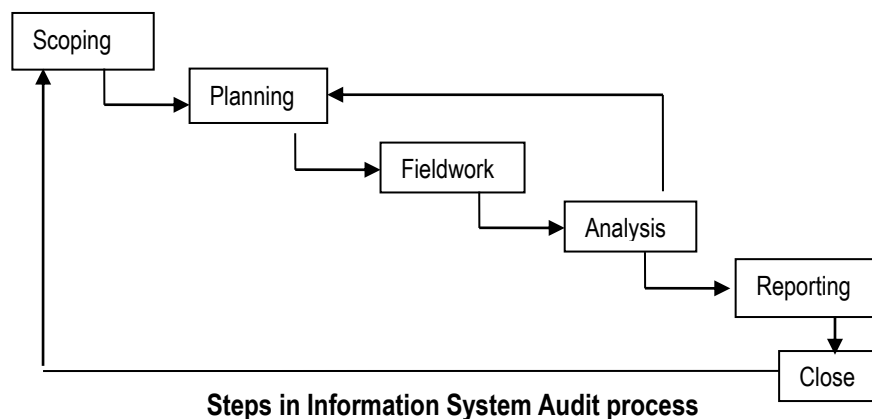


MOCK TEST PAPER- 1
FINAL COURSE GROUP-II
PAPER-6: INFORMATION SYSTEMS CONTROL & AUDIT
SUGGESTED ANSWER/HINTS

1. (a) Steps that an Auditor follows during Information System Audit 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 this step, 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, and Threats) or PEST (Political, Economic, Social, and 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.

Analysis and reporting may involve the use of automated data analysis tools such as ACL or IDEA, if not Excel, Access and hand-crafted SQL queries. Automated system security analysis, configuration or vulnerability management and security benchmarking tools are also used for reviewing security parameters, and the basic security management functions that are built-in to modern systems can help with log analysis, reviewing user access rights etc.

(b) Some of the most notable user related issues because of which an enterprise at times fails to achieve the objectives of the system development are described briefly as follows:

- **Shifting User Needs:** User requirements for IT are constantly changing. As these changes accelerate, there will be more requests for Information systems development and more development projects. When these changes occur during a development process, the development team faces the challenge of developing systems whose very purpose might change since the development process began.
- **Resistance to Change:** People have a natural tendency to resist change, and information systems development projects signal changes - often radical - in the workplace. When personnel perceive that the project will result in personnel cutbacks, threatened personnel will dig in their heels, and the development project is doomed to failure.
- **Lack of Users' 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.

(c) In Information Technology (Amendment) Act, 2008; Section 7 is related to the "Retention of Electronic Records" and Section 7A is related to the "Audit of documents in electronic form".

[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.

[Section 7A] Audit of Documents etc. in Electronic form

Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in electronic form.

- 2. (a) **Examples of Decision Support Systems in Accounting** – Many DSS are developed in-house using either a general type of decision support program or a spreadsheet program to solve specific problems. Below are several illustrations of these systems:

- **Cost Accounting System** - The health care industry is well known for its cost complexity. Managing costs in this industry require controlling costs of supplies, expensive machinery, technology, and a variety of personnel. Cost accounting applications help health care enterprises calculate product costs for individual procedures or services. One health care organization, for example, combines a variety of DSS applications in productivity, cost accounting, case mix, and nursing staff scheduling to improve its management decision making.
- **Capital Budgeting System** - Companies require new tools to evaluate high-technology investment decisions. Decision makers need to supplement analytical techniques, such as net present value and internal rate of return, with decision support tools that consider some benefits of new technology not captured in strict financial analysis. One DSS designed to support decisions about investments in automated manufacturing technology is Auto Man, which allows decision makers to consider financial, non financial, quantitative, and qualitative factors in their decision-making processes. Using this decision support system, accountants, managers, and engineers identify and prioritize these factors. Then they can evaluate up to seven investment alternatives at once.

