

Paper : Computerized Accounting**UNIT 4: Auditing in Computerized Accounting System**

Audit in Computerized Accounting System

Information technology (IT) is integral to modern accounting and management information systems. It is, therefore, imperative that auditors should be fully aware of the impact of IT on the audit of a client's financial statements, both in the context of how it is used by a client to gather, process and report financial information in its financial statements, and how the auditor can use IT in the process of auditing the financial statements.

Application controls, comprising input, processing, output and master file controls established by an audit client, over its computer-based accounting system and Computer-assisted audit techniques (CAATs) that may be employed by auditors to test and conclude on the integrity of a client's computer-based accounting system.

Application Controls

Application controls are those controls (manual and computerised) that relate to the transaction and standing data pertaining to a computer-based accounting system. They are specific to a given application and their objectives are to ensure the completeness and accuracy of the accounting records and the validity of entries made in those records. An effective computer-based system will ensure that there are adequate controls existing at the point of input, processing and output stages of the computer processing cycle and over standing data contained in master files. Application controls need to be ascertained, recorded and evaluated by the auditor as part of the process of determining the risk of material misstatement in the audit client's financial statements.

Input Controls

Control activities designed to ensure that input is authorised, complete, accurate and timely are referred to as input controls. Dependent on the complexity of the application program in question, such controls will vary in terms of quantity and sophistication. Factors to be considered in determining these variables include cost considerations, and confidentiality requirements with regard to the data input. Input controls common to most effective application programs include on-screen prompt facilities (for example, a request for an authorised user to 'log-in') and a facility to produce an audit trail allowing a user to trace a transaction from its origin to disposition in the system.

Specific input validation checks may include:

- i) Format checks: These ensure that information is input in the correct form. For example, the requirement that the date of a sales invoice be input in numeric format only – not numeric and alphanumeric.
- ii) Range checks: These ensure that information input is reasonable in line with expectations. For example, where an entity rarely, if ever, makes bulk-buy purchases with a value in excess of \$50,000, a purchase invoice with an input value in excess of \$50,000 is rejected for review and follow-up.
- iii) Compatibility checks: These ensure that data input from two or more fields is compatible. For example, a sales invoice value should be compatible with the amount of sales tax charged on the invoice.
- iv) Validity checks: These ensure that the data input is valid. For example, where an entity operates a job costing system – costs input to a previously completed job should be rejected as invalid.
- v) Exception checks: These ensure that an exception report is produced highlighting unusual situations that have arisen following the input of a specific item. For example, the carry forward of a negative value for inventory held.
- vi) Sequence checks: These facilitate completeness of processing by ensuring that documents processed out of sequence are rejected. For example, where pre-numbered goods received notes are issued to acknowledge the receipt of goods into physical inventory, any input of notes out of sequence should be rejected.

vii) Control totals: These also facilitate completeness of processing by ensure that pre-input, manually prepared control totals are compared to control totals input. For example, non-matching totals of a 'batch' of purchase invoices should result in an on-screen user prompt, or the production of an exception report for follow-up. The use of control totals in this way are also commonly referred to as output controls (see below).

viii) Check digit verification: This process uses algorithms to ensure that data input is accurate. For example, internally generated valid supplier numerical reference codes, should be formatted in such a way that any purchase invoices input with an incorrect code will be automatically rejected.

Processing Controls

Processing controls exist to ensure that all data input is processed correctly and that data files are appropriately updated accurately in a timely manner. The processing controls for a specified application program should be designed and then tested prior to 'live' running with real data. These may typically include the use of run-to-run controls, which ensure the integrity of cumulative totals contained in the accounting records is maintained from one data processing run to the next. For example, the balance carried forward on the bank account in a company's general (nominal) ledger. Other processing controls should include the subsequent processing of data rejected at the point of input, for example:

- A computer produced print-out of rejected items.
- Formal written instructions notifying data processing personnel of the procedures to follow with regard to rejected items.
- Appropriate investigation/follow up with regard to rejected items.
- Evidence that rejected errors have been corrected and re-input.

