CHAPTER 6: AUDITING OF INFORMATION SYSTEM

Need for Audit of Information system or Impact of IS audit in an organization or Factors influencing an organization towards control and audit of computers?

1. **Organizational Costs of Data Loss**: Data is a critical resource of an organization for its present and future process and its ability to adapt and survive in a changing environment.
2. **Cost of Incorrect Decision Making**: Management and operational controls taken by managers involve detection, investigations and correction of the processes.
3. **Costs of Computer Abuse**: Unauthorized access to computer systems, facilities and sensitive data can lead to destruction of assets
4. **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.
5. **High Costs of Computer Error**: In a computerized enterprise environment where many critical business processes are performed, a data error can cause great damage.
6. **Value of Computer Hardware, Software and Personnel**: These critical resources have credible impact on its infrastructure and business competitiveness.
7. **Maintenance of Privacy**: Data collected contains private information about an individual that needs to be maintained

EFFECTS OF COMPUTERS ON AUDIT

Changes to Evidence Evaluation

1. **Automated transaction processing systems:** can cause the auditor problems.
2. **System generated transactions**: Financial systems may have the ability to initiate, approve and record financial transactions
3. **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

Changes to Evidence Collection

1. **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 audit or due to which the auditor may not be able to review a whole reporting period transactions on the computer system.
2. **Absence of input documents:** Transaction data may be entered into the computer directly without the presence of supporting documentation resulting in less paperwork being available for audit examination.
3. **Lack of availability of printed output:** In the absence of physical output, it may be necessary for the auditor to directly access the electronic data retained on the client's computer
4. **Audit evidence:** Certain transactions may be generated automatically by the computer system.
5. **Non-availability of audit trail**: The audit trails may exist in computer system for short period, which makes auditor's job very difficult.
6. **Legal issues**: Making use of Electronic Data Interchange (EDI) and electronic trading over the Internet can create problems with contracts

IS AUDITOR

Explain the set of skills that is generally expected of an IS auditor?

1. Sound knowledge of business operations, practices and compliance requirements;
2. Good knowledge of Professional Standards and Best Practices of IT controls and security.
3. Knowledge of IT strategies, policy and procedural controls
4. Should possess the requisite professional technical qualification and certifications;
5. A good understanding of information Risks and Controls;
6. Ability to understand technical and manual controls relating to business continuity

Functions / Risks reviewed relating to IT systems & process as part of functions

1. Inadequate information security controls. (E.g. missing or out of date antivirus controls, open ports, open systems without password or weak passwords etc.)
2. Inefficient use of resources, or poor governance;
3. Ineffective IT strategies, policies and practices; and
4. IT-related frauds (including phishing, hacking etc.)

IS AUDIT

Objectives of IS Audit

1. **Asset Safeguarding Objectives**: The information system assets must be protected from unauthorized access by system of internal controls
2. **Data Integrity Objectives**: Data integrity important from the business perspective of the decision maker, competition and the market environment.
3. **System Effectiveness Objectives**: Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet business and user requirements.
4. **System Efficiency Objectives**: To optimize the use of various information system resources along with the impact on its computing environment

Major types/Categories of IS Audit

1. **Systems and Application**: An audit to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.
2. **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.
3. **Telecommunications, Intranets, and Extranets:** An audit to verify that controls are in place on the client, server, and on the network connecting the clients and servers
4. **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.
5. **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.

Steps / Major stages of IS Audit

1. **Scoping and pre-audit survey**: Auditors determine main area/s of focus based on scope-definitions agreed with management.
2. **Planning and preparation:** The scope is broken down into greater levels of detail, usually involving generation of audit work plan or risk-control-matrix.
3. **Fieldwork:** This step involves gathering of evidence by interviewing staff and managers, reviewing documents, and observing processes etc.
4. **Analysis:** SWOT (Strengths, Weaknesses, Opportunities, Threats) or PEST (Political, Economic, Social, Technological) techniques can be used for analysis.
5. **Reporting:** Reporting to the management is done after analysis of evidence is gathered and analyzed.
6. **Closure**: Closure involves preparing notes for future audits and follow up with management to complete actions they promised after previous audits.

TYPES OF AUDIT TOOLS

1. Snapshots: The snapshot software is built into system at those points where material processing occurs which takes images of flow of any transaction as it moves through application. These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction.

