CHAPTER-6
AUDITING OF INFORMATION SYSTEM

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.

6.2. 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. These are discussed as follows:

1) **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.

2) **Incorrect Decision Making:** Management and operational controls taken by managers involve detection, investigations and correction of the processes. These high level decisions require accurate data to make quality decision rules.

3) **Costs of Computer Abuse:** Unauthorised access to computer systems, malwares, unauthorised physical access to computer facilities and unauthorised copies of sensitive data can lead to destruction of assets (hardware, software, data, information etc.)

4) **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.

5) **High Costs of Computer Error:** In a computerised enterprise environment where many critical business processes are performed, a data error during entry or process would cause great damage.

6) **Maintenance of Privacy:** Today, data collected in a business process contains private information about an individual too. These data were also collected before computers but now, there is a fear that privacy has eroded beyond acceptable levels.

7) **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.

8) **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.

9) **Asset Safeguarding Objectives:** The information system assets (hardware, software, data information etc.) must be protected by a system of internal controls from unauthorised access.

10) **Data Integrity Objectives:** It is a fundamental attribute of IS Auditing. The importance to maintain integrity of data of an organisation requires all the time. It is also important from the business perspective of the decision maker, competition and the market environment.

11) **System Effectiveness Objectives:** Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet business and user requirements.

12) **System Efficiency Objectives:** To optimize the use of various information system resources (machine time, peripherals, system software and labour) along with the impact on its computing environment.

CHAPTER-6
AUDITING OF INFORMATION SYSTEM

6.3. 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:

1) **Changes to Evidence Collection:** Existence of an audit trail is a key financial audit requirement; since without an audit trail, the auditor may have extreme difficulty in gathering sufficient, 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:
   - **a) 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.
   - **b) 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. The increasing use of EDI will result in less paperwork being available for audit examination.
   - **c) Non availability of audit trail:** The audit trails in some computer systems may exist for only a short period of time. The absence of an audit trail will make the auditor's job very difficult and may call for an audit approach which involves auditing around the computer system by seeking other sources of evidence to provide assurance that the computer input has been correctly processed and output.
   - **d) Lack of availability of output:** The results of transaction processing may not produce a hard copy form of output, i.e. a printed record. In the absence of physical output it may be necessary for the auditor to directly access the electronic data retained on the client's computer. This is normally achieved by having the client provide a computer terminal and being granted "read" access to the required data files.
   - **e) Audit evidence:** Certain transactions may be generated automatically by the computer system. For example, a fixed asset system may automatically calculate depreciation on assets at the end of each calendar month. The depreciation charge may be automatically transferred (journalised) from the fixed assets register to the depreciation account and hence to the client's income and expenditure account.
   - **f) Legal issues:** The use of computers to carry out trading activities is also increasing. More organisations in both the public and private sector intend to make use of EDI and electronic trading over the Internet. This can create problems with contracts, e.g. when is the contract made, where is it made (legal jurisdiction), what are the terms of the contract and are the parties to the 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.
   - **a) System generated transactions:** Financial systems may have the ability to initiate, approve and record financial transactions.
   - **b) Automated transaction processing systems can cause the auditor problems**: Automated transaction generation systems are frequently used in 'just in time' (JIT) 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 (perhaps using EDI technology)
   - **c) 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.

CHAPTER-6
AUDITING OF INFORMATION SYSTEM

6.4. IS Audit

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.

The IS Audit of an Information System environment may include one or both of the following:

1) Assessment of internal controls within the IS environment to assure validity, reliability, and security of information and information systems.

2) 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.

6.5. Responsibility of IS Auditor

The audit objective and scope has a significant bearing on the skill and competence requirements of an IS auditor.

The set of skills that is generally expected to be with an IS auditor include:

1) Sound knowledge of business operations, practices and compliance requirements;

2) Should possess the requisite professional technical qualification and certifications;

3) A good understanding of information Risks and Controls;

4) Knowledge of IT strategies, policy and procedural controls;

5) Ability to understand technical and manual controls relating to business continuity; and

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

Therefore, the audit process begins by defining the scope and objectives to adapt the standards and benchmarks for developing information model for collecting and evaluating evidence to execute the audit.

6.6. 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 (not necessarily manage the technology) 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:

1) Inadequate information security controls (e.g. missing or out of date antivirus controls, open ports, open systems without password or weak passwords etc.)

2) 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.)

3) 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.)

4) IT-related frauds (including phishing, hacking etc)

6.7. Categories of IS Audits

IS Audits has been categorized into five types:

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

2) **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.

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

4) **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.

5) **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.

6.8. 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.

1) **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.

2) **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.

3) **Fieldwork:** Gathering evidence by interviewing staff and managers, reviewing documents, and observing processes etc.

4) **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.

5) **Reporting:** Reporting to the management is done after analysis of evidence gathered and analyzed

6) **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 handcrafted SQL queries.

6.9. 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.

