6

Auditing of Information Systems

Learning Objectives
• To understand Information Systems Audit, its need, methodology and related standards;
• To know about IS Audit planning, performing an IS audit and best practices;
• To discuss different types of IS audit and assurance engagements;
• To have an overview of continuous auditing;
• To review General Controls and Application Controls; and
• To understand review of controls at various levels/layers such as: Parameters, user creation, granting of access rights, input, processing and output controls.
Task Statements
• To apply appropriate audit technique/s in a specified audit situation; and
• To make proper documentation relating to IS Audit.
Knowledge Statements
• To know the importance of audit in an IS environment;
• To know the approaches to be adopted for an IS Audit; and
• To know various types of controls, related concepts and their audit.

6.1 Introduction

Information Systems have become an integral part of our day-to-day life. From morning till evening, all humans interact with systems, in one form or another. The increased usage of technology has its pitfalls. Organizations need to rely more on technology for their day-to-day jobs, e.g. management decision making and all business related activities. As the usage of technology and information system is increasing, associated risk with technology is also imposing several threats to the information systems.

More and more use of technology and the increased instances has made it imperative for organizations to place proper controls. Controls can be classified based on nature say, preventive, detective and corrective or based on some other parameters like physical, logical or environmental. More classifications are also possible like based on the asset they protect; the detail discussion has already been done in Chapter 3 of the study material. In the same

chapter, there is detailed discussion on the risk associated with non-implementation of controls or improper implementation.

It is also clear that compliance is an important audit procedure undertaken by auditor to evaluate the nature, timing and extent of other audit procedures. As a part of compliance, an auditor evaluates the existence effectiveness and continued effectiveness of internal controls. The chapter highlights the same audit procedures in terms of performing systems audit for an organization. System audit, in today's environment shall precede any financial audit. The chapter discusses the need and method of doing an Information System Audit (IS Audit). In addition, the chapter also discusses various standards for IS Audit and the methodology for conducting an IS Audit in detail.

6.2 Controls and Audit

As discussed earlier, 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. The details of controls have already been discussed in Chapter 3 of the Study Material.

6.2.1 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 depicted in the Fig. 6.2.1.

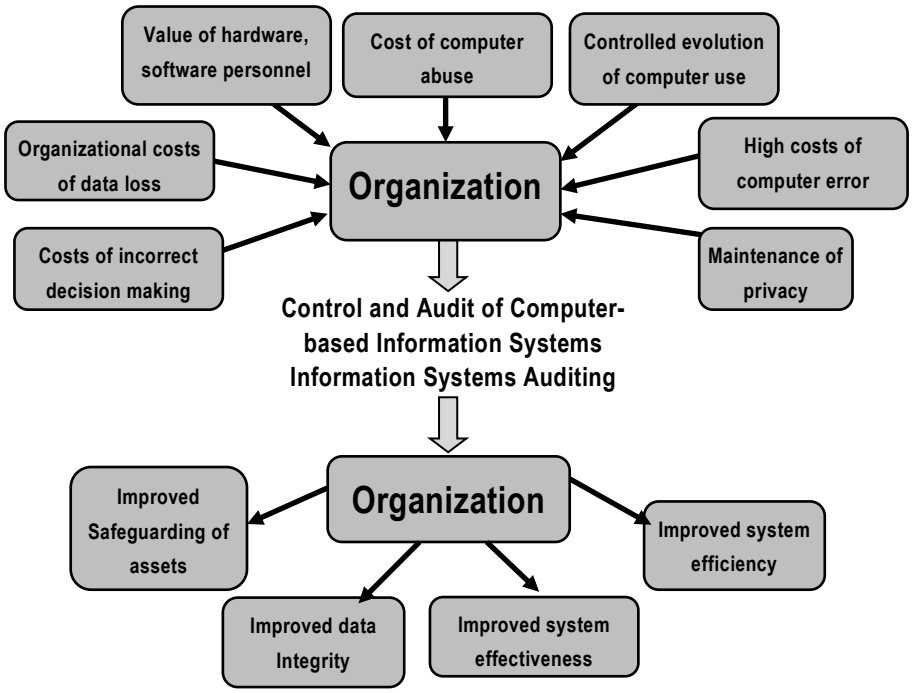

Fig. 6.2.1: Impact of Controls and Audit influencing an Organization

Let us now discuss these reasons in details:

- **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:** 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.
- **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.)
- **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 a computerised enterprise environment where many critical business processes are performed, a data error during entry or process would cause great damage.
- **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.
- **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, 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:

- **Asset Safeguarding Objectives:** The information system assets (hardware, software, data information etc.) must be protected by a system of internal controls from unauthorised access.
- **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.
- **System Effectiveness Objectives**: Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet business and user requirements.
- **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.

