contents of a weekly output report to a sales manager might consist of sales person's name, sales calls made by each sales person during the week, and the amount of each product sold by each salesperson to each major client category.
Timeliness	Timeliness refers to when users need outputs, which may be required on a regular, periodic basis - perhaps daily, weekly, monthly, at the of quarter or annually.	Data needs to be 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.	A sales manager, may be requiring a weekly sales report. Other users, such as airline agents, require both real- time information and rapid response times in order to render better client service.
Format	Input format refers to the manner in which data are physically arranged. Output format refers to the arrangement referring to data output on a printed report or in a display screen.	After the data contents and media requirements are determined, input formats are designed on the basis of few constraints like - the type and length of each data field as well as any other special characteristics (number decimal places etc.).	Format of information reports for the users should be so devised that it assists in decision-making, identifying and solving problems, planning and initiating corrective action and searching.
Media	Input-output medium refers to the physical device used for	This includes the choice of input media and subsequently the	A variety of output media are available in the market these days

	input, storage or output.	devices on which to enter the data. Various user input alternatives may include display workstations, magnetic tapes, magnetic disks, key-boards, optical character recognition, pen-based computers and voice input etc. A suitable medium may be selected depending on the application to be computerized.	which include paper, video display, microfilm, magnetic tape/disk and voice output.
Form	Form refers to the way the information is inputted in the input form and the content is presented to users in various output forms - quantitative, non-quantitative, text, graphics, video and audio.	Forms are pre-printed papers that require people to fill in responses in a standardized way. Forms elicit and capture information required by organizational members that often will be input to the computer. Through this process, forms often serve as source documents for the data entry personnel.	The form of the output should be decided keeping in view the requirements for the concerned user. For example - Information on distribution channels may be more understandable to the concerned manager if it is presented in the form of a map, with dots representing individual outlets for stores.
Input Volume/ Output Volume	Input volume refers to the amount of data that has to be entered in the computer system at any one time. The amount of data output required at any one time is	In some decision-support systems and many real-time processing systems, input volume is light. In batch-oriented transaction processing systems, input volume could be heavy which involves	It is better to use high-speed printer or a rapid-retrieval display unit, which are fast and frequently used output devices in case the volume is heavy.

	known as output volume.	thousands of records that are handled by a centralized data entry department using key-to-tape or key-to-disk systems.	

16. Information Systems' Auditor often is the assessor of business risk, as it relates to the use of IT, to management. The auditor can check the technicalities well enough to understand the risk and make a sound assessment and present risk-oriented advice to management. IS Auditors review risks relating to IT systems and processes; some of them are as follows:

- Inadequate information security controls (e.g. missing or out of date antivirus controls, open ports, open systems without password or weak passwords etc.);
- Inefficient use of resources, or poor governance (e.g. huge spending on unnecessary IT projects like printing resources, storage devices, high power servers and workstations etc.);
- Ineffective IT strategies, policies and practices (including a lack of policy for use of Information and Communication Technology (ICT) resources, Internet usage policies, Security practices etc.); and
- IT-related frauds (including phishing, hacking etc.).

17. Some of the major concerns that an Auditor should address under different activities involved in Programming Management Control Phase are as under:

Phase	Audit Trails
Planning	• They should evaluate whether the nature of and extent of planning are appropriate to the different types of software that are developed or acquired. • They must evaluate how well the planning work is being undertaken.
Control	• They must evaluate whether the nature of an extent of control activities undertaken are appropriate for the different types of software that are developed or acquired. • They must gather evidence on whether the control procedures are operating reliably. For example - they might first choose a sample if past and current software development and acquisition projects carried out at different locations in the organization they are auditing.
Design	• Auditors should find out whether programmers use some type of systematic approach to design.

	• Auditors can obtain evidence of the design practices used by undertaking interviews, observations, and reviews of documentation.
Coding	• Auditors should seek evidence – o On the level of care exercised by programming management in choosing a module implementation and integration strategy. o To determine whether programming management ensures that programmers follow structured programming conventions. o To check whether programmers employ automated facilities to assist them with their coding work.
Testing	• Auditors can use interviews, observations, and examination of documentation to evaluate how well unit testing is conducted. • Auditors are most likely concerned primarily with the quality of integration testing work carried out by information systems professionals rather than end users. • Auditors primary concern is to see that whole-of-program tests have been undertaken for all material programs and that these tests have been well-designed and executed.
Operation and Maintenance	• Auditors need to ensure effectively and timely reporting of maintenance needs occurs and maintenance is carried out in a well-controlled manner. • Auditors should ensure that management has implemented a review system and assigned responsibility for monitoring the status of operational programs.

18. (a) [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.

(b) The Securities and Exchange Board of India (SEBI) is the regulator for the securities market in India. The Audit Report Norms set up by SEBI for System Controls and Audit are as follows:

- The Systems Audit Reports and Compliance Status should be placed before the Governing Board of the Stock Exchanges/Depositories and the system audit report along with comments of Stock Exchanges / Depositories should be communicated to SEBI.
- The Audit report should have explicit coverage of each Major Area mentioned in the TOR, indicating any Nonconformity (NCs) or Observations (or lack of it). For each section, auditors should also provide qualitative input about ways to improve the process, based upon the best practices observed.

19. Some of the best practices of Green Computing are as follows:

Develop a sustainable Green Computing plan

- Involve stakeholders to include checklists, recycling policies, recommendations for disposal of used equipment, government guidelines and recommendations for purchasing green computer equipment in organizational policies and plans;
- Encourage the IT community for using the best practices and encourage them to consider green computing practices and guidelines.
- On-going communication about and campus commitment to green IT best practices to produce notable results.
- Include power usage, reduction of paper consumption, as well as recommendations for new equipment and recycling old machines in organizational policies and plans; and
- Use cloud computing so that multiple organizations share the same computing resources thus increasing the utilization by making more efficient use of hardware resources.

Recycle

- Dispose e-waste according to central, state and local regulations;
- Discard used or unwanted electronic equipment in a convenient and environmentally responsible manner as computers emit harmful emissions;
- Manufacturers must offer safe end-of-life management and recycling options when products become unusable; and
- Recycle computers through manufacturer's recycling services.

Make environmentally sound purchase decisions

- Purchase of desktop computers, notebooks and monitors based on environmental attributes;
- Provide a clear, consistent set of performance criteria for the design of products;
- Recognize manufacturer efforts to reduce the environmental impact of products by reducing or eliminating environmentally sensitive materials, designing for longevity and reducing packaging materials; and
- Use Server and storage virtualization that can help to improve resource utilization, reduce energy costs and simplify maintenance.

Reduce Paper Consumption

- Reduce paper consumption by use of e-mail and electronic archiving;
- Use of "track changes" feature in electronic documents, rather than redline corrections on paper;
- Use online marketing rather than paper based marketing; e-mail marketing solutions that are greener, more affordable, flexible and interactive than direct mail; free and low-cost online invoicing solutions that help cut down on paper waste; and
- While printing documents; make sure to use both sides of the paper, recycle regularly, use smaller fonts and margins, and selectively print required pages.

Conserve Energy

- Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors;
- Develop a thin-client strategy wherein thin clients are smaller, cheaper, simpler for manufacturers to build than traditional PCs or notebooks and most importantly use about half the power of a traditional desktop PC;
- Use notebook computers rather than desktop computers whenever possible;
- Use the power-management features to turn off hard drives and displays after several minutes of inactivity;
- Power-down the CPU and all peripherals during extended periods of inactivity;
- Try to do computer-related tasks during contiguous, intensive blocks of time, leaving hardware off at other times;
- Power-up and power-down energy-intensive peripherals such as laser printers per need;
- Employ alternative energy sources for computing workstations, servers, networks and data centres; and

- Adapt more of Web conferencing offers instead of travelling to meetings to go green and save energy.

20. Community Cloud: The community cloud is the cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (eg. mission security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises. In this, a private cloud is shared between several organizations. Fig. 8.3.6 depicts Community Cloud. This model is suitable for organizations that cannot afford a private cloud and cannot rely on the public cloud either.

Characteristics of Community Clouds 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.

21. (a) 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.

(b) Information Technology General Controls (ITGC) are the basic policies and procedures that ensure that an organization's information systems are properly safeguarded, that application programs and data are secure, and that computerized operations can be recovered in case of unexpected interruptions. 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. Failure to ensure these controls are designed and operating effectively means that there will not be any assurance over the IT Application Controls.

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.

(c) **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.

(d) **Data Integrity:** Data integrity is a reflection of the accuracy, correctness, validity, and currency of the data. The primary objective of data integrity control techniques is to prevent, detect, and correct errors in transactions as they flow through various stages of a specific date processing program. In other words, they ensure the integrity of a specific application's inputs, stored data, programs, data transmissions, and outputs. Data integrity controls protect data from accidental or malicious alteration or destruction and provide assurance to the user that the information meets expectations about its quality and integrity. Assessing data integrity involves evaluating the following critical procedures:

- Virus detection and elimination software is installed and activated.
- Data integrity and validation controls are used to provide assurance that the information has not been altered and the system functions as intended

(e) The two major components of Web 3.0 are as follows:

- **Semantic Web:** This provides the web user a common framework that could be used to share and reuse the data across various applications, enterprises, and community boundaries. This allows the data and information to be readily intercepted by machines, so that the machines are able to take contextual decisions on their own by finding, combining and acting upon relevant

information on the web.

- **Web Services:** It is a software system that supports computer-to-computer interaction over the Internet. For example - the popular photo-sharing website Flickr provides a web service that could be utilized and the developers to programmatically interface with Flickr in order to search for images.

22. (a) **Behavioral Feasibility:** It refers to the systems, which is to be designed to process data and produce the desired outputs. However, if the data input for the system is not readily available or collectable, then the system may not be successful.

Legal Feasibility: Legal feasibility is largely concerned with whether there will be any conflict between a newly proposed system and the organization's legal obligations. Any system, which is liable to violate the local legal requirements, should also be rejected. For example, a revised system should comply with all applicable statutes about financial and statuary reporting requirements, as well as the company's contractual obligations.

(b) **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.

(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) **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'.

23. (a) **IT Steering Committee:** Planning is essential for determining and monitoring the direction and achievement of the enterprise goals and objectives. As enterprises are dependent on the information generated by information systems, it is important that planning relating to information systems is undertaken by senior management or by the steering committee. Depending on the size and needs of the enterprise, the senior management may appoint a high-level committee to provide appropriate direction to IT deployment and information systems and to ensure that the information technology deployment is in tune with the enterprise business goals and objectives. This committee called as the IT Steering Committee is ideally led by a member of the Board of Directors and comprises of functional heads from all key departments of the enterprise including the audit and IT department.

The key functions of the committee would include of the following:

- To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives;
- To establish size and scope of IT function and sets priorities within the scope;
- To review and approve major IT deployment projects in all their stages;
- To approve and monitor key projects by measuring result of IT projects in terms of return on investment, etc.;
- To review the status of IS plans and budgets and overall IT performance;
- To review and approve standards, policies and procedures;
- To make decisions on all key aspects of IT deployment and implementation;
- To facilitate implementation of IT security within enterprise;
- To facilitate and resolve conflicts in deployment of IT and ensure availability of a viable communication system exists between IT and its users; and
- To report to the Board of Directors on IT activities on a regular basis.