1) **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.
   a) IS auditing standards: ISACA issued 16 auditing standards, which defines the mandatory requirements for IS auditing and reporting.

   b) IS auditing guidelines: ISACA issued 39 auditing guidelines, which provide a guideline in applying IS auditing standards.

   c) 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.

   d) COBIT (Control objectives for information and related technology): This is a framework containing good business practices relating to information technology. The details are given in Chapter 1 of the Study Material.

2) **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 is safe to say that this standard is the foundation of information security management. It also enables an organization to get certified, which means that an independent certification body has confirmed that information security has been implemented in the organisation as defined policies and procedures.

3) **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.

4) **Standards on Internal Audit issued by ICAI:** The Institute of Chartered Accountants of India (ICAI) has issued various standards. The standards issued by the ICAI highlight the process to be adopted by internal auditor in specific situation.

5) **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. In its current form (known as ITILv3 and ITIL 2011 edition), 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. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement.

6.10. 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. Materiality and significance are concepts the auditor uses to determine the planned nature, timing, and extent of audit procedures. Materiality and significance include both quantitative and qualitative factors in relation to the subject matter of the audit. Even though a system may process transactions that are quantitatively immaterial or insignificant, the system may contain sensitive information or provide an access path to other systems that contain information that is sensitive or otherwise material or significant.

Planning occurs throughout the audit as an iterative process. However, planning activities are concentrated in the planning phase, during which the objectives are to obtain an understanding of the entity and its operations, including its internal control, identify significant issues, assess risk, and design the nature, extent, and timing of audit procedures. To accomplish this, the methodology presented here is a guidance to help the auditor to perform IS Audit.

1) **Basic Plan:** Adequate planning of the audit work helps to ensure that appropriate attention is devoted to important areas of the audit, those potential problems are identified and that the work is completed expeditiously. 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:

   a) 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.

   b) Obtaining knowledge of the business is an important part of planning the work. The auditor's knowledge of the business assists in the identification of events, transactions and practices which may have a material effect on the financial statements.

c) The auditor may wish to 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 work of the entity's personnel. The overall audit plan and the audit program; however, remains the auditor's responsibility.

d) The auditor should develop and document an overall audit plan describing the expected scope and conduct of the audit.

e) The audit should be guided by an overall audit plan and underlying audit program and methodology.

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 his/her preliminary review.

3) Knowledge of the Business: Related aspects are given as follows:

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

4) Understanding the Technology: An important task for the auditor as a part of his preliminary evaluation is to gain a good understanding of the technology environment and related control issues. This could include consideration of the following:

a) Analysis of business processes and level of automation,
b) Assessing the extent of dependence of the enterprise on Information Technology to carry on its businesses i.e. Role of IT in the success and survival of business,
c) Understanding technology architecture which could be quite diverse such as a distributed architecture or a centralized architecture or a hybrid architecture.
d) Studying network diagrams to understand physical and logical network connectivity,
e) Understanding extended enterprise architecture wherein the organization systems connect seamlessly with other stakeholders such as vendors (SCM), customers (CRM), employees (ERM) and the government,
f) Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e:mail systems,
g) And finally, Studying Information Technology policies, standards, guidelines and procedures.

2) Understanding Internal Control Systems: For gaining understanding of Internal Controls emphasis to be placed on compliance and substantive testing.

3) **Legal Considerations and Audit Standards:** Related points are given as follows:
   a) The auditor should carefully evaluate the legal as well as statutory implications on his/her audit work.
   b) 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.
   c) The statutes or regulatory framework may impose stipulations as regards minimum set of control objectives to be achieved by the subject organization.
   d) The IS Auditor should also consider the Audit Standards applicable to his conduct and performance of audit work.

4) **Risk Assessment and Materiality:** It 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 (the risk of errors occurring in the area being audited). Additionally, risk assessment will aid in planning decisions such as:
   a) The nature, extent, and timing of audit procedures.
   b) The areas or business functions to be audited.
   c) The amount of time and resources to be allocated to an audit

5) Risks are categorized as follows:
   a) Inherent Risk: Inherent risk is the susceptibility (vulnerability) 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.

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

   c) 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.

6.11. IS 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:

1) Means of controlling current audit work;
2) Evidence of audit work performed;
3) Schedules supporting or additional item in the accounts; and
4) Information about the business being audited, including the recent history.

In IS environment, the critical issue is that evidences are not available in physical form, but are in electronic form.

CHAPTER-6
AUDITING OF INFORMATION SYSTEM

6.12 Limitation of Audit

IS Audit subject to inherent limitations of an audit, which include:

1) The nature of financial reporting;
2) The nature of audit procedures;
3) The need for the audit to be conducted within a reasonable period of time and at a reasonable cost.
4) Fraud, particularly fraud involving senior management or collusion.
5) The existence and completeness of related party relationships and transactions.
6) The occurrence of non:compliance with laws and regulations.
7) Future events or conditions that may cause an entity to cease to continue as a going concern.

6.12. Concurrent or Continuous Audit

Today, organizations produce information on a real time, online basis. 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. Errors in a computerized system are generated at high speeds and the cost to correct and rerun programs are high. If these errors can be detected and corrected at the point or closest to the point of their occurrence the impact thereof would be the least.