6.2.2 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:

- Changes to Evidence Collection; and
- Changes to Evidence Evaluation.

These are discussed as follows:

(i) 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-

- **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. For example, the client's computer system may save data on detachable storage device by summarising transactions into monthly, weekly or period end balances.
- **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 Electronic Data Interchange (EDI) will result in less paperwork being available for audit examination.
- **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.
- **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. In the absence of physical output, it may be necessary for an 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.
- **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.

- **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.

  The admissibility of the evidence provided by a client's computer system may need special consideration. The laws regarding the admissibility of computer evidence varies from one country to another. Within a country laws may even vary between one state and another. If the auditor intends to gather evidence for use in a court, s(he) should firstly find out what the local or national laws stipulate on the subject.

  In addition, the admissibility of evidence may vary from one court to another. What is applicable is a civil court may not be applicable in a criminal court.

(ii) Changes to Evidence Evaluation: Evaluation of audit trail and evidence is to trace consequences of control's strength and weakness throughout the system.

- **System generated transactions:** Financial systems may have the ability to initiate, approve and record financial transactions.
- **Automated transaction processing** systems can cause the auditor problems. For example when gaining assurance that a transaction was properly authorised or in accordance with delegated authorities. *Automated transaction generatio*n 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)
- **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.

If the computer is doing the right thing, then with all other things being equal, it will continue to do the right thing every time. Similarly, if the computer is doing the wrong thing and processing a type of transaction incorrectly, it will continue to handle the same type of transactions incorrectly every time. Therefore, whenever an auditor finds an error in a computer processed transaction, s(he) should be thorough in determining the underlying reason for the error. If the error is due to a systemic problem, the computer may have processed hundreds or thousands of similar transactions incorrectly

6.2.3 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 the tactical plan. The same is shown in Fig. 6.2.2.

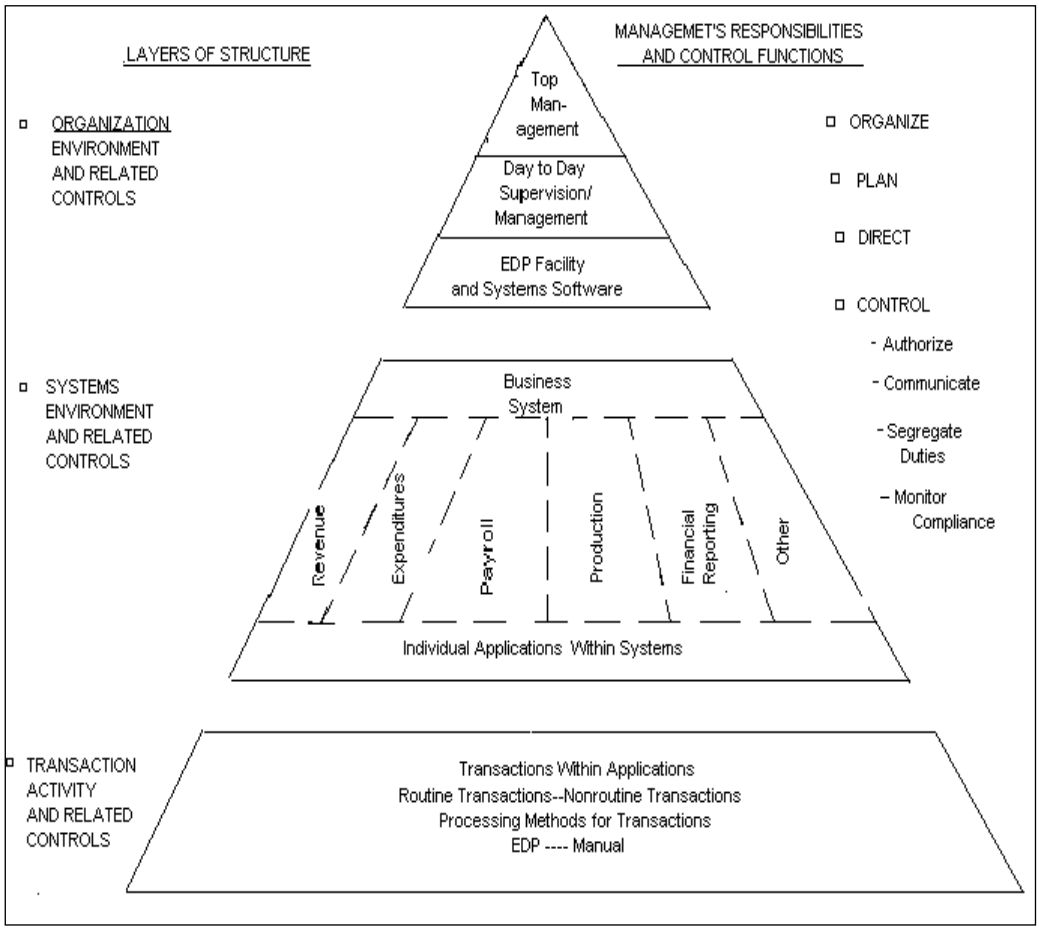

Fig. 6.2.2: Structure of the Control Environment

6.3 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.