(b) Operating System is the computer control program. It allows users and their applications to share and access common computer resources, such as processor, main memory, database and printers. Major tasks of O/S are Scheduling Jobs; Managing Hardware and Software Resources; Maintaining System Security; Enabling Multiple User Resource Sharing; Handling Interrupts and Maintaining Usage Records.

Operating system security involves policy, procedure and controls that determine, 'who can access the operating system,' 'which resources they can access', and 'what action they can take'. Operating system provides the platform for an application to use various IS resources and perform the specific business function. Some of the major control mechanisms are as follows:

- **Automated terminal identification:** This will help to ensure that a particular session could only be initiated from a particular location or computer terminal.
- **Terminal log-in procedures:** A log-in procedure is the first line of defence against unauthorized access. The log-in procedure does not provide unnecessary help or information, which could be misused by an intruder. When the user initiates the log-on process by entering user-id and password, the system compares the ID and password to a database of valid users. If the system finds a match, then log-on attempt is authorized. If password or user-id is entered incorrectly, then after a specified number of wrong attempts, the system should lock the user from the system.
- **Access Token:** If the log on attempt is successful, the Operating System creates an access token that contains key information about the user including user-id, password, user group and privileges granted to the user. The information in the access token is used to approve all actions attempted by the user during the session.
- **Access Control List:** This list contains information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compasses his or her user-id and privileges contained in the access token with those contained in the access control list. If there is a match, the user is granted access.
- **Discretionary Access Control:** The system administrator usually determines; who is granted access to specific resources and maintains the access control list. For example, the controller who is owner of the general ledger grants read only privilege to the budgeting department while accounts payable manager is granted both read and write permission to the ledger.
- **User identification and authentication:** The users must be identified and authenticated in a foolproof manner. Depending on risk assessment, more stringent methods like Biometric Authentication or Cryptographic means like Digital Certificates should be employed.

- **Password management system:** An operating system could enforce selection of good passwords. Internal storage of password should use one-way hashing algorithms and the password file should not be accessible to users.
- **Use of system utilities:** System utilities are the programs that help to manage critical functions of the operating system e.g. addition or deletion of users. Obviously, this utility should not be accessible to a general user. Use and access to these utilities should be strictly controlled and logged.
- **Duress alarm to safeguard users:** If users are forced to execute some instruction under threat, the system should provide a means to alert the authorities.
- **Terminal time out:** Log out the user if the terminal is inactive for a defined period. This will prevent misuse in absence of the legitimate user.
- **Limitation of connection time:** Define the available time slot. Do not allow any transaction beyond this time period. For example, no computer access after 8.00 p.m. and before 8.00 a.m. - or on a Saturday or Sunday.

24. (a) The key management practices for assessing and evaluating the system of internal controls in an enterprise complying with COBIT 5 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.

(b) In the given scenario, we would suggest the owner of the local store to go for Transaction Processing System (TPS), which will be the most suitable option for him. Because TPS at the lowest level of management is an information system that manipulates data from business transactions efficiently and if properly computerized, TPS provides speed and accuracy too. Various day-to-day business activities such as sales, purchase, production, billing, payments or receipts involves transactions and these transactions and these transactions are to be organized and manipulated to generate various information products for external use.

Following are the major activities, which can be performed by the proposed TPS:

- Capturing data to organize in files or databases;
- Processing of files/databases using application software;
- Generating information in the form of reports; and
- Processing of queries from various quarters of the organization.

A TPS may follow the periodic data preparation and batch processing (as in payroll application) or on-line processing (as in inventory control application). In industries and business houses, now-a-days, on-line approach is preferred as it provides information with up-to-date status.

However, the major limitation of TPS is that the people involved in TPS, usually are not able to take any management decision.

25. As per Information Technology (Amendment) Act 2008, the XYZ network service provider can get exemption from the liability under provisions of sub-sections 1 and 2 of Section 79: Exemption from liability of intermediary in certain cases.

The relevant provisions of the above section are given as follows:

[Section 79] Exemption from liability of intermediary in certain cases

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

(2) The provisions of sub-section (1) shall apply if-

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

(b) the intermediary does not -

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if -

(a) the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

ISCA RTP NOV 2016

PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

Concepts of Governance and Management of Information Systems

1. (a) What is Governance of Enterprise IT (GEIT)? Explain its key benefits in brief.
   (b) Discuss the key governance practices for evaluating risk management.
2. Discuss the seven enablers of COBIT 5 framework.
3. As an IT consultant, elaborate on the major benefits of Governance to the Management of an enterprise.

Information System Concepts

4. Discuss limitations of Management Information Systems (MIS).
5. Distinguish between General-purpose planning languages and Special-purpose planning languages.
6. Discuss the impact of IT on Information Systems for different sectors.

Protection of Information Systems

7. Discuss Information Security Policy and its hierarchy.
8. Discuss Asynchronous Attacks.
9. Discuss Data Resource Management Controls under Managerial Controls.

Business Continuity Planning and Disaster Recovery Planning

10. Differentiate between Recovery Plan and Test Plan.
11. Discuss Incremental Backup, its advantages and disadvantages.
12. Discuss Objectives and Goals of Business Continuity Planning (BCP).

Acquisition, Development and Implementation of Information Systems

13. Discuss the Agile Model and its manifesto.
14. Differentiate between File conversion and System Conversion under System implementation phase of System Development Life Cycle (SDLC).
15. What can be the major Developer-related issues and challenges in achieving the System Development objectives?

Auditing of Information Systems

16. What are the various categories of Information systems (IS) Audit?

17. Discuss the role of auditors in evaluating the implementation of Security Management Controls and Operations Management Controls.

Information Technology Regulatory Issues

18. (a) Discuss the provision given in IT (Amendment) Act, 2008 that gives "Penalty for breach of confidentiality and privacy".

    (b) Discuss the Audit Report norms set up by SEBI for System Controls and Audit.

Emerging Technologies

19. Discuss Green Computing Best Practices, in brief.

20. Discuss "Community Cloud" and its characteristics under Cloud Computing environment.

Short Note Based Questions

21. Write short notes on following:

    (a) Storage as a Service (STaaS)

    (b) Firewall

    (c) Folksonomy

    (d) Types of Audit Trail

    (e) Disadvantages of Full Backup

22. Differentiate between the following:

    (a) Physical Controls and Logical Controls under Batch Controls

    (b) Corrective Controls and Compensatory Controls

    (c) System Analysis and System Design

    (d) Hardware Acquisition and Software Acquisition

    (e) Asset and Threat

Questions based on the Case Studies

23. Examine the legal position in the given situations as per the IT Act, 2000.

    (a) Mr. X is a Government servant whose profile is to maintain the records of all the employees of the organization. The intruder Mr. Z personates as the senior member of the organization's management team and retrieved the critical data from Mr. X on mobile phone. State the liabilities of Mr. Z under the given situation.

    (b) Also, state the liability of Mr. X in the above situation.

24. (a) XYZ is a government agency that had been developing and adopting office automation systems at random and in isolated pockets of its departments. At the same time, it was felt that the organisation needs to follow some specification for

their Information Security Management System (ISMS). As an IT consultant, explain to the management to why they should follow ISO 27001:2013 standard?

(b) The management of an enterprise PQR is in lookout of an integrated information system that combines most of information systems and designed to produce information and support decision making for different levels of management and business functions. Suggest the solution and also list its benefits.

25. (a) During the equipment installation in ABC shopping mall, its construction contractor wishes to ensure that the installation is protected against any kind of water damage. Discuss some of the major ways with which the same can be achieved.

(b) As a consultant, suggest the validation methods that may be adopted by the management of ABC Mall to validate the vendor's proposal.

SUGGESTED ANSWERS/HINTS

1. (a) Governance of Enterprise IT (GEIT): Governance of Enterprise IT is a sub-set of corporate governance and facilitates implementation of a framework of Information Systems' controls within an enterprise as relevant and encompassing all key areas. The primary objectives of GEIT are to analyze and articulate the requirements for the governance of enterprise IT, and to put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.

Major benefits of 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.

(b) The key governance practices for evaluating risk management are as follows:

- **Evaluate Risk Management:** This continually examines and makes judgment on the effect of risk on the current and future use of IT in the enterprise. This further considers whether the enterprise's risk appetite is appropriate and that risks to enterprise value related to the use of IT are identified and managed;
- **Direct Risk Management:** This directs the establishment of risk management practices to provide reasonable assurance that IT risk management practices

are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite; and

- ♦ **Monitor Risk Management:** This monitors the key goals and metrics of the risk management processes and establishes how deviations or problems will be identified, tracked and reported on for remediation.

2. **Enablers of COBIT 5:** Enablers are factors that, individually and collectively, influence whether something will work; in this case, governance and management over enterprise IT. Enablers are driven by the goals cascade, i.e., higher-level IT related goals defining 'what the different enablers should achieve'. The COBIT 5 framework describes seven categories of enablers, which are as follows:

- **Principles, Policies and Frameworks** are the vehicle to translate the desired behaviour 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 Behaviour** 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.

3. Some of the major benefits of Governance to the management of an enterprise are as follows:

- Achieving enterprise objectives by ensuring that each element of the mission and strategy are assigned and managed with a clearly understood and transparent decisions rights and accountability framework;
- Defining and encouraging desirable behavior in the use of IT and in the execution of IT outsourcing arrangements;
- Implementing and integrating the desired business processes into the enterprise;

- Providing stability and overcoming the limitations of organizational structure;
- Improving customer, business and internal relationships and satisfaction, and reducing internal territorial strife by formally integrating the customers, business units, and external IT providers into a holistic IT governance framework; and
- Enabling effective and strategically aligned decision making for the IT Principles that define the role of IT, IT Architecture, IT Infrastructure, Application Portfolio and Frameworks, Service Portfolio, Information and Competency Portfolios and IT Investment & Prioritization.

4. Major limitations of Management Information Systems (MIS) are given below:

- The quality of the outputs of MIS is basically governed by the quantity of input and processes.
- MIS is not a substitute for effective management, which means that it cannot replace managerial judgment in making decisions in different functional areas. It is merely an important tool in the hands of executives for decision making and problem solving.
- MIS may not have requisite flexibility to quickly update itself with the changing needs of time, especially in fast changing and complex environment.
- MIS cannot provide tailor-made information packages suitable for the purpose of every type of decision made by executives.
- MIS takes into account mainly quantitative factors, thus it ignores the non-quantitative factors like morale and attitude of members of organization, which have an important bearing on the decision making process of executives or senior management.
- MIS is less useful for making non-programmed decisions. Such types of decisions are not of the routine type and thus require information, which may not be available from existing MIS to executives.
- The effectiveness of MIS is reduced in enterprises, where the culture of hoarding information and not sharing with other holds.
- MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.

5. **General-purpose planning languages:** These are the languages that allow users to perform many routine tasks, for example; retrieving various data from a database or performing statistical analyses. The languages in most electronic spreadsheets are good examples of general-purpose planning languages. These languages enable user to tackle abroad range of budgeting, forecasting, and other worksheet-oriented problems.

Special-purpose planning languages: These are the languages that are more limited in what they can do, but they usually do certain jobs better than the general-purpose

planning languages. Some statistical languages, such as Statistical Analysis System (SAS) and Statistical Package for the Social Sciences (SPSS), are examples of special purpose planning languages.

