PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

Multiple Choice Questions

XYZ is a life insurance company which offers wide variety of insurance plans like protection, retirement, health, saving and investment, child education and travel insurance plans etc., which cater to the risk management and insurance requirements of individuals as well as groups. It has more than 200 branches all over India which are fully automated.

Each product plan of the company offers adequate risk coverage at low rates through a simple application process. The company offers special discounts to its clients who share their fitness data with the company on regular basis.

With the goal to grow further, the company in the year 2019 launched its website that provided many online facilities to its clients to purchase its various plans. Using the Cloud Computing technology; all the data related to clients and their claims, policies, staff members and brokers are stored in a database and are hosted on a cloud.

Recently in the year 2020, audit of 50 randomly selected branches were conducted with a view to obtain a reasonable assurance on accuracy and consistency of data. The audit was performed considering standard laws, guidelines, and policies relevant to insurance business as well as IT. Various audit findings and recommendations that were reported to the Top Management of XYZ Company are as follows:

- There is a need to make voluminous data available from cloud to users on 24 x 7 basis.
- The controls that ensure the availability of system in case of data loss due to unauthorized access and equipment failure etc. are not adequate.
- There is a requirement to establish a mechanism to transfer the data in an encrypted form in its network to protect it from unauthorized access.
- Special audit routines are said to be missing in the system, with the result notifying of suspicious records with frequent change in name and address, is not possible. This arrangement has made the policyholder system more vulnerable to frauds like funds withdrawal like false claims.
- One such false claim has been observed during the audit wherein it was found that an employee of Nagpur branch, Mr. Girish fraudulently used electronic signature of his branch manager and dishonestly approved a false claim of one of its clients, Mr. Saraf thereby allowing him to withdraw his funds.

Based on the facts of the case scenario given above, choose the most appropriate answer to Q. No(s) 1 to 6.

1. The company XYZ has adopted the cloud computing technology to obtain the resources in terms of memory and database storage. Which service model of Cloud Computing is applicable in this case?

   (a) Software as a Service (SaaS)

   (b) Infrastructure as a Service (IaaS)

   (c) Platform as a Service (PaaS)

   (d) Communication as a Service (CaaS)

2. An IS auditor found that Mr. Girish, an employee of the company, dishonestly had made use of electronic signature of the branch manager of Nagpur branch of XYZ company and passed the false claim of one of the clients named Mr. Saraf. Under which section of IT Act, 2000 do you think is Mr. Girish punishable?

   (a) Section 66B

   (b) Section 66C

   (c) Section 66D

   (d) Section 43

3. In purview of above case scenario, which type of audit routines can be recommended by IS auditor to be implemented in XYZ company to avoid withdrawal of funds due to false claims?

   (a) Continuous and Intermittent Simulation

   (b) Snapshot

   (c) System Control and Review File

   (d) Audit Hook

4. To the clients who wish to buy various plans on discounted rates, the XYZ company offered them technology based wearable smart watches and bands that provided the details regarding their medical condition to the company on regular basis. Identify the risk management strategy under which this initiative of the company falls into.

   (a) Tolerate the risk

   (b) Terminate the risk

   (c) Transfer the risk

(d) Treat the risk

5. For XYZ company, the well implementation of logical access controls in the systems of all of its branches is essential as otherwise there could be potential loss resulting in total shutdown of the computer functions of any branch.

(i) Segregation of Networks (ii) Call back devices

(iii) Plastic Cards (iv) Terminal log-in procedures

(v) User identification and Authentication (vi) Alarm System

(vii) Water Detectors

Identify the set of control(s) that fit under the category of Logical Access Controls.

(a) (i), (ii), (iv), (v)

(b) (i), (ii), (iv), (v), (vii)

(c) (i), (iv), (v)

(d) (i), (v), (vi), (vii)

6. Let's assume that the XYZ Life insurance company has adopted the Incremental Backup Plan/Strategy for its data. In such a case, identify the statement that does not hold true for Incremental Backups.

(a) One full backup is done first, and subsequent backup runs are just the changed files.

(b) For restoration, all sets of backups are required to be performed.

(c) The speed of restoration is faster as compared to Differential Backup.

