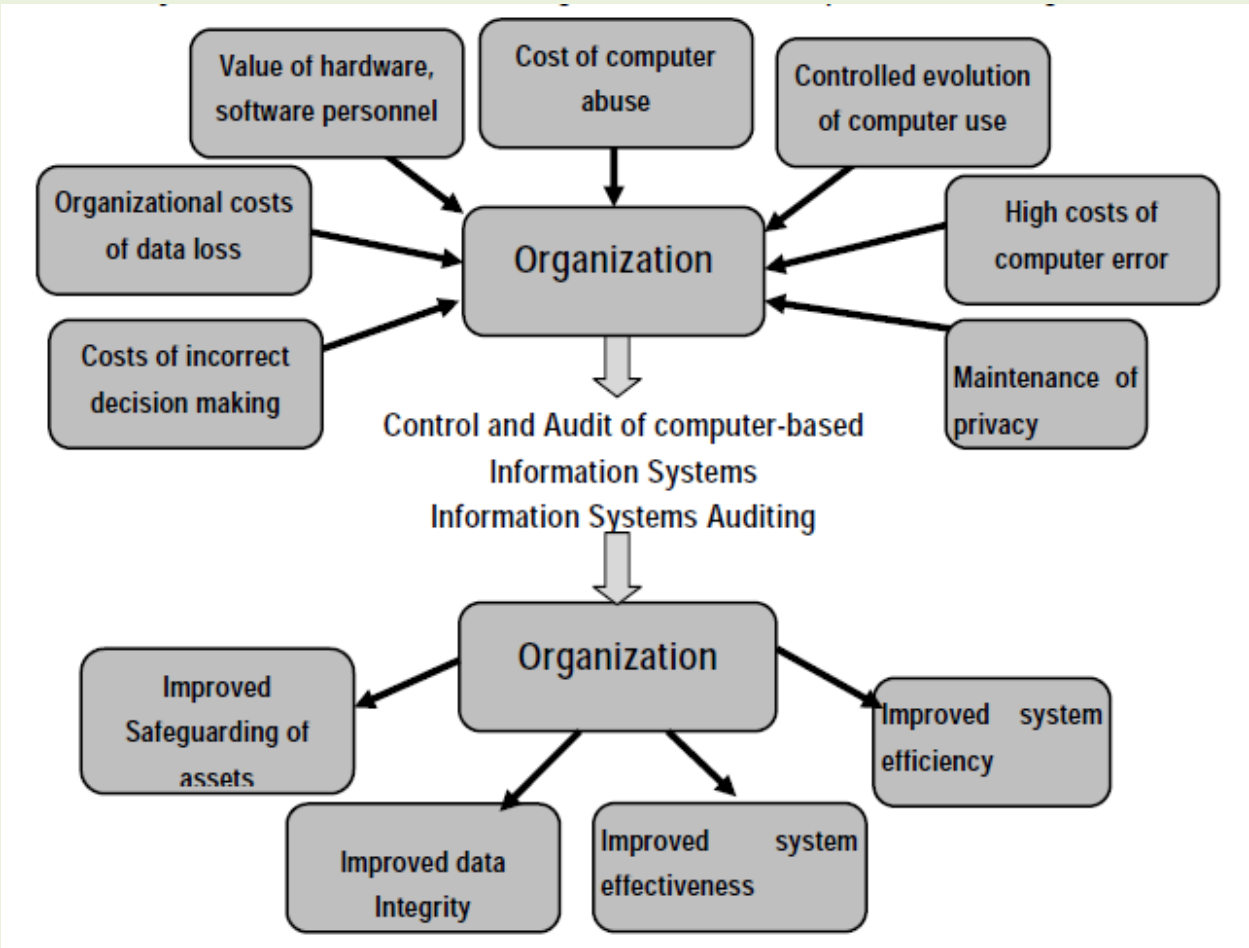
Chapter - 6

Auditing of Information Systems

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. We can better understand it with the help of following diagrammatical presentation :



These are following reseaons:

1. *Organisational Costs of Data Loss,*
2. *Incorrect Decision Making,*
3. *Costs of Computer Abuse,*
4. *Value of Computer Hardware,*
5. *Software and Personnel*,
6. *High Costs of Computer Error*,
7. *Maintenance of Privacy,*
8. *Controlled evolution of computer Use*,

Information Systems Auditing (ISA): It is the process of attesting objective s that focus on asset safeguarding, and data integrity both. Major objective of ISA is:

1) *Asset Safeguarding Objectives*,
2) *Data Integrity Objectives*,
3) *System Effectiveness Objectives* and
4) *System Efficiency Objectives*

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

I. **Changes to Evidence Collection:** The performance of evidence collection and understanding the reliability of controls involves issues like-
   a. *Data retention and storage,*
   b. *Absence of input documents*,
   c. *Non-availability of audit trail,*
   d. *Lack of availability of output,*
   e. *Audit evidence* and
   f. *Legal issues*.