6.3.1 Skill set 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:

- 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.

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.

6.3.2 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 (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:

- 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)

6.3.3 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, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.

(ii) **Information Processing Facilities:** 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 the organization and to ensure that the systems are developed in accordance with generally accepted standards for systems development.

(iv) **Management of IT and Enterprise Architecture:** 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.

6.3.4 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 shown in Fig. 6.3.1.

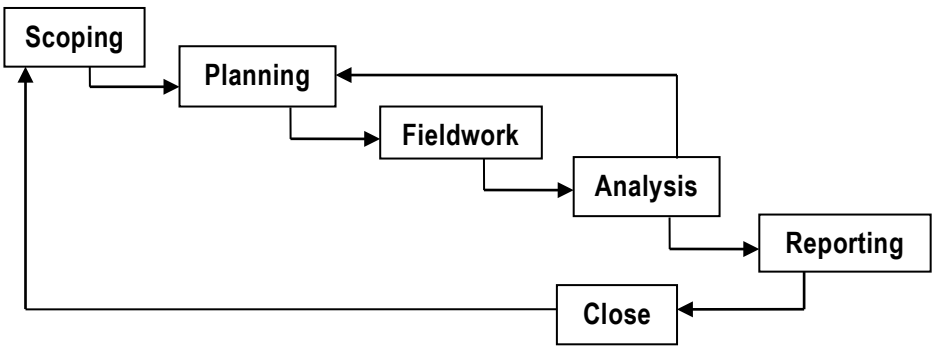

Fig. 6.3.1: Steps in IS Audit process

(i) **Scoping and pre-audit survey:** Auditors determine the main area/s of focus and any areas that are explicitly out-of-scope, based on the scope-definitions agreed with management. Information sources at this stage include background reading and web browsing, previous audit reports, pre audit interview, observations and, sometimes, subjective impressions that simply deserve further investigation.

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

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

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

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

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

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

Secondly, after accepting an engagement, the pre-audit survey is more important, as in this survey auditor has official access to client records and data. The purpose of this survey shall help auditor to assess the audit schedules, audit team size, and audit team components.

6.3.5 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.

The Institute of Chartered Accountants of India has issued various Standards on Auditing covering various aspects. Although these standards are primarily concerned with the audit of financial information; they can be adapted for the purposes of IS Audit depending on its scope and objectives. The details are available in the Auditing paper of CA Course Curriculum. In addition to these Standards, there are certain guidelines, which provide guidance in applying IS Auditing Standards. The IS auditor should consider them in determining how to achieve implementation of the standards, use professional judgment in their application and be prepared to justify any departure. 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. The details are given in Chapter 1 of the Study Material.

(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 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.

Many Indian IT companies have taken this certification, including INFOSYS, TCS, WIPRO. Companies getting themselves certified by as ISO 27001, are better competitor's to those not certified. Companies certified generate a greater client assurance. It removes the dependency from individuals and put reliance on processes. The details of this standard are given in chapter 7 of the Study Material.

(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 Institute of Chartered Accountants of India (ICAI) has issued various standards; the details are given in the Study Material of Auditing paper. The standards issued by the ICAI highlight the process to be adopted by internal auditor in specific situation.

(v) Information Technology Infrastructure Library (ITIL): The 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. The details are given in the Chapter 7 of the Study Material.

6.4 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. The underlying principle is that the auditor is not required to spend resources on items of little importance; that is, those that would not affect the judgment or

conduct of a reasonable user of the audit report, in light of surrounding circumstances. On the basis of this principle, the auditor may determine that some areas of the IS controls audit (e.g., specific systems) are not material or significant, and therefore warrant little or no audit attention.

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. For example, an application that provides public information via a website, if improperly configured, may expose internal network resources, including sensitive systems, to unauthorized access.

Planning occurs throughout the audit as an iterative process. (For example, based on findings from the testing phase, the auditor may change the planned audit approach, including the design of specific tests.) 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.