(d) The speed of restoration is slower than with a Full backup.

Question No(s). 7 and 8 are independent questions.

7. The Testing phase of Systems Development Life Cycle (SDLC) at different levels is used to identify the correctness, completeness, and quality of developed computer software. Identify the correct sequence of testing done at different levels.

(a) Regression Testing, Unit Testing, Integration Testing, System Testing, Acceptance Testing

(b) Unit Testing, System Testing, Integration Testing, Regression Testing, Acceptance Testing

(c) Unit Testing, Regression Testing, Integration Testing, Acceptance Testing, System Testing

(d) Unit Testing, Integration Testing, Regression Testing, System Testing, Acceptance Testing

8. Nowadays various educational institutions, offices and companies have adopted different electronic means like teleconferencing and videoconferencing to hold their meetings with staff members, clients, and various stakeholders. This mode of communication systems is best categorized under _____.

(a) Strategic Level Systems

(b) Knowledge Level Systems

(c) Operational Level Systems

(d) Management Level Systems

Descriptive Questions

Chapter 1: Concepts of Governance and Management of Information Systems

9. Planning is an essential key factor that determines and monitors the direction and achievement of an enterprise' goals and objectives. Discuss different levels of managerial activities that are carried out in an enterprise to decide in advance "what is to be done" and "when it is going to be done".

10. IT Governance refers to a system that focuses on IT to evaluate, direct and monitor IT management so as to ensure effectiveness, accountability and compliance of IT. As an internal auditor, what shall be your perspective while determining the status of IT Governance of an enterprise?

Chapter 2: Information System Concepts

11. DEF Pvt. Ltd. is an export house in Gujarat that manufactures wide range of house furnishing products and exports them to SAARC countries. Mr. Raj, the chief manager of the export house suggested the management to implement Enterprise Resource Planning (ERP) in their workplace so as to acquire an integrated system that automates its business functions. In light of this, discuss different components of ERP model and its benefits that company may avail.

12. Information is the backbone of any organization that can be used by Senior Managers, Middle and Operational Managers etc. for their specific purposes. Discuss important attributes of Information that make it useful to the aforementioned groups.

Chapter 3: Protection of Information Systems

13. Implementation of Output controls in an application ensures the delivery of data to users in secure and consistent manner. Considering this statement, explain the various output controls required to be reviewed by an IS auditor during audit.

14. With an increase in technology at global pace, the cyber frauds are also increasing on continuous basis. Discuss in brief, the major techniques used to commit cyber frauds.

Chapter 4: Business Continuity Planning and Disaster Recovery Planning

15. DEF Ltd. is a Knowledge Process Outsourcing (KPO) company having access to confidential data of its huge clientele worldwide. Mr Rajesh, the senior IT head suggested the company to implement Business Continuity Plan to minimize the loss associated with disaster or disruption. What should be the objectives and goals of Contingency Plan that enable the company to recover from disaster and continue with its operation with least impact?

16. Briefly explain various types of data backups that an organization may use to reserve the data so as to recover its systems and operations in case of any disaster.

Chapter 5: Acquisition, Development and Implementation of Information Systems

17. ABC Company is a manufacturer of automobile parts with many branches in different cities of India. The management of company felt that existing information system does not meet its present requirements and seek for a new system to streamline and integrate its operation processes and information flow to synergize all its major resources. Mr. Anil, the IT head of the company is working on development of new system following the best practices of System Development Life Cycle (SDLC). Briefly discuss various activities to be performed by him during the phase of System Requirement Analysis.

18. Being a part of the SDLC team, you are supposed to test the proposed software of ABC Ltd. Discuss different levels of Testing that you may conduct to detect the software defects.

Chapter 6: Auditing of Information Systems

19. Different audit organizations go about IS auditing in various ways and individual auditor has its own way of working. However, IS audit process can still be broadly categorized into various steps. Explain these steps involved in Information Systems Audit Process.

20. In terms of the audit tool, identify the audit tool used by an Auditor wherein a dummy entity is created in the application system files and performs the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness. Explain the identified audit tool.

Chapter 7: Information Technology Regulatory Issues

21. Discuss the provision given in Information Technology Act, 2008 that describes Penalties and Compensation for damage to computer, computer system, etc.

