

PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT
QUESTIONS

Concepts of Governance and Management of Information Systems

1. (a) What are the key management practices, which are required for aligning IT strategy with enterprise strategy?
(b) Discuss the key governance practices for evaluating risk management.
2. Discuss COBIT and its components in brief.
3. Discuss major benefits of Governance.

Information System Concepts

4. (a) What is an Expert System? Discuss some of its business applications.
(b) Why do we need Expert Systems?
5. What do you mean by the term "Information"? Discuss different attributes of it.
6. Discuss different types of Information Systems.

Protection of Information Systems

7. Discuss Information System Security and its objectives.
8. Discuss major techniques to commit cyber frauds.
9. Discuss different means of controlling physical access in an organization.

Business Continuity Planning and Disaster Recovery Planning

10. List down the key objectives and goals of Business Continuity Planning.
11. Discuss all the phases involved in a methodology for developing a Business Continuity Plan (BCP).
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. What can be the major user-related issues that may come in achieving the System Development Objectives?
14. Discuss strengths and weaknesses of Waterfall Model.
15. Discuss System Testing and its types.

Auditing of Information Systems

16. Discuss different categories of Information System Audit.

17. Discuss Audit Trail. How can it be used to support enterprises' security objectives?

Information Technology Regulatory Issues

18. Explain the power of Controller to give directions under Section 68 of the Information Technology (Amendment) Act, 2008.
19. What are the powers of a Police Officer under the Information Technology (Amendment) Act, 2008 to enter and search etc?

Emerging Technologies

20. Discuss Cloud Computing architecture.

Short Note Based Questions

21. Write short notes on the following:
- (a) Segregation of Duties
 - (b) Corrective Controls
 - (c) Cryptography
 - (d) Schedule Feasibility
 - (e) System Control Audit Review File (SCARF)
22. Differentiate between the following:
- (a) Asset and Threat
 - (b) Abstract System and Physical System
 - (c) Full Backup and Incremental Backup
 - (d) Platform as a Service (PaaS) and Software as a Service (SaaS)

Questions based on the Case Studies

23. 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) What are the popular implementation strategies that may be used to convert an old system into new system?

- (b) What is the provision given in Information Technology (Amendment) Act, 2008 for the retention of electronic records?
24. PQR Technologies Ltd. is in the development of web applications for various domains. For the development purposes, the company is committed to follow the best practices suggested by System Development Life Cycle. A system development methodology is a formalized, standardized, documented set of activities used to manage a system development project. It refers to the framework that is used to structure, plan and control the process of developing an information system. Each of the available methodologies is best suited to specific kinds of projects, based on various technical, organizational, project and team considerations.

Read the above carefully and answer the following:

- (a) Discuss the Feasibility study and its types under SDLC.
- (b) What can be various fact finding techniques that may be adopted to gather the requirement?
- (c) Briefly describe any five weaknesses of Rapid Application Development (RAD) Methodology.
25. Mr. A has received some information about Mr. B on his cell phone. He knows that this information has been stolen by the sender. He not only retained this information but also sends it to Mr. B and his friends. Because of this act, Mr. B is annoyed and his life is in danger.

Mr. B seeks your advice, under what sections of Information Technology (Amendment) Act, 2008; he can file an FIR with police against Mr. A? Advise Mr. B detailing the applicable sections of the Act.

SUGGESTED ANSWERS/HINTS

1. (a) The key management practices, which are required for aligning IT strategy with enterprise strategy, are as follows:
- **Understand enterprise direction:** This considers the current enterprise environment and business processes, as well as the enterprise strategy and future objectives. This further considers the external environment of the enterprise (industry drivers, relevant regulations, basis for competition).
 - **Assess the current environment, capabilities and performance:** This assesses the performance of current internal business and IT capabilities and external IT services, and develop an understanding of the enterprise architecture in relation to IT. This further identifies issues currently being experienced and develops recommendations in areas that could benefit from

improvement and considers service provider differentiators and options and the financial impact and potential costs and benefits of using external services.

