6. Auditing of Information Systems

6.1 Controls and Audit

- A Control is a system that prevents, detects or corrects unlawful events. Various controls are adapted as per requirement and accordingly, their audit become necessary.

6.1.1 Need for Audit of Information Systems

- Factors influencing an organization toward controls and audit of computers and the impact of the information systems audit function on organizations are as follows –

  - **Organisational Costs of Data Loss –**
    - Data is a critical resource of an organisation for its present and future process and its ability to adapt and survive in a changing environment.
  - **Cost of Incorrect Decision Making –**
    - High level decisions taken by managers require accurate data to make quality decision rules.
  - **Costs of Computer Abuse –**
    - Unauthorised access to computer systems, malwares, unauthorised physical access to computer facilities & unauthorised copies of sensitive data can lead to destruction of assets.
  - **Value of Computer Hardware, Software and Personnel –**
    - These are critical resources of an organisation, which has a credible impact on its infrastructure and business competitiveness.
  - **High Costs of Computer Error –**
    - In computerised environment, a data error during entry/ process would cause great damage.
  - **Maintenance of Privacy –**
    - Today, data collected in a business process contains private information about an individual too but now, there is a fear that privacy has eroded beyond acceptable levels.
  - **Controlled evolution of computer Use –**
    - Use of Technology and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.
  - **Information Systems Auditing –**
    - It is the process of attesting objectives (those of the external auditor) that focus on asset safeguarding and data integrity, and management objectives (those of the internal auditor) that include effectiveness and efficiency both.
    - This enables organizations to better achieve four major objectives that are as follows:

      i). Asset Safeguarding Objectives –

      - The information system assets (hardware, software, data information etc.) must be protected by a system of internal controls from unauthorised access.

ii). Data Integrity Objectives –

- It is a fundamental attribute of IS Auditing. It is also important from the business perspective of the decision maker, competition and the market environment.

iii). System Effectiveness Objectives –

- Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet business and user requirements.

iv). System Efficiency Objectives –

- To optimize the use of various information system resources (machine time, peripheral, system software and labour) along with the impact on its computing environment.

6.1.2 Effect of Computers on Audit

- To cope up with the new technology usage in an enterprise, the auditor should be competent to provide independent evaluation as to whether the business process activities are recorded and reported according to established standards or criteria.
- Two basic functions carried out to examine these changes are:

  i). Changes to Evidence Collection; and

  ii). Changes to Evidence Evaluation.

1) Changes to Evidence Collection –

- Without an audit trail, the auditor may have extreme difficulty in gathering sufficient and appropriate audit evidence to validate the figures in the client's accounts.
- The performance of evidence collection and understanding the reliability of controls involves issues like-

i). Data retention and storage –

- A client's storage capabilities may restrict the amount of historical data that can be retained "on-line" and readily accessible to the auditor.
- If the client has insufficient data retention capacities, the auditor may not be able to review a whole reporting period transactions on the computer system.

ii). Absence of input documents –

- Transaction data may be entered into the computer directly without the presence of supporting documentation e.g. input of telephone orders into a telesales system.

iii). Non-availability of audit trail –

- The absence of an audit trail will make the auditor's job very difficult and may call for an audit approach which involves seeking other sources of evidence to provide assurance that the computer input has been correctly processed and output.

iv). Lack of availability of printed output –

- The results of transaction processing may not produce a hard copy form of output, i.e. a printed record.

v). Audit evidence –

- Certain transactions may be generated automatically by the computer system. For example, a fixed asset system may automatically calculate depreciation on assets.

vi). Legal issues –

- The use of EDI and electronic trading over the Internet can create problems with contract, e.g. when is contract made, where is it made, what are terms and the parties to contract.

2) Changes to Evidence Evaluation –

- Evaluation of audit trail and evidence is to trace consequences of control's strength and weakness throughout the system.

i). System generated transactions –

- Financial systems may have the ability to initiate, approve & record financial transactions.

ii). Automated transaction processing systems –

- It can cause the auditor problems. Automated transaction generation systems are frequently used in 'just in time' inventory and stock control systems : When a stock level falls below a certain number, the system automatically generates a purchase order and sends it to the supplier.

iii). Systemic Error –

- Computers are designed to carry out processing on a consistent basis. Given the same inputs and programming, they invariably produce the same output.
- This consistency can be viewed in both a positive and a negative manner.