6. The impact of IT on Information Systems for different sectors is explained below:

(i) **E-business –** This is also called electronic business and includes purchasing, selling, production management, logistics, communication, support services and inventory management through the use of internet technologies. The advantage of E-business are 24 hours sale, lower cost of doing business, more efficient business relationship, eliminate middlemen, unlimited market place and access with broaden customer base, secure payment systems, easier business administration and online fast updating. Only investment is needed in the purchase of space on internet, designing and maintenance of website. Different types of business can be done e.g. it may be B2B (Business to Business), B2C (Business to Customer), C2C (Customer to Customer) and C2B (Customer to Business). Because of no limitations of time and space, people prefer to involve in E-business. Thus, we can say that IT has given new definition to business.

(ii) **Financial Service Sector –** The financial services sector (banks, building societies, life insurance companies and short term insurers) manages large amounts of data and processes enormous numbers of transactions every day. All the major financial institutions operate nationally and have wide networks of regional offices and associated electronic networks. Now-a-days most of the services are offered by the financial services on internet, which can be accessed from anywhere and anytime that makes it more convenient to the customers. It also reduces their cost in terms of office staff and office building. Through the use of internet and mobile phones, financial service sectors are in direct touch with their customers and with adequate databases, it will be easier for service sectors to manage customer relationships.

(iii) **Wholesaling and Retailing –** A visit to any large store will show that IT has become a vital part of retailing. Retail business uses IT to carry out basic functions including till systems for selling items, capturing the sales data by item, stock control, buying, management reports, customer information and accounting. The laser scanners used in most grocery supermarkets and superstores to read product bar codes are among the most distinctive examples of modern computer technology. By using internet or mobile phones retailers can collect and exchange data between stores, distribution centers, suppliers and head offices. IT can be used in wholesale for supply chain logistics management, planning, space management, purchasing, re-ordering, and analysis of promotions. Data mining and data warehousing applications helps in the analysis of market baskets, customer profiles and sales trends. E-commerce among partners (suppliers, wholesalers, retailers, distributors) helps in carrying out transactions.

(iv) Public sectors – It includes services provided by the government mainly hospitals, police stations, universities etc. IT/IS can be used to keep records of the cases, respective people involved it, other related documents and can consult the existing data warehouse or databases to take appropriate actions. For example, IS like ERP can be implemented in a university to keep record of its employees in terms of their designation, leaves availed, department, achievements that can be used further in analyzing their performance.

(iv) Others – IT is efficiently used in entertainment industry (games, picture collection etc.), agriculture industry (information is just a mouse click away to the farmers), Tour industry (railway, hotel and airline reservations) and consultancy etc. Thus, we can say that IT has changed the working style of business world drastically and make it simpler day-by-day with its advancement.

7. **Information Security Policy –** This policy provides a definition of Information Security, its overall objective and the importance that applies to all users. Various types of Information Security Policies are as follows:

- **User Security Policies** – These include User Security Policy and Acceptable Usage Policy.
  - **User Security Policy –** This policy sets out the responsibilities and requirements for all IT system users. It provides security terms of reference for Users, Line Managers and System Owners.
  - **Acceptable Usage Policy –** This sets out the policy for acceptable use of email, Internet services and other IT resources.
- **Organization Security Policies** – These include Organizational Information Security Policy, Network & System Security Policy and Information Classification Policy.
- **Organizational Information Security Policy –** This policy sets out the Group policy for the security of its information assets and the Information Technology (IT) systems processing this information. Though it is positioned at the bottom of the hierarchy, it is the main IT security policy document.
- **Network & System Security Policy –** This policy sets out detailed policy for system and network security and applies to IT department users.
- **Information Classification Policy –** This policy sets out the policy for the classification of information.
- **Conditions of Connection –** This policy sets out the Group policy for connecting to the network. It applies to all organizations connecting to the Group, and relates to the conditions that apply to different suppliers' systems.

8. **Asynchronous Attacks:** They occur in many environments where data can be moved asynchronously across telecommunication lines. Numerous transmissions must wait for the clearance of the line before data being transmitted. Data that is waiting to be

transmitted are liable to unauthorized access. Such attacks are called Asynchronous Attacks. These attacks are hard to detect because they are usually very small pin like insertions. There are many forms of asynchronous attacks; some of them are given as follows:

- **Data Leakage:** Data is a critical resource for an organization to function effectively. Data leakage involves leaking information out of the computer by means of dumping files to paper or stealing computer reports and tape.
- **Wire-tapping:** This involves spying on information being transmitted over telecommunication network.
- **Piggybacking:** This is the act of following an authorized person through a secured door or electronically attaching to an authorized telecommunication link that intercepts and alters transmissions. This involves intercepting communication between the operating system and the user and modifying them or substituting new messages. A special terminal is tapped into the communication for this purpose.
- **Shutting Down of the Computer/Denial of Service:** This is initiated through terminals or microcomputers that are directly or indirectly connected to the computer. Individuals, who know the high-level systems log on-ID initiate shutting down process. The security measure will function effectively if there are appropriate access controls on the logging on through a telecommunication network. When overloading happens, some systems have been proved to be vulnerable to shutting themselves. Hackers use this technique to shut down computer systems over the Internet.

9. **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; either by permitting only addition of data to the database or 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.

10. Recovery Plan: 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.

Test Plan: The final component of a disaster recovery plan is a test plan. The purpose of the test plan is to identify deficiencies in the emergency, backup, or recovery plans or in the preparedness of an organization and its personnel for facing a disaster. It must enable a range of disasters to be simulated and specify the criteria by which the emergency, backup, and recovery plans can be deemed satisfactory. Periodically, test plans must be invoked. Unfortunately, top managers are often unwilling to carry out a test because daily operations are disrupted. They also fear a real disaster could arise as a result of the test procedures.

To facilitate testing, a phased approach can be adopted. First, the disaster recovery plan can be tested by desk checking and inspection and walkthroughs, much like the validation procedures adopted for programs. Next, a disaster can be simulated at a convenient time-for example, during a slow period in the day. Anyone, who will be affected by the test (e.g. personnel and customers) also might be given prior notice of the test so they are prepared. Finally, disasters could be simulated without warning at any time. These are the acid tests of the organization's ability to recover from a catastrophe.

11. Incremental Backup: An Incremental Backup captures files that were created or changed since the last backup, regardless of backup type. The last backup can be a full backup or simply the last incremental backup. With incremental backups, one full backup is done first and subsequent backup runs are just the changed files and new files added since the last backup.

For example - Suppose an Incremental backup job or task is to be done every night from Monday to Friday. This first backup on Monday will be a full backup since no backups have been taken prior to this. However, on Tuesday, the incremental backup will only backup the files that have changed since Monday and the backup on Wednesday will include only the changes and new files since Tuesday's backup. The cycle continues this way.

Advantages of Incremental Backup

- Much faster backups.
- Efficient use of storage space as files is not duplicated. Much less storage space used compared to running full backups and even differential backups.

Disadvantages of Incremental Backup

- Restores are slower than with a full backup and differential backups.
- Restores are a little more complicated. All backup sets (first full backup and all incremental backups) are needed to perform a restore.

12. Objectives and Goals of Business Continuity Planning

The primary objective of a Business Continuity Plan is to minimize loss by minimizing the cost associated with disruptions and enable an organization to survive a disaster and to re-establish normal business operations. In order to survive, the organization must assure that critical operations can resume normal processing within a reasonable time frame. The key objectives of the contingency plan should be to:

- Provide the safety and well-being of people on the premises at the time of disaster;
- Continue critical business operations;
- Minimize the duration of a serious disruption to operations and resources (both information processing and other resources);

- Minimize immediate damage and losses;
- Establish management succession and emergency powers;
- Facilitate effective co-ordination of recovery tasks;
- Reduce the complexity of the recovery effort; and
- Identify critical lines of business and supporting functions.

The goals of the Business Continuity Plan should be to:

- Identify weaknesses and implement a disaster prevention program;
- minimize the duration of a serious disruption to business operations;
- facilitate effective co-ordination of recovery tasks; and
- reduce the complexity of the recovery effort.

13. **Agile Model:** This is an organized set of software development methodologies based on the *iterative and incremental* development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development and delivery; time boxed iterative approach and encourages rapid and flexible response to change. It is a conceptual framework that promotes foreseen interactions throughout the development life cycle.

    Agile Manifesto is based on following 12 features:

    - Customer satisfaction by rapid delivery of useful software;
    - Welcome changing requirements, even late in development;
    - Working software is delivered frequently (weeks rather than months);
    - Working software is the principal measure of progress;
    - Sustainable development, able to maintain a constant pace;
    - Close, daily co-operation between business people and developers;
    - Face-to-face conversation is the best form of communication (co-location);
    - Projects are built around motivated individuals, who should be trusted;
    - Continuous attention to technical excellence and good design;
    - Simplicity;
    - Self-organizing teams; and
    - Regular adaptation to changing circumstances.

14. **File Conversion:** Because large files of information must be converted from one medium to another, this phase should be started long before programming and testing are completed. The cost and related problems of file conversion are significant whether they

involve on-line files (common database) or off-line files. In order for the conversion to be as accurate as possible, file conversion programs must be thoroughly tested. Adequate control, such as record counts and control totals, should be required output of the conversion program. The existing computer files should be kept for a period of time until sufficient files are accumulated for back up. This is necessary in case, the files must be reconstructed from scratch after a "bug" is discovered later in the conversion routine.

System Conversion: After on-line and off-line files have been converted and the reliability of the new system has been confirmed for a functional area, daily processing can be shifted from the existing information system to the new one. All transactions initiated after this time are processed on the new system. System development team members should be present to assist and to answer any questions that might develop. Consideration should be given to operating the old system for some more time to permit checking, matching and balancing the total results of both systems.

15. **Developer Related Issues**: Achieving the objectives of the system development is essential but many times, such objectives are not achieved as desired. An analysis on 'why organizations fail to achieve their systems development objectives' reveals bottlenecks. The developer-related bottlenecks refer to the issues and challenges with regard to the developers. Some of them are as follows:

- **Lack of Standard Project Management and System Development Methodologies:** Some organizations do not formalize their project management and system development methodologies, thereby making it very difficult to consistently complete projects on time or within budget.
- **Overworked or Under-Trained Development Staff:** In many cases, system developers often lack sufficient educational background and requisite state of the art skills. Furthermore, many companies do a little to help their development personnel stay technically sound, and more so a training plan and training budget do not exist.

16. Information Systems (IS) Audit has been categorized into five types:

(i) **Systems and Application:** An audit to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.

(ii) **Information Processing Facilities:** An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.

(iii) **Systems Development:** An audit to verify that the systems under development meet the objectives of the organization and to ensure that the systems are developed in accordance with generally accepted standards for systems development.

(iv) **Management of IT and Enterprise Architecture:** An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.

(v) **Telecommunications, Intranets, and Extranets:** An audit to verify that controls are in place on the client (end point device), server, and on the network connecting the clients and servers.

17. The role of Auditors w.r.t evaluation of implementation of Security Management Controls is as under:

- Auditors must evaluate whether security administrators are conducting ongoing, high-quality security reviews or not;
- Auditors check whether the organizations audited have appropriate, high-quality disaster recovery plan in place; and
- Auditors check whether the organizations have opted for an appropriate insurance plan or not.