Output Controls

Output controls exist to en sure that all data is processed and that output is distributed only to prescribed authorised users. While the degree of output controls will vary from one

organisation to another (dependent on the confidentiality of the information and size of the organisation), common controls comprise:

- Use of batch control totals, as described above (see 'input controls').
- Appropriate review and follow up of exception report information to ensure that there are no permanently outstanding exception items.
- Careful scheduling of the processing of data to help facilitate the distribution of information to end users on a timely basis.
- Formal written instructions notifying data processing personnel of prescribed distribution procedures.
- Ongoing monitoring by a responsible official, of the distribution of output, to ensure it is distributed in accordance with authorised policy.

Master File Controls

The purpose of master file controls is to ensure the ongoing integrity of the standing data contained in the master files. It is vitally important that stringent 'security' controls should be exercised over all master files.

These include:

- appropriate use of passwords, to restrict access to master file data
- the establishment of adequate procedures over the amendment of data, comprising appropriate segregation of duties, and authority to amend being restricted to appropriate responsible individuals
- regular checking of master file data to authorised data, by an independent responsible official
- processing controls over the updating of master files, including the use of record counts and control totals.

Advantages or Merits of Computerized Accounts to Auditors

1. The operating system does all the complex and tedious tasks and the auditor's job is made easier.
2. It saves time and reduces manual work to a great extent.
3. EDP environment encourages decentralization of processing of data. Thus, the reports, required by the management can be obtained at any time and the management can take quick action based on such reports.
4. Decision-making is a vital function of the top management. Marginal costing techniques and operations research techniques are mere tools used by the management for decision-making. However, the Decision Supporting System and Artificial Intelligence not only analyze a business situation but also make decisions on behalf of the management (These systems are now being introduced in many organizations on an experimental basis).
5. Sophisticated software, which help the auditor in forming his opinion, are now being developed through Computer aided software engineering and Data Base Management Systems.
6. Electronic Data Interchange and other Computer Software / Hardware systems have reduced the cumbersome paper work in the auditor's office.
7. The audited balance sheets and other financial statements are now accepted by the Income Tax authorities and by the Registrar of Companies in electronic media.
8. Traditional data entry is prone to errors and frauds. Voice recognizing system and scanners have replaced the traditional data entry and have made the work easy and less prone to errors.
9. The Real Time Processing has tremendously improved the Stock-keeping and share market operations.
10. Bank balances can be verified and confirmed online.

Disadvantages or Demerits or Problems faced in the Audit of Computerized Accounts

1. An auditor cannot physically observe the process of accounting in computerized system. i.e., visual observation of the processing is denied.
2. An auditor cannot ensure that the procedure followed in processing is proper.
3. The procedure may be changed by intervention or by malicious codes. This may not come to the knowledge of the auditor.
4. The actual procedure followed may be quite different from the standard procedure to be followed.
5. The source document, intermediate document and reports are eliminated completely or partially. Therefore, the auditor may not be able to trace the data from the source. In other words, one can say "Audit trail" disappears totally or partially with computerization of accounts.
6. The '**source code**' given and the '**object code**' used may not agree with each other. It creates a major problem for the auditors.
7. To ensure efficiency in operation, many banks have introduced real-time processing wherein every transaction of the branches is processed immediately by the head office through the computers.

Though this system is extremely efficient, the insufficiency in the availability of infrastructure facility hinders the operation of the system. Sometimes, it so happens that the branches in the remote areas wait for several hours for the system to process one transaction. This affects the auditor in performing the concurrent audit.

Statutory Audit

A statutory audit is a legally required review of the accuracy of a company's or government's financial statements and records. An audit is an examination of records held by an organization, business, government entity, or individual, which involves the analysis of financial records or other areas.

A statutory audit is a legally required check of the accuracy of the financial statements and records of a company or government. A statutory audit is intended to determine if an organisation delivers an honest and accurate representation of its financial position by evaluating information, such as bank balances, financial transactions, and accounting record.

Voucher Verification

A voucher is an internal document describing and authorizing the payment of a liability to a supplier. It is most commonly used in a manual payment system, where it is part of the system of controls. A voucher typically contains the following information: ... The date on which payment should be made.

Vouching means “to vouch” i.e. examine the vouchers. On the other hand, Verification means “to verify” the assets and liabilities of the business. The Verification of Vouchers report displays all the Vouchers available for Audit under the selected Ledger. The Auditor can drill down on the required Group/Subgroup and select the required Ledger and drill down to view the Ledger Vouchers report.