6.1.3 Responsibility for Controls

- Management is responsible for establishing and maintaining control to achieve the objectives of effective and efficient operations, and reliable information systems.
- Management should consistently apply the internal control to meet each of the internal control objectives and to assess internal control effectiveness.
- The number of management levels depends on the company size and organisation structure, but generally there are three such levels senior, middle and supervisory.
- Senior management is responsible for strategic planning and objectives, thus setting the course in the lines of business that the company will pursue.
- Middle management develops the tactical plans, activities and functions that accomplish the strategic objectives.
- Supervisory management oversees and controls the daily activities and functions of tactical plan.

6.2 The IS Audit

- The IS Audit of an Information System environment may include one or both of the following:
  - ✦ Assessment of internal controls within the IS environment to assure validity, reliability, and security of information and information systems.
  - ✦ Assessment of the efficiency and effectiveness of the IS environment.

- The IS audit process is to evaluate the adequacy of internal controls with regard to both specific computer program and the data processing environment as a whole.

6.2.1 Skill set of IS Auditor

- The set of skills that is generally expected to be with an IS auditor include:
  - ✦ Sound knowledge of business operations, practices and compliance requirements;
  - ✦ Should possess the requisite professional technical qualification and certifications;
  - ✦ A good understanding of information Risks and Controls;
  - ✦ Knowledge of IT strategies, policy and procedural controls;
  - ✦ Ability to understand technical and manual controls relating to business continuity; and
  - ✦ Good knowledge of Professional Standards and Best Practices of IT controls and security.

6.2.2 Functions of IS Auditor

- IS Auditor often is the assessor of business risk, as it relates to the use of IT, to management.
- The auditor can check the technicalities well enough to understand the risk and make a sound assessment and present risk-oriented advice to management.
- IS Auditors review risks relating to IT systems and processes; some of them are:
  - ✦ Inadequate information security controls (e.g. missing or out of date antivirus controls, open ports, open systems without password or weak passwords etc.)
  - ✦ Inefficient use of resources, or poor governance (e.g. huge spending on unnecessary IT projects like printing resources, storage devices, high power servers and workstations etc.)
  - ✦ Ineffective IT strategies, policies and practices (including a lack of policy for use of Information and Communication Technology (ICT) resources, Internet usage policies, Security practices etc.)
  - ✦ IT-related frauds (including phishing, hacking etc)

6.2.3 Categories of Information Systems Audits

- Information Systems Audits has been categorized into five types:

i). Systems and Application –

- An audit to verify that systems and applications are appropriate, efficient and adequately controlled to ensure valid, reliable, timely and secure input, processing, and output.

ii). Information Processing Facilities –

- An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.

iii). Systems Development –

- An audit to verify that the systems under development meet the objectives of organization and are developed in accordance with generally accepted standard for system development.

iv). Management of IT and Enterprise Architecture –

- An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.

v). Telecommunications, Intranets, and Extranets –

- An audit to verify that controls are in place on the client (end point device), server, and on the network connecting the clients and servers.

6.2.4 Steps in Information System Audit

- Different audit organizations go about IS auditing in different ways and individual auditors have their own favourite ways of working.
- However, it can be categorized into six stages as follows –

i). **Scoping and pre-audit survey –**

- Auditors determine the main areas 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 –**

- Gathering 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 or PEST techniques can be used for analysis.

v). **Reporting –**

- Reporting to the management is done after analysis of evidence 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.

6.2.5 Audit Standards and Best Practices

- IS auditors need guidance and a yardstick to measure the 3Es' (Economy, Efficiency and Effectiveness) of a system.
- The objective is to determine on how to achieve implementation of the IS auditing standards, use professional judgement in its application and be prepared to justify any conflict.
- The auditor needs guidance on how:
  - Information System should be assessed to plan their audits effectively and efficiently?
  - To focus their effort on high-risk areas and;
  - To assess the severity of any errors or weaknesses found during the IS audit process.