The role of Auditors w.r.t evaluation of implementation of Operations Management Controls is as under:

- Auditors should pay concern to see whether the documentation is maintained securely and that it is issued only to authorized personnel.
- Auditors can use interviews, observations, and review of documentation to evaluate -
  - ♦ the activities of documentation librarians;
  - ♦ how well operations management undertakes the capacity planning ad performance monitoring function;
  - ♦ the reliability of outsourcing vendor controls;
  - ♦ whether operations management is monitoring compliance with the outsourcing contract; and
  - ♦ whether operations management regularly assesses the financial viability of any outsourcing vendors that an organization uses.

18. (a) Section 72 of the IT (Amendment) Act, 2008 gives the definition on "Penalty for breach of confidentiality and privacy".

[Section 72] Penalty for breach of confidentiality and privacy

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall

be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

(b) Audit Report Norms set up by SEBI for System Controls and Audit are as follows:

- The Systems Audit Reports and Compliance Status should be placed before the Governing Board of the Stock Exchanges/Depositories and the system audit report along with comments of Stock Exchanges / Depositories should be communicated to SEBI.
- The Audit report should have explicit coverage of each Major Area mentioned in the TOR, indicating any Nonconformity (NCs) or Observations (or lack of it). For each section, auditors should also provide qualitative input about ways to improve the process, based upon the best practices observed.

19. Green Computing Best Practices are as follows:

Develop a sustainable Green Computing plan

- Involve stakeholders to include checklists, recycling policies, recommendations for disposal of used equipment, government guidelines and recommendations for purchasing green computer equipment in organizational policies and plans;
- Encourage the IT community for using the best practices and encourage them to consider green computing practices and guidelines.
- On-going communication about and campus commitment to green IT best practices to produce notable results.
- Include power usage, reduction of paper consumption, as well as recommendations for new equipment and recycling old machines in organizational policies and plans; and
- Use cloud computing so that multiple organizations share the same computing resources, thus increasing the utilization by making more efficient use of hardware resources.

Recycle

- Dispose e-waste according to central, state and local regulations;
- Discard used or unwanted electronic equipment in a convenient and environmentally responsible manner as computers emit harmful emissions;
- Manufacturers must offer safe end-of-life management and recycling options when products become unusable; and
- Recycle computers through manufacturer's recycling services.

Make environmentally sound purchase decisions

- Purchase of desktop computers, notebooks and monitors based on environmental attributes;
- Provide a clear, consistent set of performance criteria for the design of products;
- Recognize manufacturer efforts to reduce the environmental impact of products by reducing or eliminating environmentally sensitive materials, designing for longevity and reducing packaging materials; and
- Use Server and storage virtualization that can help to improve resource utilization, reduce energy costs and simplify maintenance.

Reduce Paper Consumption

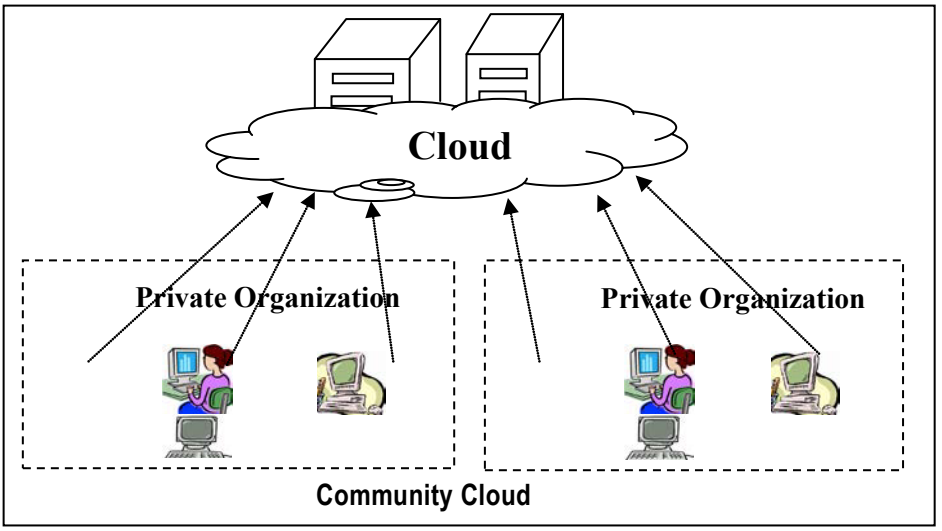
- Reduce paper consumption by use of e-mail and electronic archiving;
- Use of "track changes" feature in electronic documents, rather than redline corrections on paper;
- Use online marketing rather than paper based marketing; e-mail marketing solutions that are greener, more affordable, flexible and interactive than direct mail; free and low-cost online invoicing solutions that help cut down on paper waste; and
- While printing documents; make sure to use both sides of the paper, recycle regularly, use smaller fonts and margins, and selectively print required pages.

Conserve Energy

- Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors;
- Develop a thin-client strategy wherein thin clients are smaller, cheaper, simpler for manufacturers to build than traditional PCs or notebooks and most importantly use about half the power of a traditional desktop PC;
- Use notebook computers rather than desktop computers whenever possible;
- Use the power-management features to turn off hard drives and displays after several minutes of inactivity;
- Power-down the CPU and all peripherals during extended periods of inactivity;
- Try to do computer-related tasks during contiguous, intensive blocks of time, leaving hardware off at other times;
- Power-up and power-down energy-intensive peripherals such as laser printers according to need;
- Employ alternative energy sources for computing workstations, servers, networks and data centers; and

- Adapt more of Web conferencing offers instead of travelling to meetings in order to go green and save energy.

20. **Community Cloud:** The community cloud is the cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (eg. mission security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises. In this, a private cloud is shared between several organizations. This model is suitable for organizations that cannot afford a private cloud and cannot rely on the public cloud either.



Characteristics of Community Clouds 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 is being shared by several organizations or community, not only the responsibility gets shared; the community cloud becomes cost effective too.

21. **(a)** **Storage as a Service (STaaS):** STaaS, an instance of IaaS, provides storage infrastructure on a subscription basis to users who want a low-cost and convenient way to store data, synchronize data across multiple devices, manage off-site backups, mitigate risks of disaster recovery, and preserve records for the long-term.

It is an ability given to the end users to store the data on the storage services provided by the service provider. STaaS allows the end users to access the files at any time from any place. STaaS provider provides the virtual storage that is abstracted from the physical storage of any cloud data center. STaaS is also a cloud business model that is delivered as a utility.

(b) **Firewall:** Organizations connected to the Internet and Intranet often implements an electronic firewall to insulate their network from intrude. A Firewall is a system that enforces access control between two networks. To accomplish this, all traffic between the external network and the organization's Intranet must pass through the firewall. Only authorized traffic between the organization and the outside is allowed to pass through the firewall. The firewall must be immune to penetrate from both outside and inside the organization. In addition to insulating the organization's network from external networks, firewalls can be used to insulate portions of the organization's Intranet from internal access also.

(c) **Folksonomy:** This allows the free classification of information available on the web, which helps the users to classify and find information, using approaches such as tagging. Also known as Social Bookmarking, the bookmarks in a folder are not stored on the user's computer rather tagged pages are stored on the web increasing the accessibility from any computer connected to the Internet.

(d) Two types of audit trails that should exist in each subsystem are as follows:

- **Accounting Audit Trail:** An Accounting Audit Trail maintains a record of events within the subsystem; and
- **Operations Audit Trail:** An Operations Audit Trail maintains a record of the resource consumption associated with each event in the subsystem.

(e) Disadvantages of Full Backup are as follows:

- Backups can take very long as each file is backed up again every time the full backup is run.
- Full Backup consumes the most storage space compared to incremental and differential backups. The exact same files are stored repeatedly resulting in inefficient use of storage.

22. (a) **Physical Controls:** These controls are groups of transactions that constitute a physical unit. For example – source documents might be obtained via the email, assembled into batches, spiked and tied together, and then given to a data-entry clerk to be entered into an application system at a terminal.

Logical Controls: These are group of transactions bound together on some logical basis, rather than being physically contiguous. For example - different clerks might use the same terminal to enter transaction into an application system. Clerks keep control totals of the transactions into an application system.

(b) **Corrective Controls:** Corrective controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. A Business Continuity Plan (BCP) is considered to be a corrective control. Some of the Corrective Controls may be Contingency planning; Backup procedure; Rerun procedures; Change input value to an application system; and Investigate budget variance and report violations.

Compensatory Controls: Controls are basically designed to reduce the probability of threats, which can exploit the vulnerabilities of an asset and cause a loss to that asset. Sometimes, while designing and implementing controls, organizations because of different constraints like financial, administrative or operational, may not be able to implement appropriate controls. In such a scenario, there should be adequate compensatory measures, which may although not be as efficient as the appropriate control, but reduce the probability of loss to the assets. Such measures are called compensatory controls.

(c) **System Analysis:** System Analysis is the process of gathering and interpreting facts, diagnosing problems, and using the information to recommend improvements to the system.

System Design: System Design is the process of planning and structuring a new business system or one to replace or complement an existing system.

(d) **Hardware Acquisition:** In case of procuring such machinery as machine tools, transportation equipment, air conditioning equipment, etc., the management can normally rely on the time tested selection techniques and the objective selection criteria can be delegated to the technical specialist. The management depends upon the vendor for support services, systems design, education and training etc., and expansion of computer installation for almost an indefinite period; therefore, this is not just buying the machine and paying the vendor for it but it amounts to an enduring alliance with the supplier.

Software Acquisition: Once user output and input designs are finalized, the nature of the application software requirements must be assessed by the systems analyst. This determination helps the systems development team to decide "what type of application software products is needed" and consequently, the degree of processing that the system needs to handle. This helps the system developers in deciding about the nature of the systems software and computer hardware that will be most suitable for generating the desired outputs, and also the functions and capabilities that the application software must possess. At this stage, the system developers must determine whether the application software should be created in-house or acquired from a vendor.

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

Irrespective of the nature of the assets themselves, they all have one or more of the following characteristics:

- They are recognized to be of value to the organization.
- They are not easily replaceable without cost, skill, time, resources or a combination.
- They form a part of the organization's corporate identity, without which, the organization may be threatened.
- Their data classification would normally be Proprietary, Highly confidential or even Top Secret.

It is the purpose of Information Security Personnel to identify the threats against the risks and the associated potential damage to, and the safeguarding of Information Assets.

Threat: Any entity, circumstance, or event with the potential to harm the software system or component through its unauthorized access, destruction, modification, and/or denial of service is called a Threat. A Threat is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organization. Threat has capability to attack on a system with intent to harm. Every system has a data, which is considered as a fuel to drive a system, data is nothing but assets. Assets and threats are closely correlated. A threat cannot exist without a target asset. Threats are typically prevented by applying some sort of protection to assets.

23. (a) Mr. Z is liable under Section 66D of IT Act, 2000. Section 66D deals with the punishment for cheating by personation by using computer resource. According to the provision, whoever, by means of any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

(b) Mr. X is not liable as he was convinced that he is providing the data to the rightful person. So providing the information will utmost good faith will not make him liable.

24. (a) A company XYZ should adopt ISO 27001 for the following reasons:

- It is suitable for protecting critical and sensitive information.
- It provides a holistic, risk-based approach to secure information and compliance.
- Demonstrates credibility, trust, satisfaction and confidence with stakeholders, partners, citizens and customers.
- Demonstrates security status according to internationally accepted criteria.