The auditor must address many considerations that cover the nature, timing, and extent of testing. The auditor must devise an auditing testing plan and a testing methodology to determine whether the previously identified controls are effective. The auditor also tests whether the end-user applications are producing valid and accurate information. For microcomputers, several manual and automated methods are available to test for erroneous data. An initial step is to browse the directories of the PCs in which the end-user-developed application resides. Any irregularities in files should be investigated. Depending on the nature of the audit, computer-assisted techniques could also be used to audit the application.

The auditor should also conduct several tests with both valid and invalid data to test the ability and extent of error detection, correction, and prevention within the application. In addition, the auditor should look for controls such as input balancing and record or hash totals to ensure that the end user reconciles any differences between input and output. The intensity and extent of the testing should be related to the sensitivity and importance of the application. The auditor should be cautious of too much testing and limit his/her tests to controls that cover all the key risk exposures and possible error types. The key audit concern is that the testing should reveal any type of exposure of sensitive data and that the information produced by the application is valid, intact, and correct. One should test the critical controls, processes, and apparent exposures. The auditor performs the necessary testing by using documentary evidence, corroborating interviews, and personal observation.

Secondly, we may test the critical controls, processes, and apparent exposures. The auditor performs the necessary testing by using documentary evidence, corroborating interviews, and personal observation. Validation of the information obtained is prescribed by the auditor's work program. Again, this work program is the organized, written, and pre-planned approach to the study of the IT department. It calls for validation in several ways, which are as follows:

- Asking different personnel the same question and comparing the answers;
- Asking the same question in different ways at different times;
- Comparing checklist answers to work papers, programs, documentation, tests, or other verifiable results;
- Comparing checklist answers to observations and actual system results; and
- Conducting mini-studies of critical phases of the operation.

Such an intensive program allows an auditor to become informed about the operation in a short time. Programs are run on the computer to test and authenticate application programs that are run in normal processing. The audit team selects one of the many Generalized Audit Software (GAS) packages such as Microsoft Access or Excel, IDEA, or ACL and determines what changes are necessary to run the software at the installation. The auditor is to use one of these software's to do sampling, data extraction, exception reporting, summarize and foot totals, and other tasks to perform in-depth analysis and reporting capability.

Various steps are given as follows:

6.4.1 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. Planning takes more significance in case of Information Systems Audit since the audit risks are significantly impacted by inherent risk. Hence, for the audit efforts to be successful, a good audit plan is a critical success factor. Planning develops the annual audit schedule to perform the individual audits. It includes budgets of time and costs, and state priorities according to organizational goals and policies. 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 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:

- 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. 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.
- 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.

- The auditor should develop and document an overall audit plan describing the expected scope and conduct of the audit. While the record of the overall audit plan will need to be sufficiently detailed to guide the development of the audit program, its precise form and content will vary depending on the size of the entity, the complexity of the audit and the specific methodology and technology used by the auditor.
- The audit should be guided by an overall audit plan and underlying audit program and methodology. Audit planning is often mistaken as a onetime activity to be taken and completed in the beginning of the audit. While for all practical purposes, planning is a continuous activity which goes on throughout the entire audit cycle. Many times changes in conditions or circumstances or unexpected findings during the course of audit require changes in the audit procedures and methodology initially planned. Hence, an auditor is expected to modify the audit plan as warranted by the 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.

6.4.2 Preliminary Review

The extent of audit effort is dictated by the degree of risk of assessment, which is critical to the effectiveness of the audit effort. Amongst the critical factors affecting the risk is the appropriate assessment of the control environment. 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.

(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: 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:

- Analysis of business processes and level of automation,
- 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,

- 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. For example, authentication risks relating to e-mail systems,
- And 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. Sometimes, this may also include restrictions on the use of certain types of technologies e.g. freeware, shareware etc.
- 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 not only impact on the violation of the code of professional ethics but also have an adverse impact on the auditor's work.

(v) Risk Assessment and Materiality: Risk Assessment is a critical and inherent part of the Information Systems Auditor's planning and audit implementation. 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:

- 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 that can be followed for a risk-based approach to make an audit plan are given as follows:

- Inventory the information systems in use in the organization and categorize them.
- 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.
- Assess what risks affect these systems and the severity of the impact on the business.
- Based on the above assessment, decide the audit priority, resources, schedule and frequency.

Risks that affect a system and taken into consideration at the time of assessment can be differentiated as inherent risks, control risks and detection risks. These factors directly impact upon the extent of audit risk which can be defined as the risk that the information/financial report may contain material error that may go undetected during the course of the audit. 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 the experience of past periods, or fraud.