CAAT (Computer Assisted Audit Techniques) : Various Tools

The nature of computer-based accounting systems is such that auditors may use the audit client company’s computer, or their own, as an audit tool, to assist them in their audit procedures. The extent to which an auditor may choose between using CAATs and manual techniques on a specific audit engagement depends on the following factors:

- the practicality of carrying out manual testing
- the cost effectiveness of using CAATs
- the availability of audit time
- the availability of the audit client’s computer facility
- the level of audit experience and expertise in using a specified CAAT
- the level of CAATs carried out by the audit client’s internal audit function and the extent to which the external auditor can rely on this work.

There are three classifications of CAATs – namely:

- 1) Audit software
- 2) Test data
- 3) Other techniques

1) AUDIT SOFTWARE: Audit software is a generic term used to describe computer programs designed to carry out tests of control and/or substantive procedures. Such programs may be classified as:

i) Packaged programs: These consist of pre-prepared generalised programs used by auditors and are not 'client specific'. They may be used to carry out numerous audit tasks, for example, to select a sample, either statistically or judgementally, during arithmetic calculations and checking for gaps in the processing of sequences.

ii) Purpose written programs: These programs are usually 'client specific' and may be used to carry out tests of control or substantive procedures. Audit software may be bought or developed, but in any event the audit firm's audit plan should ensure that provision is made to ensure that specified programs are appropriate for a client's system and the needs of the audit. Typically, they may be used to re-perform computerised control procedures (for example, cost of sales calculations) or perhaps to carry out an aged analysis of trade receivable (debtor) balances.

iii) Enquiry programs: These programs are integral to the client's accounting system; however they may be adapted for audit purposes. For example, where a system provides for the routine reporting on a 'monthly' basis of employee starters and leavers, this facility may be utilised by the auditor when auditing salaries and wages in the client's financial statements. Similarly, a facility to report trade payable (creditor) long outstanding balances could be used by an auditor when verifying the reported value of creditors.

2) TEST DATA: It includes –

1) Audit test data: Audit test data is used to test the existence and effectiveness of controls built into an application program used by an audit client. As such, dummy transactions are processed through the client's computerised system. The results of processing are then compared to the auditor's expected results to determine whether controls are operating efficiently and systems' objectiveness are being achieved. For example, two dummy bank payment transactions (one inside and one outside authorised parameters) may be processed with the expectation that only the transaction processed within the parameters is 'accepted' by the system. Clearly, if dummy

transactions processed do not produce the expected results in output, the auditor will need to consider the need for increased substantive procedures in the area being reviewed.

II) Integrated test facilities: To avoid the risk of corrupting a client's account system, by processing test data with the client's other 'live' data, auditors may instigate special 'test data only' processing runs for audit test data. The major disadvantage of this is that the auditor does not have total assurance that the test data is being processed in a similar fashion to the client's live data. To address this issue, the auditor may therefore seek permission from the client to establish an integrated test facility within the accounting system. This entails the establishment of a dummy unit, for example, a dummy supplier account against which the auditor's test data is processed during normal processing runs.

3) OTHER TECHNIQUES: Other CAATs include:

I) Embedded audit facilities (EAFs): This technique requires the auditor's own program code to be embedded (incorporated) into the client's application software, such that verification procedures can be carried out as required on data being processed. For example, tests of control may include the reperformance of specific input validation checks (see input controls above) – selected transactions may be 'tagged' and followed through the system to ascertain whether stated controls and processes have been applied to those transactions by the computer system. The EAFs should ensure that the results of testing are recorded in a special secure file for subsequent review by the auditor, who should be able to conclude on the integrity of the processing controls generally, from the results of testing. A further EAF, of ten overlooked by students, is that of an analytical review program enabling concurrent performance of analytical review procedures on client data as it is being processed through the automated system.

ii) Application program examination: When determining the extent to which they may rely on application controls, auditors need to consider the extent to which specified controls have been implemented correctly. For example, where system amendments have occurred during an accounting period, the auditor would need assurance as to the existence of necessary controls both before and after the amendment. The auditor may seek to obtain such assurance by using a software program to compare the controls in place prior to, and subsequent to, the amendment date.