- Creates a market differentiation due to prestige, image and external goodwill.
- If a company is certified once, it is accepted globally.

(b) The management of an enterprise PQR should opt for the implementation of Enterprise Resource Planning (ERP). ERP is process management software that allows an organization to use a system of integrated applications to manage the business and automate many back office functions related to technology, services and human resources. ERP software integrates all facets of an operation, including product planning, development, manufacturing, sales and marketing. ERP software is considered an enterprise application as it is designed to be used by larger businesses and often requires dedicated teams to customize and analyze the data and to handle upgrades and deployment. In contrast, Small business ERP applications are lightweight business management software solutions, customized for the business industry we work in.

Benefits of Enterprise Resource Planning (ERP) are as follows:

- Streamlining processes and workflows with a single integrated system.
- Reduce redundant data entry and processes and in other hand it shares information across the department.
- Establish uniform processes that are based on recognized best business practices.
- Improved workflow and efficiency.
- Improved customer satisfaction based on improved on-time delivery, increased quality, shortened delivery times.
- Reduced inventory costs resulting from better planning, tracking and forecasting of requirements.
- Turn collections faster based on better visibility into accounts and fewer billing and/or delivery errors.
- Decrease in vendor pricing by taking better advantage of quantity breaks and tracking vendor performance.
- Track actual costs of activities and perform activity based costing.
- Provide a consolidated picture of sales, inventory and receivables.

25. (a) Some of the major ways of protecting the installation against water damage are as follows:

- **Water Detectors:** These should be placed under the raised floor, near drain holes and near any unattended equipment storage facilities.
- **Strategically Locating the Computer Room:** To reduce the risk of flooding, the computer room should not be located in the basement or ground floor of a

multi-storey building. Studies reveal that the computer room located in the top floors is less prone to the risk of fire, smoke and water.

- Some of the other 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;
  - Water proofing; and
  - Water leakage Alarms.

(b) Some of the proposal validation methods that may be adopted in order to validate 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. For those criteria, however, where published reports are not available, reports would have to be made to other methods of validation. This method is particularly useful where the buying staff has 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. The results, achieved by the machine can be compared and price performance judgment can be made.

ISCA RTP MAY 2016

PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

Note: Update on Section 66A of the IT Act, 2000

As per the decision of the Supreme Court dated 24th March, 2015; Section 66A of Information Technology Act, 2000 (Punishment for sending offensive messages through communication service, etc.) has been declared ***Unconstitutional*** as it is violative of Article 19(1)(a) related to freedom of speech and expressions. Now comments on social networking sites will not be offensive unless they come under the provisions of the Indian Penal Code, 1860.

Concepts of Governance and Management of Information Systems

1. Discuss different levels of managerial activity that are carried out in an enterprise.
2. Discuss key benefits of COBIT 5 framework.
3. As an internal auditor, what shall be your perspective while evaluating IT Governance of an enterprise?

Information System Concepts

4. Discuss major areas of Computer-based applications.
5. Discuss different components of ERP (Enterprise Resource Planning) and its benefits.
6. Discuss different attributes of Information.

Protection of Information Systems

7. Differentiate between Detective Controls and Corrective Controls.
8. Discuss the impact of Technology on Internal Controls.
9. Discuss major techniques to commit cyber frauds.

Business Continuity Planning and Disaster Recovery Planning

10. Discuss the different phases involved in the development of a Business Continuity Plan.
11. Why documentation is required in Business Continuity Management (BCM)? Which documents are classified as being part of the BCM system?
12. Discuss Business Impact Analysis (BIA).

Acquisition, Development and Implementation of Information Systems

13. What do you understand by "Incremental Model"? Discuss its strengths and weaknesses also.
14. Discuss majorly used System Development Tools.

15. How can 'System Maintenance' under System Development Life Cycle (SDLC) be categorized?

Auditing of Information Systems

16. Why is there a need for audit of Information Systems?
17. Discuss the System Control Audit Review File (SCARF) technique used in the audit of Information Systems.

Information Technology Regulatory Issues

18. Discuss the provision given in IT (Amendment) Act 2008 that gives "Power to make rules by Central Government in respect of Electronic Signature".
19. Discuss the guidelines recommended by Securities and Exchange Board of India (SEBI) to conduct audit of systems.

Emerging Technologies

20. What are the emerging threats under "Bring Your Own Device (BYOD)"?

Short Note Based Questions

21. Write short notes on following:
    (a) Benefits of Governance of Enterprise IT (GEIT)
    (b) Planning Languages in Decision Support Systems (DSS)
    (c) Objectives and Goals of Business Continuity Planning (BCP)
    (d) Strengths of Agile Model
    (e) Auditor's role in System Development Life Cycle (SDLC)
22. Differentiate between the following:
    (a) Full Backup and Incremental Backup
    (b) Open System and Closed System
    (c) Explicit Knowledge and Tacit Knowledge
    (d) Quality Assurance Management Control and Security Management Control
    (e) Program Debugging and Program Testing

Questions based on the Case Studies

23. PQR Company is a pharmaceutical retail chain having many branches located in different places for its operation. Its business processes are cumbersome and tedious as it has multiple sources of procurement and supply destinations. The Chief Executive Officer (CEO) of company feels that existing information system does not meet its present requirements. He seeks for high-end solution to streamline and integrate its operation

processes and information flow to synergize all its major resources. Further, he expects that the new system should provide a structured environment in which decisions concerning demand, supply, operational, personnel, finance, logistics etc. are fully supported by accurate and reliable information. The company follows the best practices of System Development Life Cycle (SDLC), which consists of various phases starting from preliminary investigation till post implementation review, controls and security aspects. The CEO of the company appoints a committee of three persons - IT expert, a Security expert and an Auditor of the company in order to suggest the following:

(a) List the activities to be performed during the phase of System Requirements Analysis.

(b) Discuss major Boundary Control techniques that should be used in user control?

24. ABC is a leading company in the manufacturing of food items. The company is in the process of automation of its various business processes. During this phase, technical consultant of the company has highlighted the importance of information security and has suggested introducing it right from the beginning. He has also suggested to perform the risk assessment activity and accordingly, to mitigate the assessed risk. For carrying out all these suggestions, various best practices have been followed by the company. In addition, after each activity, appropriate standards' compliances have been tested to check the quality of each process. Various policies related with business continuity planning and disaster recovery planning has been implemented to ensure three major expectations from the software, namely, resist, tolerate and recover.

Read the above carefully and answer the following:

(a) What are the major suggestions given by the technical consultant? How the company is implementing these suggestions?

(b) Discuss Recovery Plan under Business Continuity Planning.

(c) What should be the major components of a good information security policy, as per your opinion?

25. ABC Industries Ltd., a company engaged in a business of manufacture and supply of automobile components to various automobile companies in India, had been developing and adopting office automation systems, at random and in isolated pockets of its departments. The company has recently obtained three major supply contracts from International Automobile companies and the top management has felt that the time is appropriate for them to convert its existing information system into a new one and to integrate all its office activities. One of the main objectives of taking this exercise is to maintain continuity of business plans even while continuing the progress towards e-governance.

(a) When the existing information system is to be converted into a new system, what are the activities involved in the conversion process?

(b) What are the different office activities that can be performed under Office Automation Systems (OAS)?

(c) What is meant by Business Continuity Planning? Explain the areas covered by Business Continuity.

SUGGESTED ANSWERS/HINTS

1. There are three levels of managerial activity in an enterprise which are as follows:

- **Strategic Planning:** Strategic Planning is defined as the process of deciding on objectives of the enterprise, on changes in these objectives, on the resources used to attain these objectives, and on the policies that are to govern the acquisition, use, and disposition of these resources. Strategic planning is the process by which top management determines overall organizational purposes and objectives and how they are to be achieved. Corporate-level strategic planning is the process of determining the overall character and purpose of the organization, the business it will enter and leave, and how resources will be distributed among those businesses.
- **Management Control:** Management Control is defined as the process by which managers assure that resources are obtained and used effectively and efficiently in the accomplishment of the enterprise's objectives.
- **Operational Control:** Operational Control is defined as the process of assuring that specific tasks are carried out effectively and efficiently.

IT strategic plans provide direction to deployment of information systems and it is important that key functionaries in the enterprise are aware and are involved in its development and implementation. Management should ensure that IT long and short-range plans are communicated to business process owners and other relevant parties across the enterprise. Management should establish processes to capture and report feedback from business process owners and users regarding the quality and usefulness of long and short-range plans. The feedback obtained should be evaluated and considered in future IT planning.

2. The key benefits of COBIT 5 framework are as follows:

- A comprehensive framework such as COBIT 5 enables enterprises in achieving their objectives for the governance and management of enterprise IT.
- The best practices of COBIT 5 help enterprises to create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use.
- Further, COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT related interests of internal and external stakeholders.

- COBIT 5 helps enterprises to manage IT related risk and ensures compliance, continuity, security and privacy.
- COBIT 5 enables clear policy development and good practice for IT management including increased business user satisfaction.
- The key advantage in using a generic framework such as COBIT 5 is that it is useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.
- COBIT 5 supports compliance with relevant laws, regulations, contractual agreements and policies.

3. IT Governance can be evaluated by both external as well internal auditors. The Institute of Internal Auditors (IIA) issues the guidance that outlines specific areas and critical aspects relating to governance structure and practices, which can be reviewed as part of internal audit. These are briefly explained here.

- **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.

4. Major areas of Computer based applications are Finance and Accounting, Marketing and Sales, Manufacturing, Inventory/Stock Management, Human Resource Management etc., which are given as follows:

- **Finance and Accounting –** The main goal of this subsystem is to ensure the financial viability of the organization, enforce financial discipline and plan and monitor the financial budget. It also helps in forecasting revenues, determining the best resources and uses of funds and managing other financial resources. Typical sub-application areas in finance and accounting are - Financial accounting; General ledger; Accounts receivable/payable; Asset accounting; Investment management; Cash management; Treasury management; Fund management and Balance sheet.
- **Marketing and Sales –** The objective of this subsystem is to maximize the sales and ensure customer satisfaction. The marketing system facilitates the chances of order procurement by marketing the products of the company, creating new customers and advertising the products. The sales department may use an order processing system to keep the status and track of orders, generate bills for the orders executed and delivered to the customer, strategies for rendering services

during warranty period and beyond, analyzing the sales data by category such as by region, product, sales manor sales value.

- **Production or Manufacturing –** The objective of this subsystem is to optimally deploy man, machine and material to maximize production or service. The system generates production schedules and schedules of material requirements, monitors the product quality, plans for replacement or overhauling the machinery and also helps in overhead cost control and waste control.
- **Inventory /Stores Management -** The inventory management system is designed with a view to keeping the track of materials in the stores. The system is used to regulate the maximum and minimum level of stocks, raise alarm at danger level stock of any material, give timely alert for re-ordering of materials with optimal re-order quantity and facilitate various queries about inventory like total inventory value at any time, identification of important items in terms stock value (ABC analysis), identification most frequently moving items (XYZ analysis) etc.
- **Human Resource Management -** Human resource is the most valuable asset for an organization. Effective and efficient utilization of manpower in a dispute-free environment in this key functional area ensures to facilitate disruption free and timely services in business. Human Resource Management System (HRMS) aims to achieve this goal. Skill database maintained in HRM system, with details of qualifications, training, experience, interests etc. helps management for allocating manpower to right activity at the time of need or starting a new project. This system also keeps track of employees' output or efficiency. Administrative functions like keeping track of leave records or handling other related functions are also included HRM system. An HRM system may have the following modules – Personnel administration; Recruitment management; Travel management; Benefit administration; Salary administration; Promotion management etc.