- **Define the target IT capabilities:** This defines the target business and IT capabilities and required IT services. This should be based on the understanding of the enterprise environment and requirements; the assessment of the current business process and IT environment and issues; and consideration of reference standards, best practices and validated emerging technologies or innovation proposals.
- **Conduct a gap analysis:** This identifies the gaps between the current and target environments and consider the alignment of assets (the capabilities that support services) with business outcomes to optimize investment in and utilization of the internal and external asset base. This also considers the critical success factors to support strategy execution.
- **Define the strategic plan and road map:** This creates a strategic plan that defines, in co-operation with relevant stakeholders, how IT- related goals will contribute to the enterprise's strategic goals. This further includes how IT will support IT-enabled investment programs, business processes, IT services and IT assets. IT should define the initiatives that will be required to close the gaps, the sourcing strategy, and the measurements to be used to monitor achievement of goals, then prioritize the initiatives and combine them in a high-level road map.
- **Communicate the IT strategy and direction:** This creates awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy, through communication to appropriate stakeholders and users throughout the enterprise.

(b) The key governance practices for evaluating risk management are given 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. **Control Objectives for Information and Related Technology (COBIT)** is a set of best practices for Information Technology management developed by Information Systems

Audit & Control Association (ISACA) and IT Governance Institute in 1996. ISACA develops and maintains the internationally recognized COBIT framework, helping IT professionals and enterprise leaders fulfill their IT Governance responsibilities while delivering value to the business. The latest ISACA's globally accepted framework COBIT 5 is aimed to provide an end-to-end business view of the governance of enterprise IT that reflects the central role of IT in creating value for enterprises. COBIT 5 incorporates the latest thinking in enterprise governance and management techniques and provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from information systems.

Components in COBIT

- **Framework** - Organize IT governance objectives and good practices by IT domains and processes, and links them to business requirements.
 - **Process Descriptions** - A reference process model and common language for everyone in an organization. The processes map to responsibility areas of plan, build, run and monitor.
 - **Control Objectives** - Provide a complete set of high-level requirements to be considered by management for effective control of each IT process.
 - **Management Guidelines** - Help assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes.
 - **Maturity Models** - Assess maturity and capability per process and helps to address gaps.
3. Some of the major benefits of Governance can be 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. (a) **Expert System** - An Expert System is a highly developed Decision Support System that utilizes knowledge generally possessed by an expert to solve a problem. Expert System is software system that imitates the reasoning processes of human experts and provides decision makers with the type of advice they would normally receive from such expert systems. For instance, an expert system in the area of investment portfolio management might ask its user a number of specific questions relating to investments for a particular client like – How much can be invested? Does the client have any preferences regarding specific types of securities? And so on.

A characteristic of Expert System is the ability to declare or explain the reasoning process that was used to make decisions. Some of the business applications of Expert Systems are as follows:

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

(b) Major reasons for the need of Expert Systems are as given:

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

5. **Information:** Technically, Information means processed data. Data is facts or values of results and information is the relations between data and other relations. e.g. in spread

sheet student name, roll number and marks obtained in science and arts subjects represents data whereas the graph that shows the percentage of students acquire more than 80% in science subjects and 65% in arts subjects represents information. Information may be represented in the form of text, graph, pictures, voice, videos etc.

Information relates to description, definition, or perspective (what, who, when, where). 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.

Attributes of Information: Some of the important attributes of useful and effective information are given 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. According to the type of information, 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.
- **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 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.
6. Different Information Systems that serve different organizational levels are as given:
- (i) **Operational Level Systems** - These support operational managers by keeping track of the elementary activities and transactions of the enterprises e.g. sales, payroll, receipts etc. These are primarily needed to answer routine questions and keep track of flow of transactions though the enterprises. For example - it gives answer to query like how many books are in the inventory, what happens to the payment of the customer? And how many hours a particular employee works in office. To get answer of these types of queries; the information should be accurate, current and easily available.

(ii) **Knowledge Level Systems** - These systems support the business to integrate new knowledge into the business and control the flow of paperwork. These help the organization's knowledge and data workers.