- Several well-known organizations have given practical and useful information on IS Audit, which are given as follows:

i). ISACA (Information Systems Audit and Control Association) –

- ISACA is a global leader in information governance, control, security and audit. ISACA developed the following to assist IS auditor while carrying out an IS audit.
  - **IS auditing standards:** ISACA issued 16 auditing standards, which defines the mandatory requirements for IS auditing and reporting.
  - **IS auditing guidelines:** ISACA issued 39 auditing guidelines, which provide a guideline in applying IS auditing standards.
  - **IS auditing procedures:** ISACA issued 11 IS auditing procedures, which provide examples of procedure an IS auditor need to follow while conducting IS audit for complying with IS auditing standards.
  - **COBIT (Control objectives for information and related technology):** This is a framework containing good business practices relating to information technology.

ii). ISO 27001 –

- ISO 27001 is the international best practice and certification standard for an Information Security Management System (ISMS).
- An ISMS is a systematic approach to manage Information security in an IS environment It encompasses people and, processes.
- ISO 27001 defines how to organise information security in any kind of organization, profit or non-profit, private or state-owned, small or large.
- It also enables an organization to get certified, i.e. an independent certification body has confirmed that information security has been implemented in the organisation. Many Indian IT companies have taken this certification, including INFOSYS, TCS, WIPRO.

iii). Internal Audit Standards –

- IIA (The Institute of Internal Auditors) is an international professional association.
- This association provides dynamic leadership for the global profession of internal auditing. IIA issued Global Technology Audit Guide (GTAG).
- GTAG provides management of organisation about information technology management, control, and security and IS auditors with guidance on various information technology associated risks and recommended practices.

iv). Standards on Internal Audit issued by ICAI –

- The standards issued by The Institute of Chartered Accountants of India (ICAI) highlight the process to be adopted by internal auditor in specific situation.

v). ITIL –

- The Information Technology Infrastructure Library (ITIL) is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. ITIL is published in a series of five core publications, each of which covers an ITSM lifecycle stage.

- ITIL describes procedures, tasks and checklists that are not organization-specific, used by an organization for establishing a minimum level of competency.

6.3 Performing IS Audit

- An IS Auditor uses the equivalent concepts of materiality (in financial audits) and significance (in performance audits) to plan both effective and efficient audit procedures.
- The underlying principle is that the auditor is not required to spend resources on items, those would not affect the judgment or conduct of a reasonable user of the audit report.
- Various steps are given as follows:

1) Basic Plan

- ✦ Planning is one of the primary and important phases in an Information System Audit, which ensures that the audit is performed in an effective manner.
- ✦ Hence, for the audit efforts to be successful, a good audit plan is a critical success factor. The objective of audit planning is to optimize the use of audit resources. Adequate planning of the audit work helps to ensure that appropriate attention is devoted to important areas of audit.
- ✦ Planning also assists in proper assignment of work to assistants and in coordination of the work done by other auditors and experts.
- ✦ Important points are given as follows:
  - The extent of planning will vary according to the size of the entity, the complexity of the audit and the auditor's experience with the entity and knowledge of the business.
  - Obtaining knowledge of the business is an important part of planning the work. It assists in the identification of events, transactions and practices which may have a material effect on the financial statements.
  - The auditor may discuss elements of the overall audit plan and certain audit procedures with the entity's audit committee, the management and staff to improve the effectiveness and efficiency of the audit and to coordinate audit procedures with the entity's personnel. The overall audit plan and the audit program; however, remains the auditor's responsibility.
  - The auditor should develop and document an overall audit plan describing the expected scope and conduct of the audit.
  - The audit should be guided by an overall audit plan and underlying audit program and methodology. Audit planning is a continuous activity which goes on throughout entire audit cycle. So, an auditor is expected to modify the audit plan as warranted by circumstances.
  - The documentation of the audit plan is also a critical requirement. All changes to the audit plan should follow a change management procedure. Every change should be recorded with reason for change.

2) Preliminary Review

- ✦ The preliminary review of audit environment enables the auditor to gain understanding of the business, technology and control environment and also gain clarity on the objectives of the audit and scope of audit.

- The following are some of the critical factors, which should be considered by an IS auditor as part of preliminary review.

i). Knowledge of the Business –

Related aspects are given as follows:

- General economic factors and industry conditions affecting the entity's business,
- Nature of Business, its products & services,
- General exposure to business,
- Its clientele, vendors and most importantly, strategic business partners/associates to whom critical processes have been outsourced,
- Level of competence of the Top management and IT Management, and
- Finally, Set up and organization of IT department.

ii). Understanding the Technology –

A good understanding of the technology environment and related control issues could include consideration of the following:

- Analysis of business processes and level of automation,
- Assessing the extent of dependence of the enterprise on Information Technology,
- Understanding technology architecture which could be quite diverse such as a distributed architecture or a centralized architecture or a hybrid architecture,
- Studying network diagrams to understand physical and logical network connectivity,
- Understanding extended enterprise architecture wherein the organization systems connect seamlessly with other stakeholders such as vendors (SCM), customers (CRM), employees (ERM) and the government,
- Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor.
- Finally, Studying Information Technology policies, standards, guidelines and procedures.