Continuous auditing techniques use two bases for collecting audit evidence. One is the use of embedded modules in the system to collect, process, and print audit evidence and the other is special audit records used to store the audit evidence collected.

6.13. Types of Audit Tools:

Different types of continuous audit techniques may be used. Some modules for obtaining data, audit trails and evidences may be built into the programs. Audit software is available, which could be used for selecting and testing data. Many audit tools are also available; some of them are described below:

1) **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 reside 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.

2) **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..

3) **System Control Audit Review File (SCARF):** The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written onto a special audit file: the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow:up. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities. Auditors might use SCARF to collect the following types of information:
   a) **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.

b) Policy and Procedural Variances: Organizations have to adhere to the policies, procedures and standards of the organization and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.

c) System Exception: SCARF can be used to monitor different types of application system exceptions. For example, salespersons might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.

d) Statistical Sample: Some embedded audit routines might be statistical sampling routines, SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.

e) Snapshots and Extended Records: Snapshots and extended records can be written into the SCARF file and printed when required.

f) Profiling Data: Auditors can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.

g) Performance Measurement: Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.

4) 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:

a) 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.
b) CIS replicates or simulates the application system processing.
c) Every update to the database that arises from processing the selected transaction will
d) be checked by CIS to determine whether discrepancies exist between the results it produces and those the application system produces.
e) Exceptions identified by CIS are written to a exception log file.
f) The advantage of CIS is that it does not require modifications to the application system and yet provides an online auditing capability.

5) Continuous auditing has a number of potential benefits including:

a) 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;

b) Reducing the amount of time and costs auditors traditionally spend on manual examination of transactions;

c) 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

d) Specifying transaction selection criteria to choose transactions and perform both tests of controls and substantive tests throughout the year on an ongoing basis.

6) **Advantages of continuous audit techniques are given as under:**
   a) **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.

   b) **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.

   c) **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.

   d) **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.

7) **The following are some of the disadvantages and limitations of the use of the continuous audit system:**
   a) Auditors should be able to obtain resources required from the organization to support development, implementation, operation, and maintenance of continuous audit techniques.

   b) Continuous audit techniques are more likely to be used if auditors are involved in the development work associated with a new application system.

   c) Auditors need the knowledge and experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.

   d) 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.

   e) Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.

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

6.5.1 Audit Trail

Audit trails are logs 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 sequential 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.

1) **Audit Trail Objectives:** Audit trails can be used to support security objectives in three ways:
   a) Detecting unauthorized access to the system,
   b) Facilitating the reconstruction of events, and
   c) Promoting personal accountability.

Each of these is described below:

a) **Detecting Unauthorized Access:** Detecting unauthorized access can occur in real time or after the fact. The primary objective of real time detection is to protect the system from outsiders who are attempting to breach system controls. A real time audit trail can also be used to report on changes in system performance that may indicate infestation (infiltration) 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.

b) **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. Audit trail analysis also plays an important role in accounting control. For example, by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.

c) **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.

2) **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 errors, 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.

6.14. General Controls

The section deals with audit of general and application controls. This highlights 'What are the key things an auditor needs to consider while evaluating the said controls?' Various general controls are given as follows:

1) Operating System Controls
2) Data Management Controls
3) Organizational Structure Controls
4) System Development Control.
5) System Maintenance Controls
6) Computer Centre Security Controls
7) Internet & Intranet Controls
8) Personal Computers Control.

These aforementioned General Controls are discussed in detail as under:

1) **Operating System Controls:** Operating system is the computer control program. It allows users and their applications to share and access common computer resources, such as processor, main memory, database and printers. Operating system performs the following major tasks:
   a) **Scheduling Jobs:** They can determine the sequence in which jobs are executed, using priorities established.

   b) **Managing Hardware and Software Resources:** They can first cause the user's application program to be executed by loading it into primary storage and then cause the various hardware units to perform as specified by the application.

   c) **Maintaining System Security:** They may require users to enter a password: a group of characters that identifies users as being authorized to have access to the system.

   d) **Enabling Multiple User Resource Sharing:** They can handle the scheduling and execution of the application programs for many users at the same time, a feature called multiprogramming.

e) **Maintaining Usage Records:** They can keep track of the amount of time used by each user for each system unit: the CPU, secondary storage, and input and output devices. Such information is usually maintained for the purpose of charging users' departments for their use of the organization's computing resources.

2) **Operating System Security:** Operating system security involves policy, procedure and controls that determine, 'who can access the operating system, 'which resources they can access', and 'what action they can take'. The following security components are found in secure operating system:

a) **Log-in Procedure:** A log-in procedure is the first line of defense against unauthorized access. When the user initiates the log-on process by entering user-id and password, the system compares the ID and password to a database of valid users. If the system finds a match, then log-on attempt is authorized. If password or user-id is entered incorrectly, then after a specified number of wrong attempts, the system should lock the user from the system.

b) **Access Token:** If the log on attempt is successful, the Operating System creates an access token that contains key information about the user including user-id, password, user group and privileges granted to the user. The information in the access token is used to approve all actions attempted by the user during the session.

c) **Access Control List:** This list contains information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compasses his or her user-id and privileges contained in the access token with those contained in the access control list. If there is a match, the user is granted access.

d) **Discretionary Access Control:** The system administrator usually determines; who is granted access to specific resources and maintains the access control list. However, in distributed systems, resources may be controlled by the end-user. Resource owners in this setting may be granted discretionary access control, which allows them to grant access privileges to other users.

