Auditing and Assurance Standard (AAS) 29

Auditing in a Computer Information Systems Environment

The following is the text of the Auditing and Assurance Standard (AAS) 29, "Auditing in a Computer Information Systems Environment" issued by the Council of the Institute of Chartered Accountants of India. This Standard should be read in conjunction with the "Preface to the Statements on Standard Auditing Practices" issued by the Institute.

**Introduction**

1. The purpose of this Auditing and Assurance Standard (AAS) is to establish standards on procedures to be followed when an audit is conducted in a computer information systems (CIS) environment. For the purposes of this AAS, a CIS environment exists when one or more computer(s) of any type or size is (are) involved in the processing of financial information, including quantitative data, of significance to the audit, whether those computers are operated by the entity or by a third party.

2. The overall objective and scope of an audit does not change in a CIS environment. However, the use of a computer changes the processing, storage, retrieval and communication of financial information and may affect the accounting and internal control systems employed by the entity. Accordingly, a CIS environment may affect:
   - the procedures followed by the auditor in obtaining a sufficient understanding of the accounting and internal control system.
   - the auditor's evaluation of inherent risk and control risk through which the auditor assesses the audit risk.
   - the auditor's design and performance of tests of control and substantive procedures appropriate to meet the audit objective.

3. The auditor should consider the effect of a CIS environment on the audit. The auditor should evaluate, inter alia, the following factors to determine the effect of CIS environment on the audit:
   - the extent to which the CIS environment is used to record, compile and analyse accounting information;
   - the system of internal control in existence in the entity with regard to:
     - flow of authorised, correct and complete data to the processing center;
     - processing, analysis and reporting tasks undertaken in the installation; and
   - the impact of computer-based accounting system on the audit trail that could otherwise be expected to exist in an entirely manual system.

---

1 Issued in January 2003.
2 With the formation of the Auditing Practices Committee (now known as the Auditing and Assurance Standards Board) in 1982, the Council of the Institute has been issuing a series of Statements on Standard Auditing Practices (SAPs). SAPs have been renamed as Auditing and Assurance Standards (AASs). The Auditing and Assurance Standards (hitherto known as SAPs) lay down the principles governing an audit. These principles apply whenever an independent audit is carried out. Auditing and Assurance Standards become mandatory on the dates specified in the respective AAS. Their mandatory status implies that, while discharging their attest function, it will be the duty of the members of the Institute to ensure that the AASs are followed in the audit of financial information covered by their audit reports. If, for any reason, a member has not been able to perform an audit in accordance with the AASs, his report should draw attention to the material departures therefrom. The Auditing and Assurance Standards have the same authority as that attached to the Statements on Standard Auditing Practices.
4. The auditor should have sufficient knowledge of the computer information systems to plan, direct, supervise, control and review the work performed. The sufficiency of knowledge would depend on the nature and extent of the CIS environment. The auditor should consider whether any specialised CIS skills are needed in the conduct of the audit. Specialised skills may be needed inter alia to:

- obtain sufficient understanding of the effect of the CIS environment on accounting and internal control systems;
- determine the effect of the CIS environment on the assessment of overall audit risk and of risk at the account balance and class of transactions level; and
- design and perform appropriate tests of control and substantive procedures.

If specialised skills are needed, the auditor would seek the assistance of an expert possessing such skills, who may either be the auditor’s staff or an outside professional. If the use of such a professional is planned, the auditor should, in accordance with AAS 9, "Using the Work of an Expert", obtain sufficient appropriate audit evidence that the work performed by the expert is adequate for the purposes of the audit.

5. In accordance with the Auditing and Assurance Standard (AAS) 6 (Revised), "Risk Assessments and Internal Control", the auditor should obtain an understanding of the accounting and internal control systems sufficient to plan the audit and to determine the nature, timing and extent of the audit procedures. Such an understanding would help the auditor to develop an effective audit approach.