5. **Enterprise Resource Planning (ERP)** is process management software that allows an organization to use a system of integrated applications to manage the business and automate many back-office functions related to technology, services and human resources. ERP software integrates all facets of an operation, including product planning, development, manufacturing, sales and marketing. ERP model consists of four components which are implemented through a methodology and are as follows:

   (i) Software Component: The software component is the component that is most visible part and consists of several modules such as Finance, Human Resource, Supply Chain Management, Supplier Relationship Management, Customer Relationship, and Business Intelligence.

   (ii) Process Flow: It is the model that illustrates the way how information flows among the different modules within an ERP system. By creating this model makes it easier to understand how ERP work.

(iii) **Customer mindset:** By implementing ERP system, the old ways for working which user understand and comfortable with; have to be changed and may lead to users' resistance. For example, some users may say that they have spent many years doing an excellent job without help from ERP system. In order to lead ERP implementation to succeed, the company needs to eliminate negative value or belief that users may carry toward utilizing new system.

(iv) **Change Management:** In ERP implementation, change needs to be managed at several levels - User attitude; resistance to change; and Business process changes.

Benefits of ERP are as follows:

- Streamlining processes and workflows with a single integrated system.
- Reduce redundant data entry and processes and in other hand it shares information across the department.
- Establish uniform processes that are based on recognized best business practices.
- Improved workflow and efficiency.
- Improved customer satisfaction based on improved on-time delivery, increased quality, shortened delivery times.
- Reduced inventory costs resulting from better planning, tracking and forecasting of requirements.
- Turn collections faster based on better visibility into accounts and fewer billing and/or delivery errors.
- Decrease in vendor pricing by taking better advantage of quantity breaks and tracking vendor performance.
- Track actual costs of activities and perform activity based costing.
- Provide a consolidated picture of sales, inventory and receivables.

6. **Attributes of Information:** 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 purposes/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 that further 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 can be easily understand by the people. The mode may be in the form of voice, text and combination of these two. Format also plays an important role in communicating the idea. It should be designed in such a way that it assists in decision making, solving problems, initiating planning, controlling and searching. According to the type of information the different formats can be used e.g. diagrams, graphs, curves are best suited for representing the statistical data. Format of information should be simple, relevant and should highlight important points but should not be too cluttered up.
- **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. Similar is the case with broker who wants the latest information about the stock market.
- **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, one should wait for it an hour.
- **Frequency -** The frequency with which information is transmitted or received affects its value. For example- the weekly reports 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 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. **Detective Controls:** These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. An example of a detective control would be a use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend. The main characteristics of such controls are given as follows:

- Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc;
- An established mechanism to refer the reported unlawful activities to the appropriate person or group;
- Interaction with the preventive control to prevent such acts from occurring; and
- Surprise checks by supervisor.

Examples of detective controls include Hash totals; Check points in production jobs; Echo control in telecommunications; Error message over tape labels; Duplicate checking of calculations; Periodic performance reporting with variances; Past-due accounts report; The internal audit functions; Intrusion detection system; Cash counts and bank reconciliation; and Monitoring expenditures against budgeted amount.

Corrective Controls: Corrective controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. A Business Continuity Plan (BCP) is considered to be a corrective control. The main characteristics of the corrective controls are minimizing the impact of the threat; Identifying the cause of the problem; Providing Remedy to the problems discovered by detective controls; Getting feedback from preventive and detective controls; Correcting error arising from a problem; and Modifying the processing systems to minimize future occurrences of the incidents. Examples of Corrective Controls are Contingency planning; Backup procedure; Rerun procedures; Change input value to an application system, and Investigate budget variance and report violations.

8. The impact of Technology on Internal Controls is as follows:

- **Competent and Trustworthy Personnel:** Personnel should have proper skill and knowledge to discharge their duties. Substantial power is often vested in the errors responsible for the computer-based information systems developed, implemented, operated, and maintained within organizations.

- **Segregation of Duties:** In a manual system, during the processing of a transaction, there are split between different people, such that one person does not process a transaction right from start to finish. However, in a computerised system, the auditor should also be concerned with the segregation of duties within the IT department. As a basic control, segregation of duties prevents or detects errors or irregularities. Within an IT environment, the staff in the IT department of an enterprise will have a detailed knowledge of the interrelationship between the source of data, how it is processed and distribution and use of output.
- **Authorization Procedures:** In manual systems, auditors evaluate the adequacy of procedures for authorization of examining the work of employees. In computer systems, authorization procedures often are embedded within a computer program. For example: In some on-line transaction systems, written evidence of individual data entry authorisation, e.g. a supervisor's signature, may be replaced by computerised authorisation controls such as automated controls written into the computer programs (e.g. programmed credit limit approvals).
- **Adequate Documents and Records:** In a manual system, adequate documents and records are needed to provide an audit trail of activities within the system. In computer systems, documents might not be used to support the initiation, execution, and recording of some transactions. Thus, no visible audit or management trail would be available to trance the transactions in a computerized system.
- **Physical Control over Assets and Records:** Physical control over access and records is critical in both manual systems and computer systems. In the manual systems, protection from unauthorised access was through the use of locked doors and filing cabinets. Computerised financial systems have not changed the need to protect the data. A client's financial data and computer programs can all be maintained at a single site – namely the site where the computer is located. This concentration of information systems assets and records also increases the losses that can arise from computer abuse or a disaster.
- **Adequate Management Supervision:** In a manual system, management supervision of employee activities is relatively straightforward as the managers and the employees are often at the same physical location. In computer system, however, data communication facilities can be used to enable employees to be closer to the customers they service. Thus supervision of employees might have to be carried our remotely. The Management's supervision and review helps to deter and detect both errors and fraud.
- **Independent Checks on Performance:** In manual systems, independent checks are carried out because employees are likely to forget procedures, make genuine mistakes, become careless, or intentionally fail to follow prescribed procedures. If the program code in a computer system is authorized, accurate, and complete; the system will always follow the designated procedures in the absence of some other type of failure like hardware or systems software failure.

- **Comparing Recorded Accountability with Assets:** Data and the assets that the data purports to represent should periodically be compared to determine whether incompleteness or inaccuracies in the data exist or whether shortages or excesses in the assets have occurred. In a manual system, independent staff prepares the basic data used for comparison purposes. In a computer system, however, software is used to prepare this data. Again, internal controls must be implemented to ensure the veracity of program code, because traditional separation of duties no longer applies to the data being prepared for comparison purposes.
- **Delegation of Authority and Responsibility:** A clear line of authority and responsibility is an essential control in both manual and computer systems. In a computer system, however, delegating authority and responsibility in an unambiguous way might be difficult because some resources are shared among multiple users. Further, more users are developing, modifying, operating, and maintaining their own application systems instead of having this work performed by IS professionals.

9. Following are the major techniques to commit cyber frauds:

- **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.
- **Data Diddling:** Changing data before, during, or after it is entered into the system in order to delete, alter, or add key system data is referred as data diddling.
- **Data Leakage:** It refers to the unauthorized copying of company data such as computer files.
- **Denial of Service (DoS) Attack:** It refers to an action or series of actions that prevents access to a software system by its intended/authorized users; causes the delay of its time-critical operations; or prevents any part of the system from functioning.
- **Internet Terrorism:** It refers to the using Internet to disrupt electronic commerce and to destroy company and individual communications.
- **Logic Time Bombs:** These are the program that lies idle until some specified circumstances or a particular time triggers it. Once triggered, the bomb sabotages the system by destroying programs, data or both.
- **Masquerading or Impersonation:** In this case, perpetrator gains access to the system by pretending to be an authorized user.

- **Password Cracking:** Intruder penetrates a system's defence, steals the file containing valid passwords, decrypts them and then uses them to gain access to system resources such as programs, files and data.
- **Piggybacking:** It refers to the tapping into a telecommunication line and latching on to a legitimate user before s/he logs into the system.
- **Round Down:** Computer rounds down all interest calculations to 2 decimal places. Remaining fraction is placed in account controlled by perpetrator.
- **Scavenging or Dumpster Diving:** It refers to the gaining access to confidential information by searching corporate records.
- **Social Engineering Techniques:** In this case, perpetrator tricks an employee into giving out the information needed to get into the system.
- **Super Zapping:** It refers to the unauthorized use of special system programs to bypass regular system controls and performs illegal acts.
- **Trap Door:** In this technique, perpetrator enters in the system using a back door that bypasses normal system controls and perpetrates fraud.

10. The eight phases involved in the development of a Business Continuity Plan (BCP) are as follows:

- **Phase 1 – Pre-Planning Activities (Project Initiation):** This Phase is used to obtain an understanding of the existing and projected computing environment of the organization. This enables the project team to refine the scope of the project and the associated work program; develop project schedules; and identify and address any issues that could have an impact on the delivery and the success of the project.

  During this phase, a Steering Committee should be established that have the overall responsibility for providing direction and guidance to the Project Team. The Project Manager should work with the Steering Committee in finalizing the detailed work plan and developing interview schedules for conducting the Security Assessment and the Business Impact Analysis. Two other key deliverables of this phase are the development of a policy to support the recovery programs; and an awareness program to educate management and senior individuals who will be required to participate in the project.

- **Phase 2 – Vulnerability Assessment and General Definition of Requirements:** This phase addresses measures to reduce the possibility of disaster occurrence, rather than concentrating primarily on minimizing impact of an actual disaster. This phase includes the following key tasks:

  - A thorough Security Assessment of the computing and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security;

systems and access control software security; insurance; security planning and administration; application controls; and personal computers.

- The Security Assessment will enable the project team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.
- Present findings and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.
- Define the scope of the planning effort.
- Analyze, recommend and purchase recovery planning and maintenance software required to support the development of the plans and to maintain the plans current following implementation.
- Develop a Plan Framework.
- Assemble Project Team and conduct awareness sessions.

- **Phase 3 – Business Impact Assessment (BIA):** A Business Impact Assessment (BIA) of all business units that are part of the business environment enables the project team to identify critical systems, processes and functions; assess the economic impact of incidents and disasters that result in a denial of access to systems services and other services and facilities; and assess the "pain threshold," that is, the length of time business units can survive without access to systems, services and facilities. The BIA Report should be presented to the Steering Committee that identifies critical service functions and the timeframes in which they must be recovered after interruption. The BIA Report should then be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities.
- **Phase 4 – Detailed Definition of Requirements:** During this phase, a profile of recovery requirements is developed and is used as a basis for analyzing alternative recovery strategies and identifying resources required to support critical functions identified in Phase 3. This profile should include hardware (mainframe, data and voice communications and personal computers), software (vendor supplied, in-house developed, etc.), documentation (DP, user, procedures), outside support (public networks, DP services, etc.), facilities (office space, office equipment, etc.) and personnel for each business unit. Recovery Strategies will be based on short term, intermediate term and long term outages. Another key deliverable of this phase is the definition of the plan scope, objectives and assumptions.
- **Phase 5 – Plan Development:** During this phase, recovery plans components are defined and plans are documented. This phase also includes the implementation of changes to user procedures, upgrading of existing data processing operating procedures required to support selected recovery strategies and alternatives,

vendor contract negotiations (with suppliers of recovery services) and the definition of Recovery Teams, their roles and responsibilities. Recovery standards are also be developed during this phase.