2. **Integrated Test Facility (ITF):** The ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness.

(i) Methods of Entering Test Data
(ii) Methods of removing the Effects of ITF Transactions

3. System Control Audit Review File (SCARF):

- The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. Auditors might use SCARF to collect the following types of information:

  - ✓ **Application System Errors** - SCARF provides an independent check on the quality of system processing & errors into the system.
  - ✓ **Policy and Procedural Variances** - SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.
  - ✓ **Profiling Data** - Auditors can use embedded audit routines to collect data to build profiles of system users & any deviations indicate errors or irregularities.
  - ✓ **Performance Measurement** - Useful for measuring or improving the performance of an application system.
  - ✓ **System Exception** - Monitor different types of application system exceptions.
  - ✓ **Statistical Sample** - SCARF provides a convenient way of collecting all the sample information together & use analytical review tools.
  - ✓ **Snapshots and Extended Records** - It can be written into the SCARF file and printed when required.

4. Continuous and Intermittent Simulation (CIS):

This technique can be used to trap exceptions whenever the application system uses a DBMS.

Advantages of continuous audit techniques:

a) **Timely, Comprehensive and Detailed Auditing** – Evidence would be available more timely and in a comprehensive manner.
b) **Training for new users** – Using the ITFs, new users can submit data to the application system & obtain feedback on mistakes.
c) **Surprise test capability** – Auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment.
d) **Information to system staff on meeting of objectives -** Evaluate whether application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.

Disadvantages of continuous audit techniques:

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

5. 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 & will investigate these tagged records for detecting fraud. This approach of real-time notification displays a message on the auditor's terminal.

PERFORMING IS AUDIT

STEPS

1. Basic Plan

2. Preliminary Review

(i) Knowledge of Business

(ii) Understanding the Technology

- ✓ Analysis of business processes and level of automation,
- ✓ Assessing the extent of dependence of the enterprise on Information Technology to carry on its businesses
- ✓ Understanding technology architecture which could be distributed / centralized / hybrid architecture,
- ✓ Studying network diagrams to understand physical and logical network connectivity
- ✓ Understanding extended enterprise architecture
- ✓ Knowledge of various technologies & their advantages & limitations is critical competence requirement for auditor.
- ✓ Studying Information Technology policies, standards, guidelines and procedures

(iii) Understanding Internal Control Systems

(iv) Legal Considerations & Audit Standards

- ✓ The auditor should carefully evaluate the legal as well as statutory implications on audit work
- ✓ The IS audit work could be required as part of a statutory requirement in which case he should take into consideration - stipulations, regulations and guidelines.
- ✓ The statutes or regulatory framework may impose stipulations as regards minimum set of control objectives to be achieved by the subject organization.
- ✓ The IS Auditor should also consider the Audit Standards applicable to his conduct and performance of audit work

(v) Risk Assessment & Materiality

Key steps that can be followed for a risk-based approach to make an audit plan?

- ✓ Inventory the IS in use in the organization and categorize them.
- ✓ Determine which systems impact critical functions or assets & how close to real time they operate.
- ✓ Assess what risks affect these systems & the likelihood and severity of the impact on the business
- ✓ Decide audit priority, resources, schedule and frequency.

Categories of Risk

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. Internal controls are ignored in setting inherent risk. It is often an area of professional judgement by 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.

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. It is associated with lack of identification of disaster recovery plans is ordinarily low since existence is easily verified

AUDIT TRAIL

Audit trails are logs that can be designed to record activity at the system, application, and user level. When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives. Audit trail controls attempt to ensure that a chronological record of all events that have occurred in a system is maintained.

OBJECTIVES

1. Detecting Unauthorized Access: It 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. Used to determine if unauthorized access was accomplished, or attempted and failed.

2. 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.

3. Personal Accountability: Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log. Helps to monitor user activity at lowest level.

Audit of Environmental Controls

- ✓ The IPF & construction with regard to type of materials used for construction
- ✓ Presence of water & smoke detectors
- ✓ Location of fire extinguishers, equipment & refilling date of fire extinguishers
- ✓ Emergency procedures, evacuation plans & marking of fire exits
- ✓ Documents for compliance with legal & regulatory requirements with regard to fire safety equipment
- ✓ Power resources, generators etc. must be checked to test effectiveness of backup power
- ✓ Environment control equipment's – Air conditioner, heaters etc.
- ✓ Identify undesired activities such as smoking, consumption of eatables etc.