Risks are categorized as follows:

- **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. For example, inherent risk would be high in case of auditing internet banking in comparison to branch banking or inherent risk would be high if the audit subject is an off-site. ATM in an example of the same.

  Internal controls are ignored in setting inherent risk because they are considered separately in the audit risk model as control risk. It is often an area of professional judgment on the part of an auditor.

- **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.

- **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.

6.5 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 (terms such as "working papers" or "work papers" are also sometimes used). 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.

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

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 has been highlighted at many places. 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. Elaborated under this part, later on.
- 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 at a reasonable 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.

6.5.2 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 through its various sections. The said Act also highlights Electronic Governance and accordingly, digital evidences are recognized legally. The details of related regulatory issues have been given in the Chapter 7 of the Study Material.

6.5.3 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.

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:

(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. Auditors can also embed audit software modules in the application system programs to recognize transactions having certain characteristics as ITF transactions. Tagging live transactions as ITF transactions has the advantages of ease of use and testing with transactions representative of normal system processing. However, use of live data could mean that the limiting conditions within the system are not tested and embedded modules may interfere with the production processing. The auditors may also use test data that is specially prepared. Test transactions would be entered along with the production input into the application system. In this approach the test data is likely to achieve more complete coverage of the execution paths in the application system to be tested than selected production data and the application system does not have to be modified to tag the ITF transactions and to treat them in a special way. However, preparation of the test data could be time consuming and costly.
- **Methods of Removing the Effects of ITF Transactions:** The presence of ITF transactions within an application system affects the output results obtained. The effects of these transactions have to be removed. The application system may be programmed to recognize ITF transactions and to ignore them in terms of any processing that might affect users. Another method would be the removal of effects of ITF transactions by submitting additional inputs that reverse the effects of the ITF transactions. Another less used approach is to submit trivial entries so that the effects of the ITF transactions on the output are minimal. The effects of the transactions are not really removed.

(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 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:

- **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** - 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.
- **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.
- **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.
- **Snapshots and Extended Records** - Snapshots and extended records can be written into the SCARF file and printed when required.
- **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.
- **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.

Advantages and Disadvantages of Continuous Auditing: Continuous auditing enables auditors to shift their focus from the traditional "transaction" audit to the "system and operations" audit. 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.

Audit evidence gathered by performing tests of controls can be used as a basis for reducing more costly substantive tests, analytical procedures, transactions analysis, access and data flow. With continuous auditing, auditors may conduct tests of controls simultaneously with substantive tests, analytical procedures, etc. to gather persuasive evidence regarding the quality and integrity of the client's electronic system in producing reliable and credible information. CATTs can be used in performing tests of transactions continuously throughout the year in order to reduce the extent of substantive tests to be performed at the end of a period.

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

- **Timely, Comprehensive and Detailed Auditing** – Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analyzed rather than examining the inputs and the outputs only.
- **Surprise test capability** – As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.
- **Information to system staff on meeting of objectives** - Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
- **Training for new users** – Using the ITFs, new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

The following are some of the disadvantages and limitations 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.

(v) 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.

6.5.4 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. Many operating systems allow management to select the level of auditing to be provided by the system. This determines 'which events will be recorded in the log'. An effective audit policy will capture all significant events without cluttering the log with trivial activity.

Audit trail controls attempt to ensure that a chronological record of all events that have occurred in a system is maintained. This record is needed to answer queries, fulfill statutory requirements, detect the consequences of error and allow system monitoring and tuning. The accounting audit trail shows the source and nature of data and processes that update the database. The operations audit trail maintains a record of attempted or actual resource consumption within a system.

Applications system Controls involve ensuring that individual application systems safeguard assets (reducing expected losses), maintain data integrity (ensuring complete, accurate and authorized data) and achieve objectives effectively and efficiently from the perspective of users of the system from within and outside the organization.

(i) Audit Trail Objectives: Audit trails can be used to support security objectives in three ways:

- Detecting unauthorized access to the system,
- Facilitating the reconstruction of events, and
- Promoting personal accountability.

Each of these is described below:

- **Detecting Unauthorized Access*:*** Detecting unauthorized access can occur in real time or after the fact. The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls. A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by a virus or worm. Depending upon how much activity is being logged and reviewed; real-time detection can impose a significant overhead on the operating system, which can degrade operational performance. After-the-fact detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.
- **Reconstructing Events*:*** Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors. Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future. Audit trail analysis also plays an important role in accounting control. For example, by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.
- **Personal Accountability*:*** Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behavior. Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log.

(ii) 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. Audit logs, however, can generate data in overwhelming detail. Important information can easily get lost among the superfluous detail of daily operation. Thus, poorly designed logs can actually be dysfunctional.