II. **Changes to Evidence Evaluation:** Evaluation of audit trail and evidence is to trace consequences of control's strength and weakness throughout the system. Major issues are:
   a. *System generated transactions,*
   b. *Automated transaction processing*/generation *systems* and
   c. Systemic errors.

Responsibility for Controls: Management is responsible for establishing and maintaining control to achieve the objectives of effective and efficient operations, and reliable information systems.

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

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

Skills set for Information System Auditor :

- 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.

Functions of IS Auditor: IS Auditors review risks relating to IT systems and processes; some of them are:

I. *Inadequate information security controls*
II. *Inefficient use of resources, or poor governance ,*
III. *Ineffective IT strategies,*
IV. *policies and practices and*
V. *IT-related frauds.*

Categories of IS Audits: IS Audits has been categorized into five types:

1. *Systems and Application,*
2. *Information Processing Facilities*,
3. *Systems Development*,
4. *Management of IT and Enterprise Architecture* and *Telecommunications,*
5. *Intranets, and Extranets*.

Steps in Information System Audit: Different audit organizations go about IS auditing in different ways and individual auditors have their own favorite ways of working. However, it can be categorized into six stages, which are:

1) *Scoping and pre-audit survey,*
2) *Planning and preparation,*
3) *Fieldwork, Analysis,*
4) *Reporting and*
5) *Closure.*

Audit Standards and Best Practices: These are:

1) *IS auditing standards*,
2) *IS auditing guidelines*,
3) *IS auditing procedures & COBIT (Control objectives for information and related technology) of ISACA (Information Systems Audit and Control Association),*
4) *ISO 27001,*
5) *Internal Audit Standards,*
6) *Standards on Internal Audit issued by ICAI and ITIL*

Performing IS Audit: Various steps are given as follows:

A. 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. Adequate planning of the audit work helps to ensure that appropriate attention is devoted to important areas of the audit, potential problems are identified and that the work is completed expeditiously.

B . Preliminary Review: Some of the critical factors, which should be considered by an IS auditor as part of his/her preliminary review are:

1. *Knowledge of the Business,*
2. *Understanding the Technology,*
3. *Understanding Internal Control Systems*
4. *Legal Considerations and Audit Standards*
5. *Risk Assessment and Materiality.*

Risks are categorized as:

1) ***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.
2) ***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.
3) ***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.

Information system and Audit evidence

Inherent Limitations of Audit

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:

1. The nature of financial reporting;
2. The nature of audit procedures;
3. The need for the audit to be conducted within a reasonable period of time and at a reasonable cost.
4. Fraud, particularly fraud involving senior management or collusion.
5. The existence and completeness of related party relationships and transactions. The occurrence of non-compliance with laws and regulations.
6. Future events or conditions that may cause an entity to cease to continue as a going concern.
7. Use of special audit techniques, referred to as Computer Assisted Audit Techniques, for documenting evidences. Elaborated under this part, later on.
8. Audit timing can be so planned that auditor is able to validate transactions as they occur in system

Provisions relating to Digital Evidences

As per Indian Evidence Act, 1872, "Evidence" means and includes:

1. 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;
2. 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.

Concurrent or Continuous Audit: Continuous auditing enables auditors to significantly reduce and perhaps to eliminate the time between occurrence of the events at the client and the auditor's assurance services thereon. 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: Some of the well-known tools are:

(i) **Snapshots:** Tracing a transaction in 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.

(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.

(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 might use SCARF to collect the different

types of information such as *Application*

1. *System Errors*,
2. *Policy and Procedural Variances*,
3. *System Exception*,
4. *Statistical Sample*,
5. *Snapshots and Extended Records*,
6. *Profiling Data* and
7. *Performance Measurement*.