22. The National Cyber Security Policy, 2013 is designed to protect information infrastructure and preservation of confidentiality, integrity, and availability of information in cyber space. In purview of above statement, discuss the major objectives of this policy.

Chapter 8: Emerging Technologies

23. Platform as a Service (PaaS) is a service model of cloud computing that enables the user to develop and deploy an application on the development platform provided by the service provider. Discuss the services provides by PaaS along with its characteristics.

24. Mobile Computing is the technology that allows transmission of data via a computer without having to be connected to a fixed physical link and thus proves to be the solution of the biggest problem of business people on the move. Discuss the benefits as well as limitations of Mobile Computing.

SUGGESTED ANSWERS

1. **(b)** Infrastructure as a Service (IaaS)

2. **(b)** Section 66C

3. **(d)** Audit Hook

4. **(d)** Treat the risk

5. **(a)** (i), (ii), (iv), (v)

6. **(c)** The speed of restoration is faster as compared to Differential Backup.

7. **(d)** Unit Testing, Integration Testing, Regression Testing, System Testing, Acceptance Testing

8. **(b)** Knowledge Level Systems

9. The different levels of managerial activities in an enterprise 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.

10. The key practices, which determine the status of IT Governance in the enterprise, are as follows:

- Who makes directing, controlling and executing decisions?
- How are the decisions made?
- What information is required to make the decisions?
- What decision-making mechanisms are required?
- How are exceptions handled?
- How are the governance results monitored and improved?

11. The different components of Enterprise Resource Planning (ERP) 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 Intelligent.

(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's mindset:** By implementing ERP system, the old ways for working which user understand and are comfortable with, have to be changed and may lead to users' resistance. For example, some users may say that they have spent many years doing an excellence job without help from ERP system. 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.

The benefits of ERP that company may avail 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.

12. The attributes of information that make it useful to the Senior Managers, Middle and Operational Managers are as follows:

- **Availability:** It is a very important aspect of information. 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. Depending upon the activities in an organization the Information communicated to people has a purpose. 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 modes of communicating information to humans should be in such a way that it can be easily understandable 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, for example - 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.
- **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.

13. Various Output Controls required to be reviewed by an IS auditor are as follows:

- **Storage and logging of sensitive, critical forms:** Pre-printed stationery should be stored securely to prevent unauthorized destruction or removal and usage. Only

authorized persons should be allowed access to stationery supplies such as security forms, negotiable instruments, etc.

- **Logging of output program executions:** When programs used for output of data are executed, these should be logged and monitored; otherwise confidentiality/integrity of the data may be compromised.
- **Spooling/queuing:** "Spool" is an acronym for "Simultaneous Peripherals Operations Online". This is a process used to ensure that the user can continue working, while the print operation is getting completed. When a file is to be printed, the operating system stores the data stream to be sent to the printer in a temporary file on the hard disk. This file is then "spooled" to the printer as soon as the printer is ready to accept the data. This intermediate storage of output could lead to unauthorized disclosure and/or modification. A queue is the list of documents waiting to be printed on a particular printer; this should not be subject to unauthorized modifications.
- **Controls over printing:** Outputs should be made on the correct printer and it should be ensured that unauthorized disclosure of information printed does not take place. Users must be trained to select the correct printer and access restrictions may be placed on the workstations that can be used for printing.
- **Report distribution and collection controls:** Distribution of reports should be made in a secure way to prevent unauthorized disclosure of data. It should be made immediately after printing to ensure that the time gap between generation and distribution is reduced. A log should be maintained for reports that were generated and to whom these were distributed. Where users have to collect reports, the user should be responsible for timely collection of the report, especially if it is printed in a public area. A log should be maintained about reports that were printed and collected. Uncollected reports should be stored securely.
- **Retention controls:** Retention controls consider the duration for which outputs should be retained before being destroyed. Consideration should be given to the type of medium on which the output is stored. Retention control requires that a date should be determined for each output item produced. Various factors ranging from the need of the output, use of the output, to legislative requirements would affect the retention period.

14. The major techniques to commit cyber frauds are as follows:

- **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 programs that lie 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.