(iii) **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 type of systems mainly answers "what if" questions.

(iv) **Strategic Level Systems** - These support the senior level management to tackle and address strategic issues and long term trends, both inside organization and the outside world. These answer questions like what products should be launched to increase the profit and capture the market and help in long term planning.

7. **Information System Security:** Information System Security refers to the protection of valuable assets against loss, disclosure, or damage. Securing valuable assets from threats, sabotage or natural disaster with physical safeguards such as locks, perimeter fences and insurance is commonly implemented by most of the organizations. However, security must be expanded to include logical and other technical safeguards such as user identifiers, passwords, firewalls, etc.

The valuable assets are the data or information recorded, processed, stored, shared, transmitted, or retrieved from an electronic medium. The data or information is protected against harm from threats that will lead to its loss, inaccessibility, alteration, or wrongful disclosure. The protection is achieved through a layered series of technological and non-technological safeguards such as physical security and logical measures.

Information System Security Objective: The objective of Information System Security is "the protection of the interests of those relying on information, and protect the information systems and communications that deliver the information from harm resulting from failures of confidentiality, integrity, and availability".

For any organization, the security objective comprises three universally accepted attributes:

- **Confidentiality:** Prevention of the unauthorized disclosure of information;
- **Integrity:** Prevention of the unauthorized modification of information; and
- **Availability:** Prevention of the unauthorized withholding of information.

8. 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 mean unauthorized entry. 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 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.
9. Some of the common techniques for controlling physical access in an organization are discussed below:
- (a) **Locks on Doors:** These are discussed below:

- **Cipher Locks** in which on entering a four digit number, the door will unlock for a predetermined period of time, usually ten to thirty seconds;
 - **Bolting Door Locks** to avoid illegal entry; and
 - **Electronic Door Locks** which has a special code that is internally stored within the card and is used to activate the door locking mechanism.
- (b) **Physical Identification Medium:** These are discussed below:
- **Personal Identification Numbers (PIN):** A secret number assigned to an individual, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual;
 - **Plastic Cards:** Used for identification purposes. Customers should safeguard their card so that it does not fall into unauthorized hands.
 - **Identification Badges:** Special identification badges with different colors and photo Ids can be issued to personnel as well as visitors for easy identification purposes.
- (c) **Logging on Facilities:** These are given as under:
- **Manual Logging:** All visitors should be prompted to sign a visitor's log indicating their name, company represented, their purpose of visit, and person to see. A 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) **Other means of Controlling Physical Access:** Other important means of controlling physical access are given as follows:
- **Video Cameras:** Refined video cameras should be placed at specific locations and monitored by security guards. The video supervision recording must be retained for possible future play back.
 - **Security Guards:** Extra security can be provided by appointing guards aided with CCTV feeds. Guards supplied by an external agency should be made to sign a bond to protect the organization from loss.
 - **Controlled Visitor Access:** A responsible employee should escort all visitors that may be friends, maintenance personnel, computer vendors, consultants and external auditors.

- **Bonded Personnel:** All service contract personnel such as cleaning people and off-site storage services should be asked to sign a bond. This may to a certain extent can limit the financial exposure of the organization.
 - **Dead Man Doors:** These systems encompass a pair of doors that are typically found in entries to facilities such as computer rooms and document stations. The first entry door must close and lock, for the second door to operate, with only one person permitted in the holding area.
 - **Non-exposure of Sensitive Facilities:** There should be no explicit indication such as presence of windows or directional signs hinting the presence of facilities such as computer rooms. Only the general location of the information processing facility should be identifiable.
 - **Computer Terminal Locks:** These locks ensure that the device to the desk is not turned on or disengaged by unauthorized persons.
 - **Controlled Single Entry Point:** All incoming personnel can use controlled Single Entry Point. A controlled entry point is monitored by a receptionist. Multiple entry points increase the chances of unauthorized entry. Unnecessary or unused entry points should be eliminated or deadlocked.
 - **Alarm System:** Illegal entry can be avoided by linking alarm system to inactive entry point and the reverse flows of enter or exit only doors, so as to avoid illegal entry. Security personnel should be able to hear the alarm when activated.
 - **Perimeter Fencing:** Fencing at boundary of the facility may also enhance the security mechanism.
 - **Control of out of hours of employee-employees:** Employees who are out of office for a longer duration during the office hours should be monitored carefully. Their movements must be noted and reported to the concerned officials frequently
 - **Secured Report/Document Distribution Cart:** Secured carts, such as mail carts, must be covered and locked and should always be attended.
10. The primary objective of a Business Continuity Planning (BCP) is to minimize loss by minimizing the cost associated with disruptions and enable an organization to survive a disaster and to reestablish normal business operations. 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 are 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.
11. There are eight phases involved in a methodology for developing a Business Continuity Plan (BCP). These 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 has the overall responsibility for providing direction and guidance to the Project Team. The committee should also make all decisions related to the recovery planning effort. 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. 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 are the other two key deliverables of this phase.