(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.

Some of the advantages of continuous audit techniques are:

1. *Timely*,
2. *Comprehensive and Detailed Auditing*,
3. *Surprise test capability*,
4. *Information to system staff on meeting of objectives and*
5. *Training for new users*.

(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.

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

1. *Detecting unauthorized access to the system,*
2. *Facilitating the reconstruction of events, and*
3. *Promoting personal accountability*

General Controls: Various general controls are: *Organizational Controls, Management Controls, Financial Controls, BCP Controls, Operating System Controls, Data Management Controls, System Development Controls, Computer Centre Security Controls, Internet & Intranet Controls and Personal Computers Controls.*

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:

1. *Risk Assessment*,
2. *Controls Assessment* and
3. *Review of Documents*.

Role of IS Auditor in Logical Across 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. Documentation of Auditing of environmental controls activities is a critical part.

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.

B. Audit Planning and Assessment: As part of risk assessment:

1. The controls assessment must ascertain that controls safeguard the organization against all acceptable risks including probable ones are in place.
2. The security policy of the organization should be reviewed to assess policies and procedures that safeguard the organization against environmental risks.
3. 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.

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

A. The IPF(Infrastructure Planning and Facilities) and the construction with regard to the type of materials used for construction;

B. The presence of water and smoke detectors, power supply arrangements to such devices, and testing logs;

C. The location of fire extinguishers, firefighting equipment and refilling date of fire extinguishers;

D. Emergency procedures, evacuation plans and marking of fire exists. There should be half-yearly Fire drill to test the preparedness;

E. Environmental control equipment such as air-conditioning, dehumidifiers, heaters, ionizers etc;

F. Compliant logs and maintenance logs to assess if MTBF and MTTR are within acceptable levels; and

G. 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

Application Controls and their Audit Trail: *These are categorized in the following types:*

1. ***Boundary Controls:*** *IT ensures that those who are using system are authentic users.*
2. ***Input Controls****: Responsible for bringing the data and instructions in to the information system.*
3. ***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.*
4. ***Processing Controls:*** *Responsible for computing, sorting, classifying and summarizing data. It maintains the chronology of events from the time data is received from input or communication systems to the time data is stored into the database or output as results.*

5. ***Database Controls****: Responsible to provide functions to define, create, modify, delete and read data in an information system. It maintains procedural data-set of rules to perform operations on the data to help a manager to take decisions.*
6. ***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.*

Audit Trail Control: Two types of audit trails that should exist in each sub system
Accounting Audit Trails and
Operations Audit Trails

Audit of Application Security Controls

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.

Approach to Application Security Audit

Application security audit is being looked from the usage perspective. A layered approach is used based on the functions and approach of each layer. Layered approach is based on the activities being undertaken at various levels of management, namely supervisory, tactical and strategic. The approach is in line with management structure which follows top-down approach. For this, auditors need to have a clear understanding of the following.

1. Business process for which the application has been designed;
2. The source of data input to and output from the application;
3. The various interfaces of the application under audit with other applications;
4. The various methods that may be used to login to application, other than normal user-id and passwords that are being used, including the design used for such controls;
5. The roles, descriptions, user profiles and user groups that can be created in an application; and
6. The policy of the organization for user access and supporting standards.

Review of Controls at various Layers: For application security audit, a layered approach is used based on the functions and approach of each layer. This approach is in line with management structure, which follows top-down approach. Various layers are:

1) **Operational Layer:** The basic layer, where user access decisions are generally put in place.
2) **Tactical Layer:** The next is management layer, which includes supporting functions such as security administration, IT risk management and patch management.
3) **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.

Various aspects relating to each aforementioned layer are given as follows:

1) **Operational Layer:** The operational layer audit issues include:
    a. *User Accounts and Access Rights,*
    b. *Password Controls and*

c. *Segregation of Duties.*

2) **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, IT Risk Management, Interface Security and Audit Logging and Monitoring.*

3) **Strategic Layer:** At this layer, the top management takes action, in form of drawing up security policy, security training, security guideline and reporting. A comprehensive information security programme fully supported by top management and communicated well to the organization is of paramount importance to succeed in information security. The security policy should be supported and supplemented by detailed standards and guidelines. These guidelines shall be used at the appropriate level of security at the application, database and operating system layers