6.6 Audit and Evaluation Techniques for Physical and Environmental Controls

In this section we shall concentrate majorly on the controls of Physical, Logical, environmental Controls.

Auditing of these controls is discussed as follows:

6.6.1 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:

- **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.
- **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.
- **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.

6.6.2 Audit of Environmental Controls

Related aspects are given as follows:

(a) Role of Auditor in Environmental Controls: The attack on the World Trade Centre in 2001 has created a worldwide alert bringing focus on business continuity planning and 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:

(b) Audit Planning and Assessment: As part of risk assessment:

- The risk profile should include the 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, 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.
- 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.

(c) Audit of Environmental Controls: Audit of environmental controls requires the IS auditor to conduct physical inspections and observe practices. The Auditor should verify that:

- The IPF (Infrastructure Planning and Facilities) and the construction with regard to the type of materials used for construction;
- The presence of water and smoke detectors, power supply arrangements to such devices, and testing logs;
- The location of fire extinguishers, firefighting equipment and refilling date of fire extinguishers;
- Emergency procedures, evacuation plans and marking of fire exists. There should be half-yearly Fire drill to test the preparedness;
- Documents for compliance with legal and regulatory requirements with regards to fire safety equipment, external inspection certificate and shortcomings pointed out by other inspectors/auditors;
- Power sources and conduct tests to assure the quality of power, effectiveness of the power conditioning equipment, and generators. Also the power supply interruptions must be checked to test the effectiveness of the back-up power;
- Environmental control equipment such as air-conditioning, dehumidifiers, heaters, ionizers etc;
- Compliant logs and maintenance logs to assess if MTBF (Mean Time Between Failures) and MTTR (Mean Time To Repair) are within acceptable levels; and
- Identify undesired activities such as smoking, consumption of eatables etc.

(d) 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. The following Table 6.7.1 presents a brief idea about the same.

Table 6.7.1: 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 intrusion detection sensors.
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	• 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.

	generators • Humidity, temperature, and voltage control are maintained and acceptable levels • Emergency lighting, power outages and evacuation routes are appropriately located.	
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.

6.7 Managerial Controls and their Audit Trails

The overview of the Managerial Controls is provided below in Table 6.7.1 and has already been discussed in detail in Chapter - 3 of the Study Material.

Table 6.7.1: Types of Managerial Controls

Controls	Scope
Top Management and Information Systems Management Controls	Discusses the top management's role in planning, organizing, leading and controlling the information systems function. Also provides advice to top management in relation to long-run policy decision making and translates long-run policies into short-run goals and objectives.
System Development Management Controls	Provides a contingency perspective on models of the information systems development process that auditors can use as a basis for evidence collection and evaluation.

Programming Management Controls	Discusses the major phases in the program life cycle and the important controls that should be exercised in each phase.
Data Resource Management Controls	Discusses the role of database administrator and the controls that should be exercises in each phase.
Quality Assurance Management Controls	Discusses the major functions that quality assurance management should perform to ensure that the development, implementation, operation, and maintenance of information systems conform to quality standards.
Security Management Controls	Discusses the major functions performed by operations by security administrators to identify major threats to the IS functions and to design, implement, operate, and maintain controls that reduce expected losses from these threats to an acceptable level.
Operations Management Controls	Discusses the major functions performed by operations management to ensure the day-to-day operations of the IS function are well controlled.

The auditors play a vital role in evaluating the performance of various controls under managerial controls. Some of the key areas that auditors should pay attention to while evaluating Managerial controls and its types are provided below:

6.7.1 Top Management and Information Systems Management Controls

The major activities that senior management must perform are – Planning, Organizing, Controlling and Leading (already explained in Chapter – 3 of the Study Material). The Role of auditor at each activity is discussed below:

- **Planning:** Auditors need to evaluate whether top management has formulated a high-quality information system's plan that is appropriate to the needs of an organization or not. A poor-quality information system is ineffective and inefficient leading to losing of its competitive position within the marketplace.
- **Organizing:** Auditors should be concerned about how well top management acquires and manages staff resources for three reasons:
  - The effectiveness of the IS function depends primarily on the quality of its staff. The IS staff need to remain up to date and motivated in their jobs.
  - Intense competition and high turnover have made acquiring and retaining good information system staff a complex activity.
  - Empirical research indicates that the employees of an organization are the most likely persons to perpetrate irregularities.
- **Leading:** Generally, the auditors examine variables that often indicate when motivation problems exist or suggest poor leadership. For example - staff turnover statistics, frequent failure of projects to meet their budget and absenteeism level to evaluate the leading function. Auditors may use both formal and informal sources of evidence to evaluate how well top mangers' communicate with their staff. The formal sources include

IS plans, documents standards and policies whereas the informal sources of evidence include interviews with IS staff about their level of satisfaction with the top management. Auditors must try to assess both the short-run and long-run consequences of poor communications within the information systems function and to assess the implications for asset safeguarding, data integrity, system effectiveness, and system efficiency.