Phase 2 – Vulnerability Assessment and General Definition of Requirements: Security and controls within an organization are continuing concern. This phase addresses measures to reduce the probability of occurrence. 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

phase further defines the scope of the planning effort analyze, recommend and purchase recovery planning and maintenance software required to support the development and maintenance of the plans.

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 that is used as a basis for analyzing alternative recovery strategies. 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 definition of the plan scope, objectives and assumptions.

Phase 5 – Plan Development: During this phase, recovery plan 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.

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.

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. User Related Issues refer to those issues where user/customer is reckoned as the primary agent. Some of the user related issues that may come in achieving the system development objectives are given below:
 - **Shifting User Needs:** User requirements for IT are constantly changing. As these changes accelerate, there will be more requests for Information systems development and more development projects. When these changes occur during a development process, the development team faces the challenge of developing systems whose very purpose might change since the development process began.
 - **Resistance to Change:** People have a natural tendency to resist change and information systems development projects signal changes - often radical - in the workplace. When personnel perceive that the project will result in personnel cutbacks, threatened personnel will dig in their heels, and the development project is doomed to failure.

- **Lack of User Participation:** Users must participate in the development efforts to define their requirements, feel ownership for project success, and work to resolve development problems. User participation also helps to reduce user resistance to change.
 - **Inadequate Testing and User Training:** New systems must be tested before installation to determine that they operate correctly. Users must be trained to effectively utilize the new system.
14. **Strengths of Waterfall Model:** The fundamental strength of the Waterfall Model are given as below:
- 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.

Weaknesses of Waterfall Model: Though it is highly useful model, it suffers from various weaknesses too. Experts and practitioners identify a number of weaknesses including the following:

- 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.

15. **System Testing:** It is a process in which software and other system elements are tested as a whole. System Testing begins either when the software as a whole is operational or when the well-defined subsets of the software's functionality have been implemented. The purpose of system testing is to ensure that the new or modified system functions properly. These test procedures are often performed in a non-production test environment. The types of testing that might be carried out are as follows:
- **Recovery Testing:** This is the activity of testing 'how well the application is able to recover from crashes, hardware failures and other similar problems'. Recovery testing is the forced failure of the software in a variety of ways to verify that recovery is liable to be properly performed, in actual failures.
 - **Security Testing:** This is the process to determine that an Information System protects data and maintains functionality as intended or not. The six basic security concepts that need to be covered by security testing are – confidentiality, integrity, availability, authentication, authorization and non-repudiation. This testing technique also ensures the existence and proper execution of access controls in the new system.
 - **Stress or Volume Testing:** Stress testing is a form of testing that is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results. Stress testing may be performed by testing the application with large quantity of data during peak hours to test its performance.
 - **Performance Testing:** Software performance testing is used to determine the speed or effectiveness of a computer, network, software program or device. This testing technique compares the new system's performance with that of similar systems using well defined benchmarks.
16. Information System Audit has been categorized into five types:
- (i) **Systems and Application:** It is 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:** This is 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:** It refers to 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:** It is 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:** This refers to 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. **Audit Trail:** Audit Trail are 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. 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 Trail Objectives: Audit trails can be used to support security objectives in three ways:

- **Detecting Unauthorized Access:** Detecting unauthorized access can occur in real time or after the fact. 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. After-the-fact, detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.
- **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. For example - by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.
- **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.