- **Budget Variance Analysis System** - Financial institutions rely heavily on their budgeting systems for controlling costs and evaluating managerial performance. One institution uses a computerized DSS to generate monthly variance reports for division comptrollers. The system allows these comptrollers to graph, view, analyze, and annotate budget variances, as well as create additional one-and five-year budget projections using the forecasting tools provided in the system. The decision support system thus helps the comptrollers create and control budgets for the cost-center managers reporting to them.
 - **General Decision Support System** - As mentioned earlier, some planning languages used in Decision Support Systems are general purpose and therefore have the ability to analyze many different types of problems. In a sense, these types of decision support systems are a decision-maker's tools. The user needs to input data and answer questions about a specific problem domain to make use of this type of decision support system. An example is a program called Expert Choice which supports a variety of problems requiring decisions. The user works interactively with the computer to develop a hierarchical model of the decision problem. The DSS then asks the user to compare decision variables with each other. For instance, the system might ask the user how important cash inflows are versus initial investment amount to a capital budgeting decision. The decision maker also makes judgments about which investment is best with respect to these cash flows and which requires the smallest initial investment. Expert choice analyzes these judgments and presents the decision maker with the best alternative.
- (b) Audit of environmental controls requires the IS auditor to conduct physical inspections and observe practices. The Auditor should verify:
- The IPF (Infrastructure Planning and Facilities) and the construction with regard to the type of materials used for construction;
 - The presence of water and smoke detectors, power supply arrangements to such devices, and testing logs;
 - The location of fire extinguishers, firefighting equipment and refilling date of fire extinguishers;
 - Emergency procedures, evacuation plans and marking of fire exists. There should be half-yearly Fire drill to test the preparedness;
 - Documents for compliance with legal and regulatory requirements with regards to fire safety equipment, external inspection certificate and shortcomings pointed out by other inspectors/auditors;
 - Power sources and conduct tests to assure the quality of power, effectiveness of the power conditioning equipment, and generators. Also the power supply interruptions must be checked to test the effectiveness of the back-up power;

- Environmental control equipment such as air-conditioning, dehumidifiers, heaters, ionizers etc.;
 - Compliant logs and maintenance logs to assess if MTBF and MTTR are within acceptable levels; and
 - Identify undesired activities such as smoking, consumption of eatables etc.
- (c) Two primary methods with the help of which the scope of the project can be analyzed are given as follows:
- **Reviewing Internal Documents:** The analysts conducting the investigation first try to learn about the organization involved in, or affected by, the project. For example, to review an inventory system proposal, an analyst may try to know how does the inventory department operates and who are the managers and supervisors. Analysts can usually learn these details by examining organization charts and studying written operating procedures.
 - **Conducting Interviews:** Written documents tell the analyst how the systems should operate, but they may not include enough details to allow a decision to be made about the merits of a systems proposal, nor do they present users' views about current operations. To learn these details, analysts use interviews. Interviews allow analysts to know more about the nature of the project request and the reasons for submitting it. Usually, preliminary investigation interviews involve only management and supervisory personnel.
3. (a) The Disaster Recovery Planning document may include the following areas:
- The conditions for activating the plans, which describe the process to be followed before each plan, are activated.
 - Emergency procedures, which describe the actions to be taken following an incident which jeopardizes business operations and/or human life. This should include arrangements for public relations management and for effective liaisoning with appropriate public authorities e.g. police, fire, services and local government.
 - Fallback procedures, which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time-scale.
 - Resumption procedures, which describe the actions to be taken to return to normal business operations.
 - A maintenance schedule, which specifies 'how and when the plan will be tested', and the process for maintaining the plan.
 - Awareness and education activities, which are designed to create an understanding of the business continuity, process and ensure that the business continues to be effective.

- The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
 - Contingency plan document distribution list.
 - Detailed description of the purpose and scope of the plan.
 - Contingency plan testing and recovery procedure.
 - List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
 - Checklist for inventory taking and updating the contingency plan on a regular basis.
 - List of phone numbers of employees in the event of an emergency.
 - Emergency phone list for fire, police, hardware, software, suppliers, customers, back-up location, etc.
 - Medical procedure to be followed in case of injury.
 - Back-up location contractual agreement, correspondences.
 - Insurance papers and claim forms.
 - Primary computer center hardware, software, peripheral equipment and software configuration.
 - Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
 - Alternate manual procedures to be followed such as preparation of invoices.
 - Names of employees trained for emergency situation, first aid and life saving techniques.
 - Details of airlines, hotels and transport arrangements.
- (b) The major objectives of Systems Requirements Analysis phase in SDLC to generate Systems Requirements Specification (SRS) are as follows:
- To identify and consult the stake owners to determine their expectations and resolve their conflicts;
 - To analyze requirements to detect and correct conflicts and determine priorities;
 - To gather data or find facts using tools like - interviewing, research/document collection, questionnaires, observation;
 - To verify that the requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable;
 - To model activities such as developing models to document Data Flow Diagrams, E-R Diagrams; and