- **Controlling:** Auditors should focus on subset of the control activities that should be performed by top management – namely, those aimed at ensuring that the information systems function accomplishes its objectives at a global level. Auditors must evaluate whether top management's choice to the means of control over the users of IS services is likely to be effective or not.

6.7.2 System Development Management Controls

Three different types of audits may be conducted during system development process as discussed in the Table 6.7.2:

Table 6.7.2: Different types of Audit during System Development Process

Concurrent Audit	Auditors are members of the system development team. They assist the team in improving the quality of systems development for the specific system they are building and implementing.
Post - implementation Audit	Auditors seek to help an organization learn from its experiences in the development of a specific application system. In addition, they might be evaluating whether the system needs to be scrapped, continued, or modified in some way.
General Audit	Auditors evaluate systems development controls overall. They seek to determine whether they can reduce the extent of substantive testing needed to form an audit opinion about management's assertions relating to the financial statements for systems effectiveness and efficiency.

An external auditor is more likely to undertake general audits rather than concurrent or post-implementation audits of the systems development process. For internal auditors, management might require that they participate in the development of material application systems or undertake post-implementation reviews of material application systems as a matter of course.

6.7.3 Programming Management Controls

Some of the major concerns that an auditor should address under different activities involved in Programming Management Control Phase are provided in Table 6.7.3 as under:

Table 6.7.3: Audit Trails under Programming Management Controls

Phase	Audit Trails
Planning	• They should evaluate whether the nature of and extent of planning are appropriate to the different types of software that are developed

	or acquired. • They must evaluate how well the planning work is being undertaken.
Control	• They must evaluate whether the nature of and extent of control activities undertaken are appropriate for the different types of software that are developed or acquired. • They must gather evidence on whether the control procedures are operating reliably. For example - they might first choose a sample of past and current software development and acquisition projects carried out at different locations in the organization they are auditing.
Design	• Auditors should find out whether programmers use some type of systematic approach to design. • Auditors can obtain evidence of the design practices used by undertaking interviews, observations, and reviews of documentation.
Coding	• Auditors should seek evidence – o On the level of care exercised by programming management in choosing a module implementation and integration strategy. o To determine whether programming management ensures that programmers follow structured programming conventions. o To check whether programmers employ automated facilities to assist them with their coding work.
Testing	• Auditors can use interviews, observations, and examination of documentation to evaluate how well unit testing is conducted. • Auditors are most likely concerned primarily with the quality of integration testing work carried out by information systems professionals rather than end users. • Auditor's primary concern is to see that whole-of-program tests have been undertaken for all material programs and that these tests have been well-designed and executed.
Operation and Maintenance	• Auditors need to ensure effectively and timely reporting of maintenance needs occurs and maintenance is carried out in a well-controlled manner. • Auditors should ensure that management has implemented a review system and assigned responsibility for monitoring the status of operational programs.

6.7.4 Data Resource Management Controls

- Auditors should determine what controls are exercised to maintain data integrity. They might also interview database users to determine their level of awareness of these controls.
- Auditors might employ test data to evaluate whether access controls and update controls are working.

6.7.5 Quality Assurance Management Controls

- Auditors might use interviews, observations and reviews of documentation to evaluate how well Quality Assurance (QA) personnel perform their monitoring role.
- Auditors might evaluate how well QA personnel make recommendations for improved standards or processes through interviews, observations, and reviews of documentation.
- Auditors can evaluate how well QA personnel undertake the reporting function and training through interviews, observations, and reviews of documentation.

6.7.6 Security Management Controls

- Auditors must evaluate whether security administrators are conducting ongoing, high-quality security reviews or not;
- Auditors check whether the organizations audited have appropriate, high-quality disaster recovery plan in place; and
- Auditors check whether the organizations have opted for an appropriate insurance plan or not.

6.7.7 Operations Management Controls

- Auditors should pay concern to see whether the documentation is maintained securely and that it is issued only to authorized personnel.
- Auditors can use interviews, observations, and review of documentation to evaluate -
  - the activities of documentation librarians;
  - how well operations management undertakes the capacity planning ad performance monitoring function;
  - the reliability of outsourcing vendor controls;
  - whether operations management is monitoring compliance with the outsourcing contract; and
  - whether operations management regularly assesses the financial viability of any outsourcing vendors that an organization uses.