3) **Remedy from destructive programs:** The following can be used as remedies from destructive programs like viruses, warms etc.:

a) Purchase software from reputed vendor;
b) Examine all software before implementation;
c) Establish educational program for user awareness;
d) Install all new application on a standalone computer and thoroughly test them;
e) Make back up copy of key file; and
f) Always use updated anti-virus software.

6.15. Data Management Controls

These Controls fall in two categories:

1) **Access Controls:** Access controls are designed to prevent unauthorized individual from viewing, retrieving, computing or destroying the entity's data. Controls are established in the following manner:

a) User Access Controls through passwords, tokens and biometric Controls; and
b) Data Encryption: Keeping the data in database in encrypted form.

2) **Back up Controls:** Backup controls ensure the availability of system in the event of data loss due to unauthorized access, equipment failure or physical disaster; the organization can retrieve its files and databases.

Backup refers to making copies of the data so that these additional copies may be used to restore the original data after a data loss. Various backup strategies are given as follows:

a) **Dual recording of data:** Under this strategy, two complete copies of the database are maintained. The databases are concurrently updated.

b) **Periodic dumping of data:** This strategy involves taking a periodic dump of all or part of the database. The database is saved at a point in time by copying it onto some backup storage medium, magnetic tape, removable disk, Optical disk. The dump may be scheduled.

c) **Logging input transactions:** This involves logging the input data transactions which cause changes to the database. Normally, this works in conjunction with a periodic dump. In case of complete database failure, the last dump is loaded and reprocessing of the transactions are carried out which were logged since the last dump.

d) **Logging changes to the data:** This involves copying a record each time it is changed by an update action. The changed record can be logged immediately before the update action changes the record, immediately after, or both.

3) **Organizational Structure Controls**

a) In manual environment, the task may be segregated in the following manner:
- **i)** Segregate the task of transaction authorization from transaction processing;
- **ii)** Segregate record keeping from asset custody; and
- **iii)** Divide transaction:processing tasks among individuals.

b) In a Computer Based Information System (CBIS), as transaction initiation is a critical activity. It requires segregation of duties at authorization, processing and recording all aspects of a transaction. Segregation is done at the following functional levels, to adhere the following principles of internal controls:
- **i)** Segregating the maker / creator from checker;
- **ii)** Segregating the asset record keeper from physical asset keeper; and
- **iii)** Regular checking of effectiveness of internal controls.

4) **System Development Controls**

System development controls are targeted to ensure that proper documentations and authorizations are available for each phase of the system development process. Are as follows:

a) **System Authorization Activities:** All systems must be properly authorized to ensure their economic justification and feasibility. As with any transaction, system's authorization should be formal. This requires that each new system request be submitted in written form by users to systems professionals who have both the expertise and authority to evaluate and approve (or reject) the request.

b) **User Specification Activities:** Users must be actively involved in the systems development process. Regardless of the technology involved, the user can create a detailed written description of the logical needs that must be satisfied by the system. The creation of a user specification document often involves the joint efforts of the user and systems professionals. It should describe the user's view of the problem, not that of the systems professionals.

c) **Technical Design Activities:** The technical design activities in the SDLC translate the user specifications into a set of detailed technical specifications of a system that meets the user's needs. The scope of these activities includes systems analysis, general systems design, feasibility analysis, and detailed systems design. The adequacy of these activities is measured by the quality of the documentation that emerges from each phase.

d) Internal Auditor's Participation: The internal auditor plays an important role in the control of systems development activities, particularly in organizations whose users lack technical expertise. The auditor should become involved at the inception of the SDLC process to make conceptual suggestions regarding system requirements and controls. Auditor's involvement should be continued throughout all phases of the development process and into the maintenance phase.

e) Program Testing: All program modules must be thoroughly tested before they are implemented. The results of the tests are then compared against predetermined results to identify programming and logic errors.

f) User Test and Acceptance Procedures: before implementation, the individual modules of the system must be tested as a combined whole. A test team comprising user personnel, systems professionals, and internal audit personnel subjects the system to rigorous testing. Once the test team is satisfied that the system meets its stated requirements, the system is formally accepted by the user department(s).

6.16. Computer Centre Security and Controls

These are of the following types:

1) Physical Security: The security required for computer system can be categorized as security from accidental breach and incidental breach. Accidental breach of security due to such natural calamities as fire, flood and earthquake etc. may cause total destruction of important data and information.

Physical security includes arrangements for:

a) fire detection and fire suppression systems,
b) security from water damage,
c) safeguards from power variation, and
d) pollution and unauthorized intrusion.