CHAPTER 6.1: AUDITING OF INFORMATION SYSTEM

MANAGERIAL CONTROLS AND THEIR AUDIT TRAILS

MANAGERIAL CONTROLS	AUDIT TRAILS
Top Management and Information Systems Management Controls	**Planning**: Auditors evaluate whether top management has formulated a high-quality information system's plan that is appropriate to the needs of an organization or not. **Organizing**: Auditors should be concerned about how well top management acquires and manage staff resources. **Leading:** Generally, the auditors examine variables that often indicate when motivation problems exist or suggest poor leadership **Controlling:** 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.
System Development Management Controls	**Concurrent Audit**: Auditors 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. **General Audit**: Auditors seek to determine whether they can reduce extent of substantive testing needed to form an audit opinion about management's assertions relating to financial statements for systems effectiveness & efficiency.
Programming Management Controls	**Planning**: Auditors must evaluate how well the planning work is being undertaken. **Control**: Auditors must evaluate whether the nature of and extent of control activities undertaken are appropriate for different types of s/w that are developed or acquired. **Design**: Auditors should find out whether programmers use some type of systematic approach to design. **Coding**: Auditors should seek evidence to check whether programmers employ automated facilities to assist them with their coding work. **Testing:** Auditor's primary concern is to see that unit testing; integration testing of the system testing has been undertaken appropriately. **Operation and Maintenance**: Auditors need to ensure effectively & timely reporting of maintenance needs occurs & maintenance is carried out in a well-controlled manner
Data Resource Management Controls	Auditors should determine what controls are exercised to maintain data integrity. They might employ test data to evaluate whether access controls and update controls are working.
Quality Assurance Management Controls	Auditors might use interviews, observations and reviews of documentation to evaluate how well Quality Assurance (QA) personnel perform their monitoring and reporting function.
Security Management Controls	Auditors must evaluate whether security administrators are conducting ongoing, high-quality security reviews or not; and check whether organizations have opted appropriate Disaster Recovery and Insurance plan or not.
Operations Management Controls	Auditors should pay concern to see whether the documentation is maintained securely and that it is issued only to authorized personnel.

Describe how the application controls and their audit trail are categorized

BOUNDARY CONTROLS

It maintains chronology of events

- ✓ Identity of would be user of the system
- ✓ Authentication information supplied
- ✓ Resources requested
- ✓ Terminal identifier

Accounting Audit Trial

- Action privileges / denied

Operations Audit Trial

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

PROCESSING CONTROLS

The audit trail maintains the chronology of events from the time data is received from the input / communication subsystem to the time data is dispatched to the database, communication, or output subsystems

Accounting Audit Trial

- trace and replicate the processing performed on a data item.
- Triggered transactions to monitor input data entry, intermediate results and output data

Operations Audit Trial

- A comprehensive log on hardware consumption – CPU time used, 2ndary storage
- A comprehensive log on software consumption – compilers used, subroutine libraries used etc.

INPUT CONTROLS

Responsible for bringing the data and instructions in to the information system. It helps in validation & error detection of data input into system

Accounting Audit Trial

- Identity of the person who was the source of the data
- Identity of the person who entered the data into the system
-Time & date when data was capture
- Device used to enter data

Operations Audit Trial

- Time to key in source data
- No of keying errors identified during verification
- Frequency & command language used

DATABASE CONTROLS

Maintains the chronology of events that occur either to the database definition or the database itself

Accounting Audit Trial

- Attach unique time stamp to all transactions
- Attach before image & after Image
- Accommodating changes that occur within application system

Operations Audit Trial

- Maintain chronology of resource consumption that affects the database / database definition identified during verification

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 Trial

- Unique identifier of the source or sink node
- Time and date at which the message was received by the sink node & traversed by message
- Message sequence number & the image of the message received

Operations Audit Trial

- No of messages traversed at each link & node.
- Queue lengths, no of errors occurring at each link
- Log of system restarts
- Message transit time b/w nodes & at nodes

OUTPUT CONTROLS

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 Trial

- What output was presented to users?
- Who received the output?
- When the output was received?
-What actions were taken with the output

Operations Audit Trial

- To maintain the record of resources consumed
  - graphs, images, report pages, printing time, & display rate to produce various outputs