6.8 Application Controls and their Audit Trails

Application Controls and their categories have been explained in detail in Chapter 3 of the Study material. We may however again provide an overview of the same here as shown in Table 6.8.1.

Table 6.8.1: Types of Application Controls

Controls	Scope
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.
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.
Communication Controls	Responsible for controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, audit trail controls, and existence controls.
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.
Output Controls	To provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared and routed to users.
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.

Audit Trail Controls: Two types of audit trails that should exist in each subsystem are as follows:

- An **Accounting Audit Trail** to maintain a record of events within the subsystem; and
- An **Operations Audit Trail** to maintain a record of the resource consumption associated with each event in the subsystem.

We shall now discuss Audit Trails for Application Controls in detail.

6.8.1 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.

6.8.2 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.

6.8.3 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.

6.8.4 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.

6.8.5 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 before-images and after-images 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.

6.8.6 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.

6.9 Audit of Application Security Controls

There are many aspects to the application controls that are reviewed as a part of any application audit and the same has already been discussed in the earlier sections but out of these, application security is one of the most important controls that are why the same is discussed separately. The objective of this exercise is to establish whether the application security controls are operating effectively to protect the confidentiality, integrity and availability of information. Application security is concerned with maintaining these aforementioned attributes of the information. The result of lacunae in application security may lead to security related frauds that may give rise to financial and reputation losses.

6.9.1 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, 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.

- 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 user-id and passwords that are being used, including the design used for such controls;
- The roles, descriptions, user profiles and user groups that can be created in an application; and
- The policy of the organization for user access and supporting standards.

As discussed earlier, there are various layers, which are shown in the Fig. 6.9.1 and discussed as follows:

- **Operational Layer:** The basic layer, where user access decision are generally put in place.
- **Tactical Layer:** The next is management layer, which includes supporting functions such as security administration, IT risk management and patch management.
- **Strategic Layer:** This is the layer used by TOP management. It includes the overall information security governance, security awareness, supporting information security policies and standards, and the overarching an application security perspective.

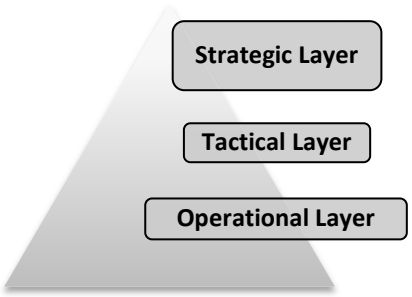

Fig. 6.9.1: Application Security Layer

6.9.2 Understanding the Layers and Related Audit Issues

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

(i) **Operational Layer:** The operational layer audit issues include:

- **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.

- **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.
- **Segregation of Duties:** As frauds due to collusions / lack of segregations increase across the world, importance of the Segregation of Duties also increases. As defined earlier, 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:
  - Record keeper of asset must not be asset keeper.
  - Cashier who creates a cash voucher in system, 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, the same need to be immediately communicated to those charged with governance.

(ii) **Tactical Layer:** At the tactical layer, security administration is put in place. This 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 the 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 the risk associated with each application and obtain a report on periodic risk assessment on the application or self-assessment/ compliance reports on the 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. Security of the interfaced data is also important, especially when unencrypted methods of transmission are used for data transmission.

- **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.

(iii) **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.

One of the key responsibilities of the IT risk management function is to promote ongoing security awareness to the organization's users. Security metrics are now becoming popular to gauge the performance of the security management function. These are often good indicators of the security health of an organization. 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.

Based on the key controls described previously, the risk assessment of failure/weakness in the operating effectiveness of the key application security controls shall be made and acted upon by auditor.

6.10 Summary

In the chapter, there has been a detailed discussion on Information System Audit, its need and the method of performing the same. Chapter outlines the losses that an organization may face, incase, it does not get it audited. The chapter also discusses the impact of computers on audit and audit procedures adopted. Afterwards, the chapter discusses the steps to perform an Information system audit. The idea of pre-audit survey and planning of an audit for effective execution of an audit has also been elaborated in the chapter.

The chapter discusses various auditing standards that an auditor can use for performing a systems audit. Chapter elaborates the standards issued by ISACA, ISO 27001 and Standards issued by ICAI. In addition, the chapter also elaborates concept of risk assessment, documentation to be done by an Information Systems Auditor (ISA). In addition, the chapter also provides a detailed discussion on Continuous Auditing. Finally, there is a detailed discussion on various types of controls, including specialized application security controls.