These are discussed as follows:

a) Fire Damage: It is a major threat to the physical security of a computer installation. Some of the major features of a well:designed fire protection system are given below:

i) Both automatic and manual fire alarms are placed at strategic locations.
ii) A control panel may be installed which shows where in the location an automatic or manual alarm has been triggered.
iii) Besides the control panel, master switches may be installed for power and automatic fire suppression system.
iv) Manual fire extinguishers can be placed at strategic locations.
v) Fire exits should be clearly marked. When a fire alarm is activated, a signal may be sent automatically to permanently manned station.
vi) 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.
vii) Less Wood and plastic should be in computer rooms.

b) Water Damage: Water damage to a computer installation can be the outcome of water pipes burst. Water damage may also result from other resources such as cyclones, tornadoes, floods etc. Some of the major ways of protecting the installation against water damage are as follows:

i) Wherever possible have waterproof ceilings, walls and floors;
ii) Ensure an adequate positive drainage system exists;
iii) Install alarms at strategic points within the installation;

iv) In flood areas have the installation above the upper floors but not at the top floor;
v) Use a gas based fire suppression system;
vi) Water proofing; and
vii) Water leakage Alarms.

c) Power Supply Variation: Voltage regulators and circuit breakers protect the hardware from temporary increase or decrease of power. UPS Battery back up can be provided in case a temporary loss of power occurs. A generator is needed for sustained losses in power for extended period.

d) Pollution Damage: The major pollutant in a computer installation is dust. Dust caught between the surfaces of magnetic tape / disk and the reading and writing heads may cause either permanent damage to data or read/ write errors. Due consideration should be given for dust free environment in the computer room. Regular cleaning of walls, floors and equipment etc. is essential. Only such materials and finishing may be used inside the room, which enables it to remain dust free. These are:
i) air conditions,
ii) dust protection, and
iii) regular cleaning.

e) Unauthorized Intrusion: Unauthorized intrusion takes two forms. First, the intruder by physically entering the room may steal assets or carry out sabotage. Alternatively, the intruder may eavesdrop on the installation by wire tapping, installing an electronic bug or using a receiver that picks up electro:magnetic signals. Physical entry may be restricted to the computer room by various means. A badge system may be used to identify the status of personnel inside the computer room. Various devices are available to detect the presence of bugs by the intruder; these are:
i) Physically or Electronically logging,
ii) Guard, dogs,
iii) Entry in computer area restricted,
iv) Log books,
v) Alarms,
vi) Preventing wire tapping,
vii) Physical Intrusion detectors.

f) Software & Data Security: In today's business world, trade is through networks & has spread over geographical area, so security is must. Following are some of the examples of requirements.
i) Authorization of persons to use data,
ii) Passwords & PINs,
iii) Monitoring after office hours activity,
iv) Segregation, check & control over critical information,
v) Frequent audits,
vi) Screening and background checks before recruitment,
vii) Encryption of data:: Viewing & recognition of data only by PINs & passwords
viii) Security software,
ix) Management checks,
x) Back up of data/information, and
xi) Antivirus software.

g) Data Communication Security: This is another important aspect to be covered. This can be implemented through the following controls:
i) Audit trails of crucial network activities,
ii) Sign on user identifier,
iii) Passwords to gain access,

iv) Terminal locks,
v) Sender & receiver authentications,
vi) Check over access from unauthorized terminals,
vii) Encryption of data / information,
viii) Proper network administration,
ix) Hardware & system software built in control,
x) Use of approved networks protocols,
xi) Network administrations, and
xii) Internally coded device identifier.

6.17. Internet and Intranet Controls

There are two major exposures in the communication sub-system including Internet and Intranet, which are given as follows:

1) **Component Failure:** The components in the communication sub-systems are given as follows:
   a) **Communication lines**: twisted pair, coaxial cables, fiber optics, microwave, satellite etc.
   b) **Hardware:** ports, modems, multiplexers, switches and concentrators etc.
   c) **Software**: Packet switching software, polling software, data compression software etc.
   d) **Due to component failure**, transmission between sender and receiver may be disrupted, destroyed or corrupted in the communication system.

2) **Subversive (Revolutionary) Threats**: An intruder attempts to violate the integrity of some components in the sub-system by:
   a) **Invasive (Aggressive) tap:** By installing it on communication line, may read /modify data.
   b) **Inductive tap:** It monitors electromagnetic transmissions and allows the data to be read only.

   Subversive attacks can provide intruders with important information about messages being transmitted and the intruder can manipulate these messages in many ways.