- To document activities such as interview, questionnaires, reports etc. and development of a system (data) dictionary to document the modeling activities.
- (c) The Advantages of Public Cloud include the following:
- It is widely used in the development, deployment and management of enterprise applications, at affordable costs.
 - It allows the organizations to deliver highly scalable and reliable applications rapidly and at more affordable costs.
 - There is no need for establishing infrastructure for setting up and maintaining the cloud.
 - Strict SLAs are followed.
 - There is no limit for the number of users.

Limitations of Public Cloud are as follows:

- One of the limitation of Public Cloud is security assurance and thereby building trust among the clients is far from desired but slowly liable to happen.
- Further, privacy and organizational autonomy are not possible.

4. (a) Risks related to the use of Personal Computers (PCs) in the business are as follows:

- Personal computers are small and easy to connect and disconnect, they are likely to be shifted from one location to another or even taken outside the organization for theft of information.
- Pen drives can be very conveniently transported from one place to another, as a result of which data theft may occur. Even hard disks can be ported easily these days.
- PC is basically a single user oriented machine and hence, does not provide inherent data safeguards. Problems can be caused by computer viruses and pirated software, namely, data corruption, slow operations and system break down etc.
- Segregation of duty is not possible, owing to limited number of staff.
- Due to vast number of installations, the staff mobility is higher and hence becomes a source of leakage of information.
- The operating staff may not be adequately trained.
- Weak access control: Most of the log-on procedures become active at the booting of the computer from the hard drive.

The Security Measures that could be exercised to overcome these aforementioned risks are given as follows:

- Physically locking the system;

- Proper logging of equipment shifting must be done;
 - Centralized purchase of hardware and software;
 - Standards set for developing, testing and documenting;
 - Uses of antimalware software; and
 - The use of personal computer and their peripheral must have controls.
 - Use of disc locks that prevent unauthorized access to floppy disk or pen drive of a computer.
- (b) The key management practices complying with COBIT 5 for assessing and evaluating the system of IT internal controls in an enterprise are given as follows:
- **Monitor Internal Controls:** Continuously monitor, benchmark and improve the IT control environment and control framework to meet organizational objectives.
 - **Review Business Process Controls Effectiveness:** Review the operation of controls, including a review of monitoring and test evidence to ensure that controls within business processes operate effectively. It also includes activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing of controls, continuous controls monitoring, independent assessments, command and control centers, and network operations centers.
 - **Perform Control Self-assessments:** Encourage management and process owners to take positive ownership of control improvement through a continuing program of self- assessment to evaluate the completeness and effectiveness of management's control over processes, policies and contracts.
 - **Identify and Report Control Deficiencies:** Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.
 - **Ensure that assurance providers are independent and qualified:** Ensure that the entities performing assurance are independent from the function, groups or organizations in scope. The entities performing assurance should demonstrate an appropriate attitude and appearance, competence in the skills and knowledge necessary to perform assurance, and adherence to codes of ethics and professional standards.
 - **Plan Assurance Initiatives:** Plan assurance initiatives based on enterprise objectives and conformance objectives, assurance objectives and strategic priorities, inherent risk resource constraints, and sufficient knowledge of the enterprise.

- **Scope assurance initiatives:** Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.
 - **Execute assurance initiatives:** Execute the planned assurance initiative. Report on identified findings. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control system residual risks.
- (c) **Detective Controls:** These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. An example of a detective control would be a use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend. The main characteristics of such controls are given as follows:
- Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc.;
 - An established mechanism to refer the reported unlawful activities to the appropriate person or group;
 - Interaction with the preventive control to prevent such acts from occurring; and
 - Surprise checks by supervisor.

