

4. Audit under Computerised Information System (CIS) Environment

Important Point of this chapter

1. CIS Environment

Scope of Audit in CIS Environment

1. High Speed
2. Low clerical error
3. Concentration of Duties
4. Shifting of internal control base on
 - Application system development control
 - System Software control
5. Disappearance of manual process
6. Impact of poor system
7. Exception reporting
8. Man-Machine interface/ Human computer interface

Audit Approach in CIS Environment

- a. **Black Box Approach:** in the black box approach or auditing around the computer, the auditor concentrates on input and output and ignores the specific of how computer process the data or transactions. If input matches the output, the auditor assumes that the processing of transaction must have been correct.
- b. **White Box Approach:** The process and controls surrounding the subject are not only subject to audit but also the processing controls operating over this process are investigated. In order to help the auditor to gain access to these processes computer audit software may be used.

Effects of Computer on Internal Controls

1. Separation of Duties
2. Delegation of Authority and Responsibility
3. Competent and Trustworthy personnel
4. System of authorization
5. Adequate Document and Records
6. Physical control over assets and records
7. Adequate management supervision
8. Independent checks on performance
9. Comparing recorded accountability with assets

Effects of Computers on auditing

1. Changes to Evidence Collection: collecting evidence on the reliability of a computer system is often more complex than collecting evidence on the reliability of manual system.
2. Changes to evidence Evaluation: with increasing complexity of computer systems and control technology, it is becoming more and more difficult for the auditors to evaluate the

consequences of strength and weaknesses of control mechanism for placing overall reliability on the system

Internal control in CIS Environment

Internal control is an essential prerequisite for efficient and effective management of any organization. Internal control in a CIS system depends on the same principal as that of manual system. Thus,, the plan of organization, delegation of powers, system authorization, distribution of duties etc., are determined on similar consideration as in a manual system.

In setting up an internal control system in a CIS environment, the overall CIS operation need to be broken into defined subsystem and controls established accordingly, addressing each function separately so that auditors can place reliance on them. The basic components that can be identified in a CIS environment are as

- Hardware
- Software
- People
- Transmission media

Different control

In a computer system many different types of control are used to enhance component reliability. Major classes of control that are auditor must evaluate are

- a. Authenticity control
- b. Accuracy control
- c. Completeness control
- d. Redundancy control
- e. Privacy control
- f. Audit trail controls
- g. Existence control
- h. Asset safeguarding controls
- i. Effectiveness controls
- j. Efficiency controls

Consideration of control attributes by the auditors

In evaluating the effects of a control, the auditor needs to assess the reliability by considering the various attributes of a control. Some of the attributes are

1. Whether the control is in place and is functioning as desired
2. Generality versus specificity of the control with respect to the various types of errors and irregularities that might occur.
3. Whether the control acts to prevent, detect or correct errors. The auditor here mainly focuss on preventive, detective and corrective control.
4. The number of components used to execute he control.

Internal Control Requiems in CIS environment

The requirement of internal control under CIS environment may cover the following aspects

1. Organization and management control: Controls are designed to framework for CIS activities including Policies and procedures relating to control or appropriate segregation of incomputable function.
2. Application System development and Maintenance control: Control are designed to provide reasonable assurance that systems are developed and maintained in an authorizes and efficient manner
3. Computer operation control: Designed to control the operation of the system provide reasonable assurance that the system used for authorized purpose in authorized manner and with authorized software only.
4. System software control: controls are designed to provide reasonable assurance that system software is acquired or developed in authorized and efficient manner.
5. Data entry and program control: designed for authorized transaction is entered and access to data and program is restricted to authorized personnel only.
6. Control over input: designed to provide reasonable assurance about the transaction entered in system are by authorization process only.
7. Control over processing and computer data files.
8. Control over output
9. Other safeguards: offsite backup of data, recovery procedure on theft or accidental destruction or provision for offset processing in the event of disaster.

Approach to auditing in CIS environment

The auditor should consider the effect of factor in accounting while audit the entity like:

- a. The extent of use of computer for preparing accounting information
- b. Efficiency of internal control over input, processing, analysis and reporting undertaken in the CIS installation and;
- c. The impact of computerization on the audit trail that could otherwise be expected to exist in manual system

Points to be consider while evaluating the reliability of internal control and accounting system

- a. Ensure that authorized, correct and complete data is made available for processing;
- b. Provide for timely detection and correction of errors;
- c. Ensure that the case of interruption in the work of CIS environment due to power, merchant or processing failures, and the system restarts without disporting the completion of the entries and records.
- d. Ensure that accuracy and completeness of output;
- e. Provide adequate data security against fire and other calamities, wrong processing, frauds etc.
- f. Prevent unauthorized amendments to the program;
- g. Provide for safe custody of source code of application software and data files.

Computer Assisted Audit Techniques (CAAT's)

CAATs are computer programs and data that the auditor uses as part of the audit procedures to process data of audit significance, contained in an entity's information system. This process is used in performing various procedures including the following;

- Tests of details of transaction and balances
- Analytical procedures
- Tests of general controls
- Sampling programs and extract data for audit testing
- Test of application control
- Repperforming calculations performed by the entity's accounting system.

Consideration in use of CAATs

Before using the CAATs the auditor considers the controls incorporated in the design of the entity's computer system which CAAT would be applied in order to determine whether, and if so, how CAATs would be used.

- IT Knowledge, Expertise and Experience of the Audit team
- Availability of CAATs and suitable computer facilities
- The impracticability of manual tests
- Effectiveness and efficiency of the System
- Time constraints

Using CAATs

The major steps to be undertaken by the auditor in the application of CAAT are to:

1. Set the objective of CAAT application
2. Determine the content and accessibility of the entity's files
3. Identify the specific files or databases to be examined
4. Understand the relationship between the data tables where a database is to be examined
5. Define the specific tests to procedures and related transaction and balance affected
6. Define the output requirements
7. Arrange with the user and IT departments, if appropriate, for copies of the relevant files or database tables to be made at the appropriate cut off data and time
8. Identify the personnel who may participate in the design and application of CAAT
9. Refine the estimated of costs and benefits
10. Ensure that the use of CAAT is properly controlled
11. Arrange the administrative activities, including the necessary skills and computer facilities
12. Reconcile data to be used for CAAT with the accounting and other records
13. Execute CAAT application
14. Evaluate the results
15. Document CAATs to be used including objectives, high level flowcharts and run instruction; and;
16. Assess the effect changes to programs/system on the use of CAAT.

Procedures carried out by the auditor to control CAATs application

- a. Participating in the design and testing of CAAT;
- b. Checking, if applicable, the coding of the program to ensure that it conforms with the detailed program specifications;
- c. Asking the entity's staff to review the operating system instructions to ensure that the software will run in the entity's computer installation.
- d. Running the audit software on small test files before running it on the main data files;
- e. Checking whether the connect files were used
- f. Obtaining evidence that the audit software functioned as planned
- g. Establishing appropriate security measures to safeguard the integrity and confidentiality of data.