6.18. Mechanism can be used to control above risks

1) **Fire wall:** Organizations connected to the Internet and Intranet often implements an electronic firewall to insulate their network from intrude. A firewall is a system that enforces access control between two networks. To accomplish this, all traffic between the external network and the organization's Intranet must pass through the firewall. Only authorized traffic between the organization and the outside is allowed to pass through the firewall. The firewall must be immune to penetrate from both outside and inside the organization. In addition to insulating the organization's network from external networks, firewalls can be used to insulate portions of the organization's Intranet from internal access also.
2) **Controlling Denial of Service (DoS) Attacks:** When a user establishes a connection on the Internet through TCP/IP, a three way handshake takes place between SYN packets, SYN ACK packets and ACK packets. Computer hacker transmits hundreds of SYN packets to the receiver but never responds with an ACK to complete the connection. As a result, the ports of the receiver's server are clogged with incomplete communication requests and legitimate requests are prevented from access. This is known as connection flooding.
3) **Encryption:** Encryption is the conversion of data into a secret code for storage in databases and transmission over networks. The sender uses an encryption algorithm and the original message called the clear text is converted into cipher text. This is decrypted at the receiving end. The encryption algorithm uses a key. The more bits in the key, the stronger is the encryption algorithms. Two general approaches are used for encryption viz. private key and public key encryption.
4) **Recording of Transaction Log:** An intruder may penetrate the system by trying different passwords and user ID combinations. All incoming and outgoing requests along with attempted access should be recorded in a transaction log. The log should record the user ID, the time of the access and the terminal location from where the request has been originated.

5) **Call Back Devices:** It is based on the principle that the key to network security is to keep the intruder off the Intranet rather than imposing security measure after the criminal has connected to the intranet. The call back device requires the user to enter a password and then the system breaks the connection. If the caller is authorized, the call back device dials the caller's number to establish a new connection. This limits access only from authorized terminals or telephone numbers and prevents an intruder masquerading as a legitimate user. This also helps to avoid the call forwarding and man in the middle attack.

6.19. Personal Computers Controls

Related risks are given as follows:

1) Personal computers are small in size 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.

2) 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.

3) 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.

4) Segregation of duty is not possible, owing to limited number of staff.

5) Due to vast number of installations, the staff mobility is higher and hence becomes a source of leakage of information.

6) The operating staff may not be adequately trained.

7) Weak access control: Security software that provides log on procedures is available for PCs. Most of these programs, however, become active only when the computer is booted from the hard drive. Disc locks are devices that prevent unauthorized individuals from accessing the floppy disk or pen drive of a computer.

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

1) Physically locking the system;
2) Proper logging of equipment shifting must be done;
3) Centralized purchase of hardware and software;
4) Standards set for developing, testing and documenting;
5) Uses of antimalware software; and
6) The use of personal computer and their peripheral must be controls.

6.20. 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:

1) **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.

2) **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.

3) **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.

6.21. Audit of 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:

1) **Audit Planning and Assessment:** As part of risk assessment:
   - **a)** The risk profile should include the different kinds of environmental risks that the organization is exposed to. These should comprise both natural and manmade threats. The profile should be periodically reviewed to ensure updation with newer risks that may arise.
   - **b)** The controls assessment must ascertain that controls safeguard the organization against all acceptable risks including probable ones are in place.
   - **c)** The security policy of the organization should be reviewed to assess policies and procedures that safeguard the organization against environmental risks.
   - **d)** 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.
   - **e)** The IS auditor should interview relevant personnel to satisfy himself about employees' awareness of environmental threats and controls, role of the interviewee in environmental control procedures such as prohibited activities in IPF, incident handling, and evacuation procedures to determine if adequate incident reporting procedures exist.
   - **f)** 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.

2) **Audit of Environmental Controls:** Audit of environmental controls requires the IS auditor to conduct physical inspections and observe practices. The Auditor should verify:
   - **a)** The IPF and the construction with regard to the type of materials used for construction;
   - **b)** The presence of water and smoke detectors, power supply arrangements to such devices, and testing logs;
   - **c)** The location of fire extinguishers, firefighting equipment and refilling date of fire extinguishers;
   - **d)** Emergency procedures, evacuation plans and marking of fire exists. There should be half:yearly Fire drill to test the preparedness;
   - **e)** 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;
   - **f)** 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;
   - **g)** Environmental control equipment such as air:conditioning, dehumidifiers, heaters, ionizers etc;
   - **h)** Compliant logs and maintenance logs to assess if MTBF and MTTR are within acceptable levels; and
   - **i)** Identify undesired activities such as smoking, consumption of eatables etc.

3) **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.