15. The 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 Contingency 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.

16. Various types of Data backups that an organization may use are as follows:

(i) **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. At each backup run, all files designated in the backup job will be backed up again. This includes files and folders that have not changed. It is commonly used as an initial or first backup followed with subsequent incremental or differential backups. After several incremental or differential backups, it is common to start over with a fresh full backup again. Some also like to do full backups for all backup runs typically for smaller folders or projects that do not occupy too much storage space. The Windows operating system lets us to copy a full backup on several DVD disks. Any good backup plan has at least one full backup of a server. For example - Suppose a full backup job or task is to be done every night from Monday to Friday. The first backup on Monday will contain the entire list of files and folders in the backup job. On Tuesday, the backup will include copying all the files and folders again, no matter the files have got changed or not. The cycle continues this way.

(ii) **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.

(iii) 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. Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved. Restoring from a differential backup is a two-step operation: Restoring from the last full backup; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup probably includes files that were already included in earlier differential backups. 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.

(iv) Mirror back-up: Mirror backups are, as the name suggests, a mirror of the source being backed up. With mirror backups, when a file in the source is deleted, that file is eventually also deleted in the mirror backup. Because of this, mirror backups should be used with caution as a file that is deleted by accident, sabotage or through a virus may also cause that same file in mirror to be deleted as well. Some do not consider a mirror to be a backup. Further, a mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data. For example - Many online backup services offer a mirror backup with a 30 day delete. This means that when you delete a file on your source, that file is kept on the storage server for at least 30 days before it is eventually deleted. This helps strike a balance offering a level of safety while not allowing the backups to keep growing since online storage can be relatively expensive. Many backup software utilities do provide support for mirror backups.

17. Various activities to be performed by Mr. Anil during the phase of System Requirement Analysis of Systems Development Life Cycle (SDLC) are as follows:

(i) 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 that are used by the system analyst for determining these needs/requirements are Documents including manuals, input forms, diagrams of how the current system works, organization charts etc., Questionnaires, Interviews and Observation approach.

(ii) Analysis of the Present System: Detailed investigation of the present system involves collecting, organizing and evaluating facts about the system and the environment in which it operates. There should be enough information assembled so that a qualified person can understand the present system without visiting any of the operating departments. The survey of existing methods, procedures, data flow, outputs, files, input and internal controls should be intensive in order to fully understand the present system and its related problems. The areas studied in depth should include reviewing historical aspects, analyzing inputs and outputs, reviewing data files, methods and internal controls, procedure and data communications, modeling the existing system and undertaking overall analysis of the existing system.

(iii) System Analysis of Proposed Systems: After a thorough analysis of each functional area of the present information system, the proposed system specifications must be clearly defined, which are determined from the desired objectives set forth at the first stage of the study. Likewise, consideration should be given to the strengths and short comings of the present system. The required systems specifications should be in conformity with the project's objectives articulated and in accordance with the following:

- Outputs are produced with great emphasis on timely managerial reports that utilize the management by exception' principle.
- Databases are maintained with great accent on online processing capabilities.
- Input data is prepared directly from original source documents for processing by the computer system.
- Methods and procedures that show the relationship of inputs and outputs to the database, utilize data communications as, when and where deemed appropriate.
- Work volumes and timings are carefully considered for present and future periods including peak periods.

(iv) System Development Tools: Many tools and techniques including structured English, Flowcharts, Data Flow Diagrams, Decision Trees etc., have been developed to improve current information systems and to develop new ones. Such tools help end users and systems analysts primarily for the following:

- To conceptualize, clarify, document and communicate the activities and resources involved in the organization and its information systems;
- To analyze present business operations, management decision making and information processing activities of the organization; and
- To propose and design new or improved information systems to solve business problems or pursue business opportunities that have been identified.

(v) 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 contain 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.

18. The different levels of testing to detect software defects are as follows:

(i) Unit Testing: In computer programming, unit testing is a software verification and validation method in which a programmer tests if individual units of source code are fit for use. A unit is the smallest testable part of an application, which may be an individual program, function, procedure, etc. or may belong to a base/super class, abstract class or derived/child class. Unit tests are typically written and run by software developers to ensure that code meets its design and behaves as intended. The goal of unit testing is to isolate each component of the program and show that they are correct. A unit test provides a strict, written contract that the piece of code

must satisfy. There are five categories of tests that a programmer typically performs on a program unit are – functional tests, performance tests, stress test, structural test and parallel test.