iii). Understanding Internal Control Systems –

For gaining understanding of Internal Controls emphasis to be placed on compliance and substantive testing.

iv). Legal Considerations and Audit Standards –

Related points are given as follows:

- The auditor should carefully evaluate the legal as well as statutory implications on his/her audit work.
- The Information Systems audit work could be required as part of a statutory requirement in which case he should take into consideration the related stipulations, regulations and guidelines for conduct of his audit.
- The statutes or regulatory framework may impose stipulations as regards minimum set of control objectives to be achieved by the subject organization.

- The IS Auditor should also consider the Audit Standards applicable to his conduct and performance of audit work. Non-compliance with the mandatory audit standards would result in the violation of the code of professional ethics.

v). Risk Assessment and Materiality –

- Risk Assessment implies the process of identifying the risk, assessing the risk, and recommending controls to reduce the risk to an acceptable level, considering both the probability and the impact of occurrence.
- Risk assessment allows the auditor to determine the scope of the audit and assess the level of audit risk and error risk.
- Additionally, risk assessment will aid in planning decisions such as:
  - The nature, extent, and timing of audit procedures.
  - The areas or business functions to be audited.
  - The amount of time and resources to be allocated to an audit

❖ The steps followed for a risk-based approach to make an audit plan are given as follows:

i). Inventory the information systems in use in the organization and categorize them.

ii). Determine which of the systems impact critical functions or assets, such as money, materials, customers, decision making, and how close to real time they operate.

iii). Assess what risks affect these systems and the severity of the impact on the business.

iv). Based on the above assessment, decide the audit priority, resource, schedule and frequency.

❖ At this stage, the auditor needs to:

- Assess the expected inherent, control and detection risk and identify significant audit areas.
- Set materiality levels for audit purposes.
- Assess the possibility of potential vulnerabilities, including experience of past periods or fraud.

❖ Risks are categorized as follows:

i). Inherent Risk –

- ✦ Inherent risk is the susceptibility of information resources or resources controlled by the information system to material theft, destruction, disclosure, unauthorized modification, or other impairment, assuming that there are no related internal controls.
- ✦ Inherent risk is the measure of auditor's assessment that there may or may not be material vulnerabilities or gaps in the audit subject exposing it to high risk before considering the effectiveness of internal controls.
- ✦ If the auditor concludes that there is a high likelihood of risk exposure, ignoring internal controls, the auditor would conclude that the inherent risk is high.
- ✦ Internal controls are ignored in setting inherent risk because they are considered separately in the audit risk model as control risk.

ii). Control Risk –

- ✦ Control risk is the risk that could occur in an audit area, and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system.
- ✦ Control risk is a measure of the auditor's assessment of the likelihood that risk exceeding a tolerable level and will not be prevented or detected by the client's internal control system.
- ✦ This assessment includes an assessment of whether a client's internal controls are effective for preventing or detecting gaps and the auditor's intention to make that assessment at a level below the maximum (100 percent) as a part of the audit plan.

iii). Detection Risk –

- ✦ Detection risk is the risk that the IT auditor's substantive procedures will not detect an error which could be material, individually or in combination with other errors.
- ✦ For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high because logs for the whole period of the audit are not available at the time of the audit.
- ✦ The detection risk associated with lack of identification of disaster recovery plans is ordinarily low since existence is easily verified.

6.4 IS Audit and Audit Evidence

- According to SA-230, Audit Documentation refers to the record of audit procedures performed, relevant audit evidence obtained, and conclusions the auditor reached. The objects of an auditor's working papers are to record and demonstrate the audit work from one year to another.
- Evidences are also necessary for the following purposes:
  - Means of controlling current audit work;
  - Evidence of audit work performed;
  - Schedules supporting or additional item in the accounts; and
  - Information about the business being audited, including the recent history.

6.5.1 Inherent Limitations of Audit

- To be able to prepare proper report, auditor needs documented evidences. The problem of documents not available in physical form.
- Following is list of actions that auditor needs to take to address the problems:
  - ✦ Use of special audit techniques, referred to as Computer Assisted Audit Techniques, for documenting evidences.
  - ✦ Audit timing can be so planned that auditor is able to validate transactions as they occur in system.
- Auditor shall form his/her opinion based on above processes.