Documentation of Auditing of Environmental Controls

Control Activities	Control Techniques	Audit Procedures
➢ **Safeguards against the risks of heating, ventilation and air: conditioning systems.**	➢ Identify systems that provide constant temperature and humidity levels within the organization.	➢ Review a heating, ventilation and air conditioning design to verify proper functioning within an organization.
➢ **Control of radio emissions affect on computer systems.**	➢ Evaluate electronic shielding to control radio emissions that affect the computer systems.	➢ Review any shielding strategies against interference or unauthorized access through emissions.
➢ **Establish adequate interior security based on risk**	➢ Critical systems have emergency power supplies for alarm systems; monitoring devices, exit lighting, communication systems.	➢ Verify critical systems (alarm systems, monitoring devices, and entry control systems) have emergency power supplies. ➢ Identify back up systems and procedures and determine the frequency of testing. Review test results.
➢ **Adequately protect against emerging threats, based on risk.**	➢ Appropriate plans and controls such as shelter in place or for a potential CBR attack(chemical, biological and radioactive attack) ➢ Restricting public access and protect critical entry points air intake vents, protective grills and roofs.	➢ Interview officials, review planning documents and related test results. ➢ Observe and document the controls in place to mitigate emerging threats. ➢ Observe location of these devices and identify security measures implemented. ➢ Verify the controls existence and
➢ **Adequate environmental controls have been implemented**	➢ Fire detection and suppression devices are installed and working.(smoke detectors, fire extinguishers and sprinkle systems) ➢ Controls are implemented to mitigate disasters, such as floods, earthquakes. ➢ Redundancy exists in critical systems like, uninterrupted power supply, air cooling system, and backup generators ➢ Humidity, temperature, and voltage control are maintained and acceptable levels ➢ Emergency lighting, power outages and evacuation routes are appropriately located	➢ Interview managers and scrutinize that operations staff are aware of the locations of fire alarms, extinguishers, emergency power off switches, air ventilation apparatus and other emergency devices. ➢ Determine that humidity, temperature and voltage are controlled within the accepted levels. ➢ Check cabling, plumbing, room ceiling smoke detectors, water detectors on the floor are installed and in working properly.

➢ **Staff have been trained to react to emergencies**	➢ Operational and support personnel are trained and understand emergency procedures. ➢ Emergency procedures are documented and periodically tested: incident plan, inspection plan and maintenance plan.	➢ Interview security personnel to ensure their awareness and responsibilities. ➢ Review training records and documentation. Determine the scope and adequacy of training. ➢ Review test policies, documentation and know- how of operational staff. ➢ Review incident handling procedures and maintenance and inspection plan.

6.22. Application Controls

These are categories in the following types:

1) Input Controls
2) Process Controls, and
3) Output Controls.

1) Input Controls

Input controls are divided into the following broad classes:

a) Source Document Control,
b) Data Coding Controls, and
c) Validation Controls.

The details of each aforementioned class are given as under:

a) Source Document Controls: In systems that use physical source documents to initiate transactions, careful control must be exercised over these instruments. Source document fraud can be used to remove assets from the organization. For example, an individual with access to purchase orders and receiving reports could fabricate a purchase transaction to a non-existent supplier. If these documents were entered into the data processing stream along with a fictitious vendor's invoice, the system could process these documents as if a legitimate transaction had taken place. In the absence of other compensating controls to detect this type of fraud, the system would create an account payable and subsequently write a cheque for payment.

To control against this type of exposure, the organization must implement control procedures over source documents to account for each document, as described below:

i) Use pre numbered source documents: Source documents should come pre numbered from the printer with a unique sequential number on each document. Source document numbers enable accurate accounting of document usage and provide an audit trail for tracing transactions through accounting records.

ii) Use source documents in sequence: Source documents should be distributed to the users and used in sequence. This requires the adequate physical security be maintained over the source document inventory at the user site. When not in use, documents should be kept under lock and key and access to source documents should be limited to authorized persons.

iii) Periodically audit source documents: Missing source documents should be identified by reconciling document sequence numbers. Periodically, the auditor should compare the numbers of documents used to date with those remaining in inventory plus those voided due to errors. Documents not accounted for should be reported to management.

b) Data Coding Controls: Two types of errors can corrupt a data code and cause processing errors. These are transcription and transposition errors, which are as discussed below:

i) Transcription Errors: These fall into three classes:

(1) **Addition errors** occur when an extra digit or character is added to the code. For example, inventory item number 83276 is recorded as 832766.

(2) **Truncation errors** occur when a digit or character is removed from the end of a code. In this type of error, the inventory item above would be recorded as 8327.

(3) **Substitution errors** are the replacement of one digit in a code with another. For example, code number 83276 is recorded as 83266.

ii) Transposition Errors: There are two types of transposition errors.

(1) **Single transposition** errors occur when two adjacent digits are reversed. For instance, 12345 is recorded as 21345.

(2) **Multiple transposition** errors occur when nonadjacent digits are transposed. For example, 12345 is recorded as 32154.

c) Validation Controls: Input validation controls are intended to detect errors in the transaction data before the data are processed. There are three levels of input validation controls:

i) Field Interrogation: It involves programmed procedures that examine the characters of the data in the field. The following are some common types of field interrogation. Various field checks used to ensure data integrity have been described below:

(1) Limit Check: This is a basic test for data processing accuracy and may be applied to both the input and output data. The field is checked by the program against predefined limits to ensure that no input/output error has occurred or at least no input error exceeding certain pre:established limits has occurred.

(2) Picture Checks: These check against entry into processing of invalid characters.

(3) Valid Code Checks: Checks are made against predetermined transactions codes, tables or order data to ensure that input data are valid. The predetermined codes or tables may either be embedded in the programs or stored in (direct access) files.