18. **[Section 68] Power of Controller to give directions**

(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in

the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.

- (2) Any person who intentionally or knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or with both.
19. The Power of a Police Officer is given in the Section 80 of the IT Act (Amendment) 2008 which is as follows:

[Section 80] Power of Police Officer and Other Officers to Enter, Search, etc.

- (1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Inspector or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act

Explanation

For the purposes of this sub-section, the expression "Public Place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

- (2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.
- (3) The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section
20. **Cloud Computing Architecture:** The Cloud Computing Architecture (CCA) of a cloud solution is the structure of the system which comprises of on-premise and cloud resources, services, middleware, and software components, their geo-location, their externally visible properties and the relationships between them. Cloud architecture typically involves into multiple cloud components communicating with each other over a loose coupling mechanism, such as a messaging queue. Elastic provisioning implies intelligence in the use of tight or loose coupling of cloud resources, services, middleware, and software components.

A cloud computing architecture consists of **Front End** and a **Back End**. They connect to each other through a network, usually the Internet. The Front End is the side, the computer user sees and interacts through, and the Back End is the "cloud" section of the system, truly facilitating the services. The details are given as follow:

- **Front End Architecture:** The Front End of the cloud computing system comprises of the client's devices (or computer network) and some applications needed for accessing the cloud computing system. All the cloud computing systems do not give the same interface to users. Web services like electronic mail programs use some existing web browsers such as Firefox, Microsoft's Internet Explorer or Apple's Safari. Other types of systems have some unique applications which provide network access to its clients.
- **Back End Architecture:** Back End refers to some service facilitating peripherals. In cloud computing, the Back End is cloud itself, which may encompass various computer machines, data storage systems and servers. Groups of these clouds make up a whole cloud computing system. Theoretically, a cloud computing system can include any type of web application program such as video games to applications for data processing, software development and entertainment. Usually, every application would have its individual dedicated server for services.

A central server is established to be used for administering the whole system. It is also used for monitoring client's demand as well as traffic to ensure that everything of system runs without any problem. There are some protocols that are followed by this server and it uses a special type of software known as Middleware that allows computers that are connected on networks to communicate with each other. If any cloud computing service provider has many customers, then there's likely to be very high demand for huge storage space. The cloud computing system must have a redundant back-up copy of all the data of its client's.

21. (a) **Segregation of Duties:** Segregation of duties means that in the processing of a transaction, there are split between different people, such that one person cannot process a transaction right from start to finish. Various stages in the transaction cycle are spread between two or more individuals. However, in a computerized system, the auditor should also be concerned with the segregation of duties within the IT department. 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. IT staff may also be in a position to alter transaction data or even the financial applications which process the transactions.
- (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. The main characteristics of the corrective controls are as follows:
- 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 given as follows:

- Contingency planning;
 - Backup procedure;
 - Rerun procedures;
 - Change input value to an application system; and
 - Investigate budget variance and report violations.
- (c) **Cryptography:** It deals with programs for transforming data into cipher text that are meaningless to anyone, who does not possess the authentication to access the respective system resource or file. A cryptographic technique encrypts data (clear text) into cryptograms (cipher text) and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst. 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).
- (d) **Schedule Feasibility:** Schedule feasibility or Time 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.
- (e) **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.
22. (a) **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.

- (b) **Abstract System:** Also known as Conceptual System, it can be defined as an orderly arrangement of interdependent ideas or constructs. For example, a system of theology is an orderly arrangement of ideas about God and the relationship of humans to God.

Physical System: It is a set of tangible elements which operate together to accomplish an objective e.g. Computer system, University system etc.

- (c) **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.

- (d) **Platform as a Service (PaaS):** Cloud providers deliver a computing platform including operating system, programming language execution environment,

database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of acquiring and managing the underlying hardware /software layers. In PaaS, one can make applications and software on other's database. Thus, it gives us the platform to create, edit, run and manage the application programs we want.