- **Phase 6 – Testing/Exercising Program:** The plan Testing/Exercising Program is developed during this phase. Testing/exercising goals are established and alternative testing strategies are evaluated. Testing strategies tailored to the environment should be selected and an on-going testing program should be established.
- **Phase 7 – Maintenance Program:** Maintenance of the plans is critical to the success of an actual recovery. The plans must reflect changes to the environments that are supported by the plans. It is critical that existing change management processes are revised to take recovery plan maintenance into account. In areas, where change management does not exist, change management procedures will be recommended and implemented. Many recovery software products take this requirement into account.
- **Phase 8 – Initial Plan Testing and Implementation:** Once plans are developed, initial tests of the plans are conducted and any necessary modifications to the plans are made based on an analysis of the test results. Specific activities of this phase include defining the test purpose/approach; identifying test teams; structuring the test; conducting the test; analyzing test results; and modifying the plans as appropriate. As the recovery strategies are defined, specific testing procedures should be developed to ensure that the written plans are comprehensive and accurate.

11. It is important to keep preparations including documentation, up-to-date for the following reasons:

- Contracts and agreements are needed to reflect the changes.
- If additional equipment is needed, it must be maintained and periodically replaced when it is no longer dependable or no longer fits the organization's architecture.
- The BCM maintenance process demonstrate the documented evidence of the proactive management and governance of the enterprise's business continuity program; the key people who are to implement the BCM strategy and plans are trained and competent; the monitoring and control of the BCM risks faced by the enterprise; and the evidence that material changes to the enterprise's structure, products and services, activities, purpose, staff and objectives have been incorporated into the enterprise's business continuity and incident management plans.

The following documents (representative only) are classified as being part of the Business Continuity Management system:

- The business continuity policy;
- The business continuity management system;

- The business impact analysis report;
- The risk assessment report;
- The aims and objectives of each function;
- The activities undertaken by each function;
- The business continuity strategies;
- The overall and specific incident management plans;
- The business continuity plans;
- Change control, preventative action, corrective action, document control and record control processes;
- Local Authority Risk Register;
- Exercise schedule and results;
- Incident log; and
- Training program.

12. **Business Impact Analysis (BIA):** Business Impact Analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. The process of BIA determines and documents the impact of a disruption of the activities that support its key products and services. It enables the business continuity team to identify critical systems, processes and functions, assess the economic impact of incidents and disasters that result in a denial of access to the system, services and facilities, and assess the "pain threshold, "that is, the length of time business units can survive without access to the system, services and facilities. For each activity supporting the delivery of key products and services within the scope of its Business Continuity Management (BCM) program, the enterprise should:

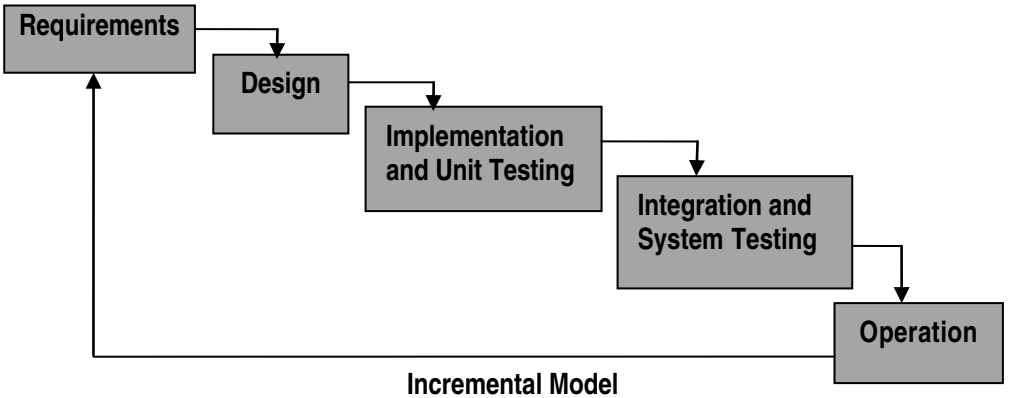
    - assess the impacts that would occur if the activity was disrupted over a period of time;
    - identify the maximum time period after the start of a disruption within which the activity needs to be resumed;
    - identify critical business processes;
    - assess the minimum level at which the activity needs to be performed on its resumption;
    - identify the length of time within which normal levels of operation need to be resumed; and
    - identify any inter-dependent activities, assets, supporting infrastructure or resources that have also to be maintained continuously or recovered over time.

    The enterprise should have a documented approach to conduct BIA. The enterprise should document its approach to assessing the impact of disruption and its findings and conclusions. The BIA Report should be presented to the Top Management. This report

identifies critical service functions and the time frame in which they must be recovered after interruption. The BIA Report should then be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities. Developing the Business Continuity Plan (BCP) also takes into account the BIA process.

13. **Incremental Model:** The Incremental Model is a method of software development where the model is designed, implemented and tested incrementally (a little more is added each time) until the product is finished. The product is defined as finished when it satisfies all of its requirements. This model combines the elements of the waterfall model with the iterative philosophy of prototyping. The product is decomposed into a number of components, each of which are designed and built separately. Each component is delivered to the client when it is complete. This allows partial utilization of product and avoids a long development time. It also creates a large initial capital outlay with the subsequent long wait avoided. This model of development also helps to ease the traumatic effect of introducing completely new system all at once. A few pertinent features are listed as follows:

- A series of mini-waterfalls are performed, where all phases of the waterfall development model are completed for a small part of the system, before proceeding to the next increment.
- Overall requirements are defined before proceeding to evolutionary, mini – Waterfall development of individual increments of the system.
- The initial software concept, requirement analysis, and design of architecture and system core are defined using the Waterfall approach, followed by iterative Prototyping, which culminates in installation of the final prototype (i.e. Working system).



Incremental Model

Strengths: Some of the strengths of Incremental Model identified by the experts and practitioners include the following:

- Potential exists for exploiting knowledge gained in an early increment as later increments are developed.
- Moderate control is maintained over the life of the project through the use of written documentation and the formal review and approval/signoff by the user and information technology management at designated major milestones.
- Stakeholders can be given concrete evidence of project status throughout the life cycle.
- It is more flexible and less costly to change scope and requirements.
- It helps to mitigate integration and architectural risks earlier in the project.
- It allows the delivery of a series of implementations that are gradually more complete and can go into production more quickly as incremental releases.
- Gradual implementation provides the ability to monitor the effect of incremental changes, isolated issues and make adjustments before the organization is negatively impacted.

Weaknesses: Some of the weaknesses of Incremental Model identified by the experts and practitioners include the following:

- When utilizing a series of mini-waterfalls for a small part of the system before moving onto the next increment, there is usually a lack of overall consideration of the business problem and technical requirements for the overall system.
- Each phase of an iteration is rigid and do not overlap each other.
- Problems may arise pertaining to system architecture because not all requirements are gathered up front for the entire software life cycle.
- Since some modules will be completed much earlier than others, well-defined interfaces are required.
- It is difficult to demonstrate early success to management.

14. Some of the prominent System Development Tools are as follows:

(a) Structured English: Structured English 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.

(b) Flowcharts: 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.

(c) **Data Flow Diagrams:** A Data Flow Diagram (DFD) 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 and have specified symbols.

(d) **Decision Tree:** A Decision Tree is a support tool that uses a tree-like graph or model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility. Decision tree is commonly used in operations research, specifically in decision analysis, to help identify a strategy most likely to reach a goal and to calculate conditional probabilities.

(e) **Decision Table:** A Decision Table is a table, which may accompany a flowchart, defining the possible contingencies that may be considered within the program and the appropriate course of action for each contingency. Decision tables are necessitated by the fact that branches of the flowchart multiply at each diamond (comparison symbol) and may easily run into scores and even hundreds. If, therefore, the programmer attempts to draw a flowchart directly, s/he is liable to miss some of the branches.

(f) **CASE Tools:** CASE (Computer-Aided-Software Engineering) refers to the automation of anything that humans do to develop systems and support virtually all phases of traditional system development process. For example, these packages can be used to create complete and internally consistent requirements specifications with graphic generators and specifications languages. An ideal CASE system would have an integrated set of tools and features to perform all aspects in the life cycle. Some of the features that various CASE products possess are - Repository / Data Dictionary; Computer aided Diagramming Tools; Word Processing; Screen and Report generator; Prototyping; Project Management; Code Generation; and Reverse Engineering.

(g) **System Components Matrix:** A System Component Matrix provides a matrix framework to document the resources used, the activities performed and the information produced by an information system. It can be used as an information system framework for both systems analysis and system design and views the information system as a matrix of components that highlights how the basic activities of input, processing, output, storage and controls are accomplished in an information system; and how the use of hardware, software and people resources can convert data resources into information products.

(h) **Data Dictionary:** A Data Dictionary contains descriptive information about the data items in the files of a business information system. Thus, a data dictionary is a computer file about data. Each computer record of a data dictionary contains

information about a single data item used in a business information system. This information may include - the identity of the source document(s) used to create the data item; the names of the computer files that store the data item; the names of the computer programs that modify the data item; the identity of the computer programs or individuals permitted to access the data item for the purpose of file maintenance, upkeep, or inquiry; the identity of the computer programs or individuals not permitted to access the data item etc.

(i) **User Interface Layout and Forms:** Several type layout forms for both soft and hard copy are used to model input/output components of an automated information system. Some of the prominent and inevitable ones are Layout form and Screen Generator; Menu Generator; Report Generator and Code Generator.

15. System Maintenance is an important aspect of SDLC. As key personnel change positions in the organization, new changes will be implemented, which will require system updates at regular intervals. Most of the information systems require at least some modification after development. The need for modification arises from a failure to anticipate/capture all the requirements during system analysis/design and/or from changing organizational requirements. 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 in this context refers to the totality of all conditions and influences, which act from outside upon the system, for example, business rule, government policies, work patterns, software and hardware operating platforms. The need for adaptive maintenance can only be recognized by monitoring the environment.

- **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. The long-term effect of corrective, adaptive and perfective changes increases the system's complexity. As a large program is continuously changed, its complexity, which reflects deteriorating structure, increases unless work is done to maintain or reduce it. This work is known as preventive change.

16. 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.

17. 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. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities. 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.

18. Section 10 of IT Amendment Act 2008 discusses the provision of "Power to make rules by Central Government in respect of Electronic Signature" which states that -

The Central Government may, for the purposes of this Act, by rules, prescribe

(a) the type of Electronic Signature;

(b) the manner and format in which the Electronic Signature shall be affixed;

(c) the manner or procedure which facilitates identification of the person affixing the Electronic Signature;

(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to Electronic Signature.

19. Mandatory audits of systems and processes bring transparency in the complex workings of Securities and Exchange Board of India (SEBI), prove integrity of the transactions and build confidence among the stakeholders. SEBI has mandated that exchanges shall conduct an annual system audit by a reputed independent auditor. The guidelines recommended by Securities and Exchange Board of India (SEBI) to conduct audit of systems are as follows:

- 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. Sample areas of review covered by IS Audit assignments are given here.