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

5. (a) Enablers are factors that, individually and collectively, influence whether something will work; in this case, governance and management over enterprise IT. Enablers are driven by the goals cascade, i.e., higher-level IT related goals defining 'what the different enablers should achieve'. The COBIT 5 framework describes seven categories of enablers, which are discussed as follows:
- **Principles, Policies and Frameworks** are the vehicle to translate the desired behaviour into practical guidance for day-to-day management.
 - **Processes** describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
 - **Organizational structures** are the key decision-making entities in an enterprise.
 - **Culture, Ethics and Behaviour** of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.

- **Information** is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
 - **Services, Infrastructure and Applications** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
 - **People, Skills and Competencies** are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.
- (b) Components of ERP model are as follows:
- ERP model is consists of four components which are implemented through a methodology. All four components 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 mindset:** By implementing ERP system, the old ways for working which user understand and comfortable with have to be changed and may lead to users' resistance. For example, some users may say that they have spent many years doing an excellence job without help from ERP system. In order to lead ERP implementation to succeed, the company needs to eliminate negative value or belief that users may carry toward utilizing new system.
 - (iv) **Change Management:** In ERP implementation, change needs to be managed at several levels - User attitude; resistance to change; and Business process changes.
- (c) Some of the advantages of continuous audit techniques are given as under:
- **Timely, Comprehensive and Detailed Auditing** – Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analyzed rather than examining the inputs and the outputs only.
 - **Surprise test capability** – As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.

- **Information to system staff on meeting of objectives** - Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
 - **Training for new users** – Using the ITFs, new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.
6. (a) Some of the major ways of protecting the installation against fire damage are as follows:
- Both automatic and manual fire alarms may be placed at strategic locations and a control panel may be installed to clearly indicate this.
 - Besides the control panel, master switches may be installed for power and automatic fire suppression system. Different fire suppression techniques like Dry-pipe sprinkling systems, water based systems, halon etc., depending upon the situation may be used.
 - Manual fire extinguishers can be placed at strategic locations.
 - Fireproof Walls; Floors and Ceilings surrounding the Computer Room and Fire Resistant Office Materials such as wastebaskets, curtains, desks, and cabinets should be used.
 - Fire exits should be clearly marked. When a fire alarm is activated, a signal may be sent automatically to permanently manned station.
 - All staff members should know how to use the system. The procedures to be followed during an emergency should be properly documented are Fire Alarms, Extinguishers, Sprinklers, Instructions / Fire Brigade Nos., Smoke detectors, and Carbon dioxide based fire extinguishers.
 - Less Wood and plastic should be in computer rooms.
 - Use a gas based fire suppression system;
 - To reduce the risk of firing, the location of the computer room should be strategically planned and should not be located in the basement or ground floor of a multi-storey building.
 - Regular Inspection by Fire Department should be conducted.
 - Fire repression systems should be supplemented and not replaced by smoke detectors.
 - **Documented and Tested Emergency Evacuation Plans:** Relocation plans should emphasize human safety, but should not leave information processing facilities physically unsecured. Procedures should exist for a controlled shutdown of the computer in an emergency situation. In all circumstances saving human life should be given paramount importance.