- As per (SA 200) “Overall Objectives of An Independent Auditor and Conduct of An Audit in Accordance With Standards of Auditing”, any opinion formed by the auditor is subject to inherent limitations of an audit, which include:
  - ✦ The nature of financial reporting;
  - ✦ The nature of audit procedures;
  - ✦ The need for the audit to be conducted within a reasonable period of time and cost.
  - ✦ The matter of difficulty, time, or cost involved is not in itself a valid basis for the auditor to omit an audit procedure for which there is no alternative or to be satisfied with audit evidence that is less than persuasive.
  - ✦ Fraud, particularly fraud involving senior management or collusion.
  - ✦ The existence and completeness of related party relationships and transactions.
  - ✦ The occurrence of non-compliance with laws and regulations.
  - ✦ Future events or conditions that may cause an entity to cease to continue as a going concern.

6.4.2 Provisions relating to Digital Evidences

- As per Indian Evidence Act, 1872, “Evidence” means and includes:

  i). All statements, which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called oral evidence;

  ii). All documents produced for the inspection of the Court, such documents are called documentary evidence.

- Documentary Evidence also includes ‘Electronic Records’. The Information Technology Act, 2000 provides the legal recognition of electronic records and electronic signature.

6.4.3 Concurrent or Continuous Audit

- Real-time recordings need real-time auditing to provide continuous assurance about the quality of the data that is continuous auditing.
- Continuous auditing enables auditors to significantly reduce and perhaps to eliminate the time between occurrence of the client's events and the auditor's assurance services thereon.
- Continuous auditing enables auditors to shift their focus from the traditional "transaction" audit to the "system and operations" audit.
- Continuous auditing techniques use two bases for collecting audit evidence.
  - – One is use of embedded module in the system to collect, process and print audit evidence and
  - – the other is special audit records used to store the audit evidence collected.
- **Advantages of Continuous Auditing –**

  Continuous auditing has a number of potential benefits including:
  - ✦ Reducing the cost of the basic audit assignment by enabling auditors to test a larger sample (up to 100 percent) of client's transactions and examine data faster and more efficiently than the manual testing required when auditing around the computer;

- ✦ Reducing the amount of time and costs auditors traditionally spend on manual examination of transactions;
- ✦ Increasing the quality of audits by allowing auditors to focus more on understanding a client's business and industry and its internal control structure; and
- ✦ Specifying transaction selection criteria to choose transactions and perform both tests of controls and substantive tests throughout the year on an ongoing basis.

- **Some of the advantages of continuous audit techniques are given as under:**

i). 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 & outputs only.

ii). 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. This brings in the surprise test advantages.

iii). 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.

iv). 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.

- **The following are some of the disadvantages of the use of the continuous audit system:**

- ✦ Auditors should be able to obtain resources required from the organization to support development, implementation, operation, and maintenance of continuous audit techniques.
- ✦ Continuous audit techniques are more likely to be used if auditors are involved in the development work associated with a new application system.
- ✦ Auditors need the knowledge and experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.
- ✦ Continuous auditing techniques are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.
- ✦ Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.

- **Types of Audit Tools:**

i). Snapshots –

- ✦ Tracing a transaction is a computerized system can be performed with the help of snapshots or extended records.
- ✦ The snapshot software is built into the system at those points where material processing occurs which takes images of the flow of any transaction as it moves through the application.

- These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction.
- The main areas to dwell upon while involving such a system are to locate the snapshot points based on materiality of transactions when the snapshot will be captured and the reporting system design and implementation to present data in a meaningful way.

ii). Integrated Test Facility (ITF) –

- 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.
  - 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.
  - 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 application system to be tested. However, preparation of test data could be time consuming & 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 effect of transactions are not really removed.

iii). System Control Audit Review File (SCARF) –

- The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of system's transactions. The information collected is written onto a special audit file - the SCARF master files. Auditors examine the information contained on this file to see if some aspect of the application system needs follow-up.
- In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities.