(ii) **Integration Testing:** Integration testing is an activity of software testing in which individual software modules are combined and tested as a group. It occurs after unit testing and before system testing with an objective to evaluate the validity of connection of two or more components that pass information from one area to another. Integration testing takes as its input modules that have been unit tested, groups them in larger aggregates, applies tests defined in an integration test plan to those aggregates, and delivers as its output the integrated system ready for system testing. This is carried out in the two manners i.e. Bottom up integration and top-down integration.

(iii) **Regression Testing:** Each time a new module is added or any modification made in the software, it changes. New data flow paths are established, new I/O may occur and new control logic is invoked. These changes may cause problems with functions that previously worked flawlessly. In the context of the integration testing, the regression tests ensure that changes or corrections have not introduced new faults. The data used for the regression tests should be the same as the data used in the original test.

(iv) **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. It can be carried out as recovery testing, security testing, stress or volume testing and performance testing.

(v) **Final Acceptance Testing:** It is conducted when the system is just ready for implementation. During this testing, it is ensured that the new system satisfies the quality standards adopted by the business and the system satisfies the users. Thus, the final acceptance testing has two major parts **Quality Assurance testing** and **User Acceptance testing.** Quality Assurance testing ensures that the new system satisfies the prescribed quality standards and the development process is as per the organization's quality assurance policy, methodology and prescriptions. User Acceptance testing ensures that the functional aspects expected by the users have been well addressed in the new system.

19. The steps involved in Information Systems Audit Process are as follows:

(i) **Scoping and pre-audit survey:** Auditors determine the main area/s of focus and any areas that are explicitly out-of-scope, based on the scope-definitions agreed with management. Information sources at this stage include background reading

and web browsing, previous audit reports, pre audit interview, observations and, sometimes, subjective impressions that simply deserve further investigation.

(ii) Planning and preparation: During which the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan or risk-control-matrix.

(iii) Fieldwork: This step involves gathering of evidence by interviewing staff and managers, reviewing documents, and observing processes etc.

(iv) Analysis: This step involves desperately sorting out, reviewing and trying to make sense of all that evidence gathered earlier. SWOT (Strengths, Weaknesses, Opportunities, Threats) or PEST (Political, Economic, Social, Technological) techniques can be used for analysis.

(v) Reporting: Reporting to the management is done after analysis of evidence is gathered and analyzed.

(vi) Closure: Closure involves preparing notes for future audits and follow up with management to complete the actions they promised after previous audits.

20. The audit tool used by an Auditor in this case is Integrated Test Facility (ITF), the description of the tool is given below:

The ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness. This test data would be included with the normal production data used as input to the application system. In such cases the auditor has to decide what would be the method to be used to enter test data and the methodology for removal of the effects of the ITF transactions.

- **Methods of Entering Test Data:** The transactions to be tested have to be tagged. The application system has to be programmed to recognize the tagged transactions and have them invoke two updates, one to the application system master file record and one to the ITF dummy entity. Auditors can also embed audit software modules in the application system programs to recognize transactions having certain characteristics as ITF transactions. Tagging live transactions as ITF transactions has the advantages of ease of use and testing with transactions representative of normal system processing. However, use of live data could mean that the limiting conditions within the system are not tested and embedded modules may interfere with the production processing. The auditors may also use test data that is specially prepared. Test transactions would be entered along with the production input into the application system. In this approach the test data is likely to achieve more complete coverage of the execution paths in the application system to be tested than selected production data and the application system does not have to be modified to tag the ITF transactions and to treat them in a special way. However, preparation of the test data could be time consuming and costly.

- **Methods of Removing the Effects of ITF Transactions:** The presence of ITF transactions within an application system affects the output results obtained. The effects of these transactions have to be removed. The application system may be programmed to recognize ITF transactions and to ignore them in terms of any processing that might affect users. Another method would be the removal of effects of ITF transactions by submitting additional inputs that reverse the effects of the ITF transactions. Another less used approach is to submit trivial entries so that the effects of the ITF transactions on the output are minimal. The effects of the transactions are not really removed.