- **Smoke Detectors:** Smoke detectors are positioned at places above and below the ceiling tiles. Upon activation, these detectors should produce an audible alarm and must be linked to a monitored station (for example, a fire station).
 - **Wiring Placed in Electrical Panels and Conduit:** Electrical fires are always a risk. To reduce the risk of such a fire occurring and spreading, wiring should be placed in the fire-resistant panels and conduit. This conduit generally lies under the fire-resistant raised floor in the computer room.
- (b) **Characteristics of an effective MIS:** Major characteristic of an effective MIS are given as follows:
- **Management Oriented** – It means that efforts for the development of the information system should start from an appraisal of management needs and overall business objectives. Such a system is not necessarily for top management only but may also meet the information requirements of middle level or operating levels of management as well.
 - **Management Directed** – Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts. For system's effectiveness, it is necessary for management to devote their sufficient time not only at the stage of designing the system but for its review as well to ensure that the implemented system meets the specifications of the designed system.
 - **Integrated** – The best approach for developing information systems is the integrated approach as all the functional and operational information sub-systems are tied together into one entity. An integrated Information system has the capability of generating more meaningful information to management as it takes a comprehensive view or a complete look at the interlocking sub-systems that operate within a company.
 - **Common Data Flows** – It means the use of common input, processing and output procedures and media whenever required. Data is captured by the system analysts only once and as close to its original source as possible. Afterwards, they try to utilize a minimum of data processing procedures and sub-systems to process the data and strive to minimize the number of output documents and reports produced by the system. This eliminates duplication in data collections, simplifies operations and produces an efficient information system.
 - **Heavy Planning Element** – An MIS usually takes one to three years and sometimes even longer period to get established firmly within a company. Therefore, a MIS designer must be present in MIS development and should consider future enterprise objectives and requirements of information as per the organization structure of the enterprise as per requirements.
 - **Sub System Concept** – Even though the information system is viewed as a single entity, it must be broken down into digestible sub-systems, which can be implemented one at a time by developing a phased plan. The breaking down of

MIS into meaningful sub-systems sets the stage for this phasing plan.

- **Common Database** – Database is the mortar that holds the functional systems together. It is defined as a "super-file", which consolidates and integrates data records formerly stored in many separate data files. The organization of a database allows it to be accessed by several information sub-systems and thus, eliminates the necessity of duplication in data storage, updating, deletion and protection.
- **Computerized** - Though MIS can be implemented without using a computer; the use of computers increases the effectiveness of the system. In fact, its use equips the system to handle a wide variety of applications by providing their information requirements quickly. Other necessary attributes of the computer to MIS are accuracy and consistency in processing data and reduction in clerical staff. These attributes make computer a prime requirement in management information system.

(c) Major Data Integrity policies are given as under:

- **Virus-Signature Updating:** Virus signatures must be updated automatically when they are made available from the vendor through enabling of automatic updates.
- **Software Testing:** All software must be tested in a suitable test environment before installation on production systems.
- **Division of Environments:** The division of environments into Development, Test, and Production is required for critical systems.
- **Offsite Backup Storage:** Backups older than one month must be sent offsite for permanent storage.
- **Quarter-End and Year-End Backups:** Quarter-end and year-end backups must be done separately from the normal schedule, for accounting purposes
- **Disaster Recovery:** A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

7. (a) The key governance practices required to implement GEIT in enterprises are highlighted here:

- **Evaluate the Governance System:** Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and make judgment on the current and future design of governance of enterprise IT;
- **Direct the Governance System:** Inform leadership and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of IT in line with agreed governance design principles, decision-making models and authority levels. Define the information required for informed decision making; and

- **Monitor the Governance System:** Monitor the effectiveness and performance of the enterprise's governance of IT. Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of IT.
- (b) A good security policy should clearly state the following:
- Purpose and Scope of the Document and the intended audience;
 - The Security Infrastructure;
 - Security policy document maintenance and compliance requirements;
 - Incident response mechanism and incident reporting;
 - Security organization Structure;
 - Inventory and Classification of assets;
 - Description of technologies and computing structure;
 - Physical and Environmental Security;
 - Identity Management and access control;
 - IT Operations management;
 - IT Communications;
 - System Development and Maintenance Controls;
 - Business Continuity Planning;
 - Legal Compliances; and
 - Monitoring and Auditing Requirements.
- (c) **[Section 3] Authentication of Electronic Records**
- (1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.
 - (2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation -

For the purposes of this sub-section, "Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

- (a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

- (b) that two electronic records can produce the same hash result using the algorithm.
- (3) Any person by the use of a public key of the subscriber can verify the electronic record.
- (4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.
- (d) 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.
- (e) **Strengths of Waterfall Model:** The fundamental strength of the waterfall model has made it quite popular and handy among the fraternity. Major strengths are given as follows:
 - It is ideal for supporting less experienced project teams and project managers or project teams, whose composition fluctuates.
 - The orderly sequence of development steps and design reviews help to ensure the quality, reliability, adequacy and maintainability of the developed software.
 - Progress of system development is measurable.
 - It enables to conserve resources.