- Auditors might use SCARF to collect the following types of information:
  - **Application System Errors** –
    - SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.
  - **Policy and Procedural Variances** –
    - SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.
  - **System Exception** –
    - SCARF can be used to monitor different types of application system exceptions. For example, salespersons might be given some leeway in prices they charge to customers.
  - **Statistical Sample** –
    - SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.
  - **Snapshots and Extended Records** –
    - Snapshots & extended record can be written into SCARF file and printed when required.
  - **Profiling Data** –
    - Auditor can use embedded audit routines to collect data to build profile of system user. Deviations from these profiles indicate that there may be some errors or irregularities.
  - **Performance Measurement** –
    - Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.

iv). Continuous and Intermittent Simulation (CIS) –

- This is a variation of the SCARF continuous audit technique. This technique can be used to trap exceptions whenever the application system uses a database management system.
- During application system processing, CIS executes in the following way:
  - The database management system reads an application system transaction. It is passed to CIS. CIS then determines whether it wants to examine the transaction further. If yes, the next steps are performed or otherwise it waits to receive further data from the database management system.
  - CIS replicates or simulates the application system processing.
  - Every update to the database that arises from processing the selected transaction will be checked by CIS to determine whether discrepancies exist between the results it produces and those the application system produces.
  - Exceptions identified by CIS are written to a exception log file.
  - The advantage of CIS is that it does not require modifications to the application system and yet provides an online auditing capability.

v). Audit Hooks –

- ✦ There are audit routines that flag suspicious transactions. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach of real-time notification displays a message on the auditor's terminal.
- ✦ For example, internal auditors at Insurance Company determined that their policyholder system was vulnerable to fraud every time a policyholder changed his or her name or address and then subsequently withdrew funds from the policy. They devised a system of audit hooks to tag records with a name or address change. The internal audit department will investigate these tagged records for detecting fraud.

6.4.4 Audit Trail

- Audit trails 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.
- **Audit Trail Objectives –**

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

  i). **Detecting Unauthorized Access –**
  - The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls.
  - A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by a virus or worm.
  - 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.

  ii). **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.

  iii). **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.

- **Implementing an Audit Trail –**
  - ✦ The information contained in audit logs is useful to accountants in measuring the potential damage and financial loss associated with application error, abuse of authority or unauthorized access by outside intruders.
  - ✦ Logs also provide valuable evidence or assessing both the adequacies of controls in place and the need for additional controls. Audit logs can generate data in overwhelming detail.

6.5 Audit and Evaluation Techniques for Physical and Environmental Controls

- We shall concentrate majorly on the controls of Physical, Logical, and environmental Controls. Auditing of these controls is discussed as follows:

6.5.1 Role of IS Auditor in Physical Access Controls

- Auditing physical access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls.
- This involves the following:

i). Risk Assessment –

- The auditor must satisfy him/herself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures there from.

ii). Controls Assessment –

- The auditor based on the risk profile evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks.

iii). Review of Documents –

- It requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams.

6.5.2 Audit of Environmental Controls

Related aspects are given as follows:

- **Role of Auditor in Environmental Controls –**
  - ✦ Audit of environmental controls should form a critical part of every IS audit plan.
  - ✦ The IS auditor should satisfy not only the effectiveness of various technical controls but also the overall controls safeguarding the business against environmental risks.
  - ✦ Some of the critical audit considerations that an IS auditor should take into account while conducting his/her audit is given below:

i). Audit Planning and Assessment –

As part of risk assessment:

- ✦ The risk profile should include different kinds of environmental risks that the organization is exposed to. These should comprise both natural and man-made threats. The profile should be periodically reviewed to ensure updation with newer risks that may arise.

- The controls assessment must ascertain that controls safeguard the organization against all acceptable risks including probable ones are in place.
- The security policy of the organization should be reviewed to assess policies and procedures that safeguard the organization against environmental risks.
- Building plans and wiring plans need to be reviewed to determine the appropriateness of location of IPF, review of surroundings, power and cable wiring etc.
- The IS auditor should interview relevant personnel to satisfy himself about employees' awareness of environmental threats and controls.
- Administrative procedures such as preventive maintenance plans and their implementation, incident reporting and handling procedures, inspection and testing plan and procedures need to be reviewed.

ii). Audit of Environmental Controls –

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 extinguisher, firefighting equipment and refilling date of 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.
- Environmental control equipment such as air-conditioning, dehumidifier, heater, ionizers;
- Compliant & maintenance log to assess if MTBF and MTTR are within acceptable level and
- Identify undesired activities such as smoking, consumption of eatables etc.

iii). Documentation –

- As part of the audit procedures, the IS auditor should also document all findings.
- The working papers could include audit assessments, audit plans, audit procedures, questionnaires, interview sheets, inspection charts etc.