Software as a Service (SaaS): SaaS provides users to access large variety of applications over internet that are hosted on service provider's infrastructure. For example, one can make his/her own word document in Google docs online, s/he can edit a photo online on pixlr.com so s/he need not install the photo editing software on his/her system- thus Google is provisioning Software as a Service.

23. (a) The popular implementation strategies that may be used to convert an old system into new system 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. This 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 as 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.
- (b) **[Section 7] Retention of Electronic Records**
- (1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to

have been satisfied if such documents, records or information are retained in the electronic form, -

- (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:

However,

this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

- (2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records, publication of rules, regulation, etc. in Electronic Gazette.

24. (a) **Feasibility Study:** After possible solution options are identified, project feasibility i.e. the likelihood that these systems will be useful for the organization is determined. 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:** Is the technology needed available?
- **Financial:** Is the solution viable financially?
- **Economic:** Return on Investment?
- **Schedule/Time:** Can the system be delivered on time?
- **Resources:** Are human resources reluctant for the solution?
- **Operational:** How will the solution work?
- **Behavioural:** Is the solution going to bring any adverse effect on quality of work life?
- **Legal:** Is the solution valid in legal terms?

(b) **Fact Finding:** Every system is built to meet some set of needs, for example, the need of the organization for lower operational costs, better information for

managers, smooth operations for users or better levels of services to customers. To assess these needs, the analysts often interact extensively with people, who will be benefited from the system in order to determine 'what are their actual requirements'. Various fact-finding techniques/tools used by the system analyst for determining these needs/requirements are briefly discussed below:

- (i) **Documents:** Documents mean manuals, input forms, output forms, diagrams of how the current system works, organization charts showing hierarchy of users and manager responsibilities, job descriptions for the people, who work with the current system, procedure manuals, program codes for the applications associated with the current system, etc. Documents are a very good source of information about user needs and the current system.
 - (ii) **Questionnaires:** Users and managers are asked to complete questionnaire about the information systems when the traditional system development approach is chosen. The main strength of questionnaire is that a large amount of data can be collected through a variety of users quickly. Also, if the questionnaire is skilfully drafted, responses can be analyzed rapidly with the help of a computer.
 - (iii) **Interviews:** Users and managers may also be interviewed to extract information in depth. The data gathered through interviews often provide system developers with a larger picture of the problems and opportunities. Interviews also give analyst the opportunity to observe and record first-hand user reaction and to probe for further information.
 - (iv) **Observation:** In general and particularly in prototyping approaches, observation plays a central role in requirement analysis. Only by observing how users react to prototypes of a new system, the system can be successfully developed.
- (c) Some of the weaknesses of Rapid Application Development (RAD) model identified by the experts and practitioners include the following:
- Fast speed and lower cost may affect adversely the system quality.
 - The project may end up with more requirements than needed (gold-plating).
 - Potential for feature creep where more and more features are added to the system over the course of development.
 - It may lead to inconsistent designs within and across systems.
 - It may call for violation of programming standards related to inconsistent naming conventions and inconsistent documentation,
 - It may call for lack of attention to later system administration needs built into system.

- Formal reviews and audits are more difficult to implement than for a complete system.
 - Tendency for difficult problems to be pushed to the future to demonstrate early success to management.
 - Since some modules will be completed much earlier than others, well-defined interfaces are required.
25. If Mr. B wants to file an FIR against Mr. A, then he may file the same under the following Section of Information Technology (Amendment) Act, 2008:
- Section 66A: Punishment for sending offensive messages through communication service, etc.; and
 - Section 66B: Punishment for dishonestly receiving stolen computer resource or communication device.

All these applicable sections in this case are given as follows:

[Section 66A] Punishment for sending offensive messages through communication service, etc.

Any person who sends, by means of a computer resource or a communication device,-

- (a) any information that is grossly offensive or has menacing character; or
- (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently by making use of such computer resource or a communication device,
- (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

[Section 66B] Punishment for dishonestly receiving stolen computer resource or communication device.

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.