(4) Check Digit: One method for detecting data coding errors is a check digit. A check digit is a control digit (or digits) added to the code when it is originally assigned that allows the integrity of the code to be established during subsequent processing. The check digit can be located anywhere in the code, as a prefix, a suffix, or embedded someplace in the middle.

(5) Arithmetic Checks: Simple Arithmetic is performed in different ways to validate the result of other computations of the values of selected data fields.

(6) Cross Checks: may be employed to verify fields appearing in different files to see that the result tally.

ii) Record Interrogation: These are discussed as follows:

(1) Reasonableness Check: Whether the value specified in a field is reasonable for that particular field?

(2) Valid Sign: The contents of one field may determine which sign is valid for a numeric field.

(3) Sequence Check: If physical records follow a required order matching with logical records.

iii) File Interrogation: These are discussed as follows:

(1) Version Usage: Proper version of a file should be used for processing the data correctly. In this regard it should be ensured that only the most current file be processed.

(2) Internal and External Labeling: Labeling of storage media is important to ensure that the proper files are loaded for process. Where there is a manual process for loading files, external labeling is important to ensure that the correct file is being processed. Where there is an automated tape loader system, internal labeling is more important.

(3) Data File Security: Unauthorized access to data file should be prevented, to ensure its confidentiality, integrity and availability. These controls ensure that the correct file is used for processing.

(4) Before and after Image and Logging: The application may provide for reporting of before and after images of transactions. These images combined with the logging of events enable re-constructing the data file back to its last state of integrity, after which the application can ensure that the incremental transactions/events are rolled back or forward.

(5) File Updating and Maintenance Authorization: Sufficient controls should exist for file updating and maintenance to ensure that stored data are protected. The access restrictions may either be part of the application program or of the overall system access restrictions.

(6) Parity Check: When programs or data are transmitted, additional controls are needed. Transmission errors are controlled primarily by detecting errors or correcting codes.

6.23. Processing Controls

Various processing controls are given as follows:

1) **Run-to-run Totals:** These help in verifying data that is subject to process through different stages. If the current balance of an invoice ledger is ` 150,000 and the additional invoices for the period total ` 20,000 then the total sales value should be ` 170,000. A specific record probably the last record can be used to maintain the control total.

2) **Reasonableness Verification:** Two or more fields can be compared and cross verified to ensure their correctness. For example, the statutory percentage of provident fund can be calculated on the gross pay amount to verify if the provident fund contribution deducted is accurate.

3) **Edit Checks:** Edit checks similar to the data validation controls can also be used at the processing stage to verify accuracy and completeness of data.

4) **Field Initialization:** Data overflow can occur, if records are constantly added to a table or if fields are added to a record without initializing it, i.e. setting all values to zero/blank before inserting the field or record.

5) **Exception Reports:** Exception reports are generated to identify errors in the data processed. Such exception reports give the transaction code and why a particular transaction was not processed or what is the error in processing the transaction.

6.24. Output Controls Various Output Controls are given as follows:

1. **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.

2. **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.

3. **Spooling/queuing:** "Spool" is an acronym for "Simultaneous Peripherals Operations Online". This is a process used to ensure that the user is able to 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.

4. **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.

5. **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.

6. **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.

6.25. 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, namely supervisory, tactical and strategic. 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.

1) Business process for which the application has been designed;
2) The source of data input to and output from the application;
3) The various interfaces of the application under audit with other applications;
4) 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;
5) The roles, descriptions, user profiles and user groups that can be created in an application; and
6) The policy of the organization for user access and supporting standards.

There are various layers, discussed as follows:

1) **Operational Layer:** The operational layer audit issues include:
   a) **User Accounts and Access Rights:** This includes defining unique user accounts 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. Likewise, vendor accounts and third party accounts should be reviewed. In essence, users and applications should be uniquely identifiable.
   b) **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 applications where password controls are weak. In case such instances are found, then auditor may look for compensating controls against such issues.
   c) **Segregation of Duties:** Segregation of duties is a basic internal control that prevents or detects errors and irregularities by assigning to separate individuals' responsibility for initiating and recording transactions and custody of assets to separate individuals.
   Example to illustrate:
      i) Record keeper of asset must not be asset keeper
      ii) Cashier who creates a cash voucher in system, must not have right to authorize payments.
      iii) Maker must not be checker.
2) **Tactical Layer**: At the tactical layer, security administration is put in place. This includes:
   a) 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.
   b) IT Risk Management: This function is another important function performed, it includes the following activities:
      i) Assessing risk over key application controls;
      ii) Conducting a regular security awareness programme on application user;
      iii) Enabling application users to perform a self:assessment/complete compliance checklist questionnaire to gauge the users' understanding about application security;
      iv) Reviewing application patches before deployment and regularly monitoring critical application logs;
      v) Monitoring peripheral security in terms of updating antivirus software;
      vi) 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. Security of the interfaced data is also important, especially when unencrypted methods of transmission are used for data transmission.
      vii) 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:** 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 the organization is of paramount importance to succeed in information security. The security policy should be supported and supplemented by detailed standards and guidelines. These guidelines shall be used at the appropriate level of security at the application, database and operating system layers.