6.6 Application Controls and their Audit Trails

An overview of the Application Controls and their categories are as follows –

S.No	Controls	Scope
1	Boundary Controls	Establishes interface between the user of the system and the system itself. The system must ensure that it has an authentic user. Users allowed using resources in restricted ways.
2	Input Controls	Responsible for bringing both the data and instructions in to the information system. Input Controls are validation and error detection of data input into the system.
3	Communication Controls	Responsible for controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attack, internetworking controls, communication architecture controls, audit trail controls, and existence controls.
4	Processing Controls	Responsible for computing, sorting, classifying and summarizing data. It maintains the chronology of events from the time data is received from input or communication systems to the time data is stored into the database or output as results.
5	Output Controls	To provide functions that determine data content available to users, data format, timeliness of data and how data is prepared and routed to users.
6	Database Controls	Responsible to provide functions to define, create, modify, delete and read data in an information system. It maintains procedural data-set of rules to perform operations on the data to help a manager to take decisions.

6.6.1 Audit Trail Controls

- Two types of audit trails that should exist in each subsystem.
  i). An **Accounting Audit Trail** to maintain a record of events within the subsystem; and
  ii). An **Operations Audit Trail** to maintain a record of the resource consumption associated with each event in the subsystem.

6.6.2 Boundary Controls

- This maintains the chronology of events that occur when a user attempts to gain access to and employ systems resources.
  - ✦ Identity of the would-be user of the system;
  - ✦ Authentication information supplied;
  - ✦ Resources requested;
  - ✦ Action privileges requested;
  - ✦ Terminal Identifier;
  - ✦ Start and Finish Time;
  - ✦ Number of Sign-on attempts;
  - ✦ Resources provided/denied; and

Accounting Audit Trail

- Action privileges allowed/denied.

Operations Audit Trail

- Resource usage from log-on to log-out time.
- Log of Resource consumption.

6.6.3 Input Controls

- This maintains the chronology of events from the time data and instructions are captured and entered into an application system until the time they are deemed valid and passed onto other subsystems within the application system.
- **Accounting Audit Trail**
  - The identity of the person(organization) who was the source of the data;
  - The identity of the person(organization) who entered the data into the system;
  - The time and date when the data was captured;
  - The identifier of the physical device used to enter the data into the system;
  - The account or record to be updated by the transaction;
  - The standing data to be updated by the transaction;
  - The details of the transaction; and
  - The number of the physical or logical batch to which the transaction belongs.
- **Operations Audit Trail**
  - Time to key in a source document or an instrument at a terminal;
  - Number of read errors made by an optical scanning device;
  - Number of keying errors identified during verification;
  - Frequency with which an instruction in a command language is used; and
  - Time taken to invoke an instruction using a light pen versus a mouse.

6.6.4 Communication Controls

- This maintains a chronology of the events from the time a sender dispatches a message to the time a receiver obtains the message.
- **Accounting Audit Trail**
  - Unique identifier of the source/sink node;
  - Unique identifier of each node in the network that traverses the message; Unique identifier of the person or process authorizing dispatch of the message; Time and date at which the message was dispatched;
  - Time and date at which the message was received by the sink node;

- Time and date at which node in the network was traversed by the message; and
- Message sequence number; and the image of the message received at each node traversed in the network.

- **Operations Audit Trail**
  - Number of messages that have traversed each link and each node;
  - Queue lengths at each node; Number of errors occurring on each link or at each node; Number of retransmissions that have occurred across each link; Log of errors to identify locations and patterns of errors;
  - Log of system restarts; and
  - Message transit times between nodes and at nodes.

6.6.5 Processing Controls

- The audit trail maintains the chronology of events from the time data is received from the input or communication subsystem to the time data is dispatched to the database, communication, or output subsystems.
- **Accounting Audit Trail**
  - To trace and replicate the processing performed on a data item.
  - Triggered transactions to monitor input data entry, intermediate results and output data values.
- **Operations Audit Trail**
  - A comprehensive log on hardware consumption – CPU time used, secondary storage space used, and communication facilities used.
  - A comprehensive log on software consumption – compilers used, subroutine libraries used, file management facilities used, and communication software used.

6.6.5 Database Controls

- The audit trail maintains the chronology of events that occur either to the database definition or the database itself.
- **Accounting Audit Trail**
  - To attach a unique time stamp to all transactions,
  - To attach beforeimages and afterimages of the data item on which a transaction is applied to the audit trail; and
  - Any modifications or corrections to audit trail transactions accommodating the changes that occur within an application system.
- **Operations Audit Trail**
  - To maintain a chronology of resource consumption events that affects the database definition or the database.