20. Emerging threats under "Bring Your Own Device (BYOD)" 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 Information Technology 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. For example - if a virus hits the network and all the devices connected to the network need be scanned, it is probable that some of the devices would miss out on this routine scan operation. In

addition to this, the network security lines become blurred when BYOD is implemented.

- **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'. 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.

21. (a) **Governance of Enterprise IT (GEIT)** is a sub-set of corporate governance and facilitates implementation of a framework of IS controls within an enterprise as relevant and encompassing all key areas. The primary objectives of GEIT are to analyze and articulate the requirements for the governance of enterprise IT, and to put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives. Some of the key benefits of 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.

(b) Two types of planning languages that are commonly used in DSS are **General-purpose planning languages** and **Special-purpose planning languages**. These are discussed below:

- **General-purpose planning languages** that allow users to perform many routine tasks, for example; retrieving various data from a database or performing statistical analyses. The languages in most electronic spreadsheets are good examples of general-purpose planning languages. These languages enable user to tackle abroad range of budgeting, forecasting, and other worksheet-oriented problems.
- **Special-purpose planning languages** are more limited in what they can do, but they usually do certain jobs better than the general-purpose planning languages. Some statistical languages, such as SAS (Statistical Analysis System) and SPSS (Statistical Package for the Social Sciences) are examples of special purpose planning languages.

(c) Objectives and Goals of Business Continuity Planning (BCP): The primary objective of a Business Continuity Plan is to minimize loss by minimizing the cost associated with disruptions and enable an organization to survive a disaster and to re-establish normal business operations. In order to survive, the organization must assure that critical operations can resume normal processing within a reasonable time frame. The key objective of the contingency plan should be to:

- Provide the safety and well-being of people on the premises at the time of disaster;
- Continue critical business operations;
- Minimize the duration of a serious disruption to operations and resources (both information processing and other resources);
- Minimize immediate damage and losses;
- Establish management succession and emergency powers;
- Facilitate effective co-ordination of recovery tasks;
- Reduce the complexity of the recovery effort; and
- Identify critical lines of business and supporting functions.

The goals of the Business Continuity Plan should be to:

- Identify weaknesses and implement a disaster prevention program;
- minimize the duration of a serious disruption to business operations;
- facilitate effective co-ordination of recovery tasks; and
- reduce the complexity of the recovery effort.

(d) Strengths of Agile Model: Some of the strengths identified by the experts and practitioners include the following:

- Agile methodology has the concept of an adaptive team, which enables to respond to the changing requirements.
- The team does not have to invest time and efforts and finally find that by the time they delivered the product, the requirement of the customer has changed.
- Face to face communication and continuous inputs from customer representative leaves a little space for guesswork.
- The documentation is crisp and to the point to save time.

The end result is generally the high quality software in least possible time duration and satisfied customer.

(e) In System Development Life Cycle (SDLC), some of the roles that an auditor has to perform are following:

- To attend project and steering committee meetings and examine project control documentation and conducting interviews in order to ensure 'what project control standards are to be complied with, (such as a formal systems development process) and determining the extent to which compliance is being achieved;
- To examine system documentation such as functional specifications to arrive at an opinion on controls based on the degree to which the system satisfies the general control objectives that any information system should meet;
- To provide a list of the standard controls, over such operational concerns as response time, CPU usage, and random access space availability that the auditor has used as assessment criteria;
- To rate various phases of SDLC on a rating system scale of 1 to 10 ;
- To give control objectives, directives and in general, validate the opinion expressed by technical experts.
- To provide control considerations that include documented policy and procedures; Established Project team with all infrastructure and facilities; Developers/ IT managers are trained on the procedures; Appropriate approvals are being taken at identified mile-stones; Development is carried over as per standards, functional specifications; Separate test environment for development/ test/ production / test plans; Design norms and naming conventions are as per standards and are adhered to; Business owners testing and approval before system going live; Version control on programs; Source Code is properly secured; Adequate audit trails are provided in system; and Appropriateness of methodologies selected etc.;

- To determine if the expected benefits of the new system are realized and whether users are satisfied with the new system during post implementation review etc.

22. (a) **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.

(b) **Open System:** An Open System interacts with other systems in its environment. For example - Information system is an open system because it takes input from the environment and produces output to the environment, which changes as per the changes in the environment.

Closed System: Closed System does not interact with the environment and does not change with the changes in environment. Consider a 'throw-away' type sealed digital watch, which is a system, composed of a number of components that work in a cooperative fashion designed to perform some specific task. This watch is a closed system as it is completely isolated from its environment for its operation.

(c) **Explicit knowledge:** Explicit Knowledge 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 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.

(d) **Quality Assurance Management Control:** It is responsible for ensuring information systems development; implementation, operation, and maintenance conform to established quality standards. 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 information systems projects that require more stringent quality requirements and are becoming more concerned about their liabilities if they produce and sell defective software.

Security Management Control: It is responsible for access controls and physical security over the information systems function. Information security administrators are responsible for ensuring that information systems assets are secure. Assets are secure when the expected losses that will occur over some time are at an acceptable level. Some of the major threats and to the security of information systems and their controls are Fire, Water, Energy Variations, Structural Damage, Pollution, Unauthorized Intrusion, Viruses and Worms, Misuse of software, data and services, Hackers etc.

(e) **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 - Give input the source program to the compiler; Let the compiler to find errors in the program; Correct lines of code that are erroneous, and Resubmit the corrected source program as input to the compiler.

Program Testing: A careful and thorough testing of each program is imperative to the successful installation of any system. The programmer should plan the testing to be performed, including testing of all the possible exceptions. The test plan should require the execution of all standard processing logic based on chosen testing strategy/techniques. The program test plan should be discussed with the project manager and/or system users. A log of test results and all conditions successfully tested should be kept. The log will prove invaluable in finding the faults and debugging.

23. (a) The final deliverable during the System Requirements Analysis (SRA) phase is Systems Requirements Specification (SRS). The activities to be performed during this phase are as follows:

- To identify and consult the stakeholders to determine their expectations and resolve their conflicts;
- To analyze requirements to detect and correct conflicts and determine their priorities;
- To verify that the requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable;
- To gather data or find facts using tools like interviewing, research/document collection, questionnaires, observation;

- To model the activities such as developing models to document Data Flow Diagrams, E-R Diagrams; and
- To document activities such as interview, questionnaires, reports etc. and development of a system (data) dictionary to document the modelling activities.

(b) The major Boundary controls of the system are the access control mechanisms. Access controls are implemented with an access control mechanism and links the authentic users to the authorized resources for which they are permitted to access. The access control mechanism has three steps - Identification, Authentication and Authorization with respect to the access control policy.

Major Boundary Control techniques are as follows:

- **Cryptography:** It deals with programs for transforming data into codes that are meaningless to anyone, who does not possess the authentication to access the respective system resource or file. A cryptographic technique encrypts data into cryptograms and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst. The three techniques of cryptography are transposition (permute the order of characters within a set of data), substitution (replace text with a key-text) and product cipher (combination of transposition and substitution).
- **Passwords:** User identification by an authentication mechanism with personal characteristics like name, birth date, employee code, function, designation or a combination of two or more of these can be used as a password boundary access control. A few best practices followed to avoid failures in this control system are - minimum password length, avoid usage of common dictionary words, periodic change of passwords, encryption of passwords and number of entry attempts.
- **Personal Identification Numbers (PIN):** PIN is similar to a password assigned to a user by an institution based on the user characteristics and encrypted using a cryptographic algorithm or the institute generates a random number stored in its database independent to a user identification details, or a customer selected number. Hence, a PIN or a digital signature are exposed to vulnerabilities while issuance or delivery, validation, transmission and storage.
- **Identification Cards:** Identification cards are used to store information required in an authentication process. These cards used to identify a user; are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.
- **Biometric devices:** Biometric identification e.g. thumb and/or finger impression, eye retina etc. are also used as boundary control techniques.

24. (a) During the automation of various processes of ABC Company, the technical consultant of the company has given the following major suggestions:

- By realizing the importance of information security, he suggested to introduce it right from the beginning.
- In addition, he also suggested performing the risk assessment activity.
- Finally, he advised to mitigate the assessed risk.

For the implementation of all the above mentioned suggestions, the company takes the following steps:

- The company followed various best practices for each process for the proper implementation of the suggestions.
- In addition, the company also tested the compliance of appropriate standards' after each activity, to check the quality of each process.
- Further, the company also implemented the policies related to business continuity planning and disaster recovery to ensure three broad expectations from the software: resist, tolerate and recover.

(b) **Recovery Plan:** The Recovery plans set out procedures to restore full information system capabilities. Recovery plans should identify a recovery committee that will be responsible for working out the specification 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 and must periodically review and practice for executing their responsibilities so that they are prepared for a disaster. If committee members leave the organization, new members must be appointed immediately and briefed about their responsibilities.

(c) A good Information Security Policy should clearly state the following:

- Purpose and scope of the document and the intended audience,
- The Security infrastructure,
- Security policy document maintenance and compliance requirements,
- Incident response mechanism and incident reporting,
- Security organization structure,
- Inventory and classification of assets,
- Description of technologies and computing structure,
- Physical and environmental security,
- Identity management and access control,

- IT operations management,
- IT communications,
- System development and maintenance controls,
- Business Continuity Planning (BCP),
- Legal compliances,
- Monitoring and auditing requirements, and
- Underlying technical policy.

25. (a) Conversion from existing information system to a new system involves the following activities:

(i) Defining the procedures for correcting and converting the data into the new application, determining 'what data can be converted through software and what data manually';

(ii) Performing data cleansing before data conversion;

(iii) Identifying the methods to assess the accuracy of conversion like record counts and control totals;

(iv) Designing exception reports showing the data which could not be converted through software; and

(v) Establishing responsibility for verifying and signing off and accepting overall conversion by the system owner.

(b) The different office activities under Office Automation Systems (OAS) are discussed as under:

(i) **Document capture:** Documents originating from outside sources like incoming mails, notes, handouts, charts, graphs etc. need to be preserved.

(ii) **Document Creation:** This consists of preparation of documents, dictation, editing of texts etc. and takes up major part of the secretary's time.

(iii) **Receipts and Distribution:** This basically includes distribution of correspondence to designated recipients.

(iv) **Filling, Search, Retrieval and Follow-up:** This is related to filling, indexing, searching of documents, which takes up significant time.

(v) **Calculations:** These include the usual calculator functions like routine arithmetic, operations for bill passing, interest calculations, working out the percentages and the like.

(vi) **Recording Utilization of Resources:** This includes, where necessary, record keeping in respect of specific resources utilized by office personnel.

All the activities mentioned have been made very simple and effective by the use of computers. The application of computers to handle the office activities is also termed as office automation.

(c) Business Continuity Planning (BCP) is the creation and validation of a practical logistical plan for how an organization will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a Business Continuity Plan. Planning is an activity to be performed before the disaster occurs otherwise it would be too late to plan an effective response. The resulting outage from such a disaster can have serious effects on the viability of a firm's operations, profitability, quality of service, and convenience.

Business Continuity covers the following areas:

(i) **Business Resumption Planning:** The Operation's piece of business continuity planning;

(ii) **Disaster Recovery Planning:** The technological aspect of BCP, the advance planning and preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of a disaster.

(iii) **Crisis Management:** The overall co-ordination of an organization's response to a crisis in an effective timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation or ability to operate.