21. The provision of Information Technology Act, 2008 that describes Penalties and Compensation for damage to computer, computer system, etc. is **Section 43**, which is described as below:

If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network, -

(a) accesses or secures access to such computer, computer system or computer network or computer resource;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(j) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage,

he shall be liable to pay damages by way of compensation to the person so affected.

Explanation –

For the purposes of this section, -

(i) "**computer contaminant**" means any set of computer instructions that are designed-

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "**computer database**" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "**computer virus**" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) "**damage**" means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means.

(v) "**computer source code**" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

22. The objectives of the National Cyber Security Policy, 2013 are as follows:

- To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy;
- To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology, & people);
- To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem;

- To enhance and create National and Sectorial level 24*7 mechanisms for obtaining strategic information regarding threats of ICT infrastructure creating scenarios for response, resolution and crisis management through effective predicative, protective, response and recovery actions;
- To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Center(NCIIPC) and mandating security practices related to the design, acquisition, development and operation of information resources;
- To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, and pilot development of secure ICT products/processes in general and specifically for addressing National Security requirements;
- To improve visibility of the integrity of Information & Communication Technology products & services and establishing infrastructure for testing & validation of security of such products;
- To create a workforce of 500,000 professional skilled in cyber security in the next 5 years through capacity building, skill development and training;
- To provide fiscal benefits to businesses for adoption of standard security practices and processes;
- To enable protection of information while in process, handling, storage & transit so as to Safeguard privacy of citizen's data and for reducing economic losses due to cybercrime or data theft;
- To enable effective prevention, investigation and prosecution of cybercrime and enhancements of law enforcement capabilities through appropriate legislative intervention;
- To create a culture of cyber security and privacy enabling responsible user behavior & actions through an effective communication and promotion strategy;
- To develop effective public private partnerships and collaborative engagements through technical and operational and contribution for enhancing the security of cyberspace and
- To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

23. The services provided by Platform as a Service (PaaS) are as follows:

- **Programming Languages:** PaaS providers provide a wide variety of programming languages like Java, PHP, Python, Ruby etc. for the developers to develop applications.

- **Application Frameworks:** PaaS vendors provide application development framework like Joomla, WordPress, Sinatra etc. for application development.
- **Database:** Along with PaaS platforms, PaaS providers provide some of the popular databases like ClearDB, Cloudant, Redis etc. so that application can communicate with the databases.
- **Other Tools:** PaaS providers provide all the tools that are required to develop, test, and deploy an application.

The characteristics of PaaS are as follows:

- **All in One:** Most of the PaaS providers offer services like programming languages to develop, test, deploy, host and maintain applications in the same Integrated Development Environment (IDE).
- **Web access to the development platform:** PaaS provides web access to the development platform that helps the developers to create, modify, test, and deploy different applications on the same platform.
- **Offline Access:** To enable offline development, some of the PaaS providers allow the developer to synchronize their local IDE with the PaaS services. The developers can develop an application locally and deploy it online whenever they are connected to the Internet.
- **Built-in Scalability:** PaaS services provide built-in scalability to an application that is developed using any particular PaaS. This ensures that the application is capable of handling varying loads efficiently.
- **Collaborative Platform:** To enable collaboration among developers, most of the PaaS providers provide tools for project planning and communication.
- **Diverse Client Tools:** PaaS providers offer a wide variety of client tools like Web User Interface (UI), Application Programming Interface (API) etc. to help the developers to choose the tool of their choice.

24. The benefits of Mobile Computing are as follows:

- It provides mobile workforce with remote access to work order details, such as work order location, contact information, required completion date, asset history relevant warranties/service contracts.
- It enables mobile sales personnel to update work order status in real-time, facilitating excellent communication.
- It facilitates access to corporate services and information at any time, from anywhere.
- It provides remote access to the corporate Knowledgebase at the job location.

- It enables to improve management effectiveness by enhancing information quality, information flow, and ability to control a mobile workforce.

The 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.