6.6.6 Output Controls

- The audit trail maintains the chronology of events that occur from the time the content of the output is determined until the time users complete their disposal of output because it no longer should be retained.
- **Accounting Audit Trail**
  - ✦ What output was presented to users;
  - ✦ Who received the output;
  - ✦ When the output was received; and
  - ✦ What actions were taken with the output?
- **Operations Audit Trail**
  - ✦ To maintain the record of resources consumed – graphs, images, report pages, printing time and display rate to produce the various outputs.

6.7Audit of Application Security Controls

- The objective of audit of application security control is to establish whether application security control are operating effectively to protect confidentiality, integrity & availability of information.

6.7.1 Approach to Application Security Audit

- ✦ Application security audit is being looked from the usage perspective. A layered approach is used based on the functions and approach of each layer.
- ✦ Layered approach is based on the activities being undertaken at various levels of management. The approach is in line with management structure which follows top-down approach.
- ✦ For this, auditors need to have a clear understanding of the following:
  - Business process for which the application has been designed;
  - The source of data input to and output from the application;
  - The various interfaces of the application under audit with other applications;
  - The various methods that may be used to login to application, other than normal used id and passwords that are being used, including the design used for such controls;
  - The roles, descriptions, user profiles and groups that can be created in an application; and
  - The policy of the organization for user access and supporting standards.

6.7.2 Understanding the Layers and Related Audit Issues

In this section, various aspects relating to each aforementioned layer have been discussed.

1) **Operational Layer –**
   - The Operational Layer is the basic layer, where user access decision are generally put in place.

- The operational layer audit issues include:

i). User Accounts and Access Rights –

- ✦ This includes defining unique user account and providing them access rights appropriate to their roles and responsibilities.
- ✦ Auditor needs to always ensure the use of unique user IDs, and these need to be traceable to individual for whom created. In case, guest IDs are used then test of same should also be there. Vendor accounts and third-party accounts should be reviewed.

ii). Password Controls –

- ✦ In general, password strength, password minimum length, password age, password non-repetition and automated lockout after three attempts should be set as a minimum.
- ✦ Auditor needs to check whether there are application where password control are weak.

iii). Segregation of Duties –

- ✦ Segregation of duties is a basic internal control that prevents or detects errors and irregularities by assigning to separate individual responsibility for initiating and recording transactions and custody of assets to separate individuals.
- ✦ Example to illustrate:
  - Record keeper of asset must not be asset keeper.
  - Cashier who creates a cash voucher, must not have right to authorize payments.
  - Maker must not be checker.
- ✦ Auditor needs to check that there is no violation of above principle. Any violation may have serious repercussions.

2) Tactical Layer –

- Tactical Layer is the management layer, which includes supporting functions such as security administration, IT risk management and patch management.
- At the tactical layer, security administration is put in place and includes:
  - ✦ Timely updates to user profiles, like creating/deleting and changing of user accounts. Auditor needs to check that any change to user rights is a formal process including approval from manager of the employee.
  - ✦ **IT Risk Management –**
    - This function is another important function performed, it includes following activities:
      - Assessing risk over key application controls;
      - Conducting a regular security awareness programme on application user;
      - Enabling application users to perform a self-assessment/complete compliance checklist questionnaire to gauge the users' understanding about application security;

- Reviewing application patches before deployment and regularly monitoring critical application logs;
- Monitoring peripheral security in terms of updating antivirus software;

- An auditor should understand risk associated with each application and obtain a report on periodic risk assessment on the application or self-assessment reports on application.

✦ **Interface Security –**

- This relates to application interfaced with another application in an organization. An auditor needs to understand that data flow to and from the application.

✦ **Audit Logging and Monitoring –**

- Regular monitoring the audit logs is required. The same is not possible for all transactions, so must be done on an exception reporting basis.

3) Strategic Layer –

- Strategic layer is the layer used by the Top Management.
- It includes the overall information security governance, security awareness, supporting information security policies & standard, and overarching an application security perspective.
- At this layer, the top management takes action, in form of drawing up security policy, security training, security guideline and reporting.
- A comprehensive information security programme fully supported by top management and communicated well to organization is of vital importance to succeed in information security.
- The security policy should be supported and supplemented by detailed standards and guidelines.
- One of the key responsibilities of the IT risk management function is to promote ongoing security awareness to the organization's users.
- Auditor needs to check whether all these aforementioned guidelines have been properly framed and are they capable of achieving the business objectives sought from the application under audit.