6. In planning the portions of the audit which may be affected by the CIS environment, the auditor should obtain an understanding of the significance and complexity of the CIS activities and the availability of the data for use in the audit. This understanding would include such matters as:

- the computer information systems infrastructure [hardware, operating system(s), etc. and application software(s) used by the entity, including changes therein since last audit if any],
- the significance and complexity of computerised processing in each significant accounting application. Significance relates to materiality of the financial statement assertions affected by the computerised processing. An application may be considered to be complex when, for example:
  - the volume of transactions is such that users would find it difficult to identify and correct errors in processing.
  - the computer automatically generates material transactions or entries directly to another application.
  - the computer performs complicated computations of financial information and/or automatically generates material transactions or entries that cannot be (or are not) validated independently.
  - transactions are exchanged electronically with other organisations [as in electronic data interchange (EDI) systems] without manual review for propriety or reasonableness.
- determination of the organisational structure of the client’s CIS activities and the extent of concentration or distribution of computer processing throughout the entity, particularly, as they may affect segregation of duties.
- determination of the availability of data. Source documents, computer files, and other evidential matter that may be required by the auditor may exist for only a short period or only in machine-readable form. Computer information systems may generate reports that might be useful in performing substantive tests (particularly analytical procedures). The potential for use of computer-assisted audit techniques may permit increased efficiency in the performance of audit procedures, or may enable the auditor to economically apply certain procedures to the entire population of accounts or transactions.

7. When the computer information systems are significant, the auditor should also obtain an understanding of the CIS environment and whether it may influence the assessment of inherent and control risks. The nature of the risks and the internal control characteristics in CIS environments include the following:

- Lack of transaction trails: Some computer information systems are designed so that a complete transaction trail that is useful for audit purposes might exist for only a short period of time or
only in computer readable form. Where a complex application system performs a large number of processing steps, there may not be a complete trail. Accordingly, errors embedded in an application’s program logic may be difficult to detect on a timely basis by manual (user) procedures.

- **Uniform processing of transactions:** Computer processing uniformly processes like transactions with the same processing instructions. Thus, clerical errors ordinarily associated with manual processing are virtually eliminated. Conversely, programming errors (or other systemic errors in hardware or software) will ordinarily result in all transactions being processed incorrectly.

- **Lack of segregation of functions:** Many control procedures that would ordinarily be performed by separate individuals in manual systems may become concentrated in a CIS environment. Thus, an individual who has access to computer programs, processing or data may be in a position to perform incompatible functions.

- **Potential for errors and irregularities:** The potential for human error in the development, maintenance and execution of computer information systems may be greater than in manual systems, partially because of the level of detail inherent in these activities. Also, the potential for individuals to gain unauthorised access to data or to alter data without visible evidence may be greater in CIS than in manual systems.

In addition, decreased human involvement in handling transactions processed by computer information systems can reduce the potential for observing errors and irregularities. Errors or irregularities occurring during the design or modification of application programs or systems software can remain undetected for long periods of time.

- **Initiation or execution of transactions:** Computer information systems may include the capability to initiate or cause the execution of certain types of transactions, automatically. The authorisation of these transactions or procedures may not be documented in the same way as that in a manual system, and management’s authorisation of these transactions may be implicit in its acceptance of the design of the computer information systems and subsequent modification.

- **Dependence of other controls over computer processing:** Computer processing may produce reports and other output that are used in performing manual control procedures. The effectiveness of these manual control procedures can be dependent on the effectiveness of controls over the completeness and accuracy of computer processing. In turn, the effectiveness and consistent operation of transaction processing controls in computer applications is often dependent on the effectiveness of general computer information systems controls.

- **Potential for increased management supervision:** Computer information systems can offer management a variety of analytical tools that may be used to review and supervise the operations of the entity. The availability of these analytical tools, if used, may serve to enhance the entire internal control structure.

- **Potential for the use of computer-assisted audit techniques:** The case of processing and analysing large quantities of data using computers may require the auditor to apply general or specialised computer audit techniques and tools in the execution of audit tests.

Both the risks and the controls introduced as a result of these characteristics of computer information systems have a potential impact on the auditor’s assessment of risk, and the nature, timing and extent of audit procedures.

8. While evaluating the reliability of the accounting and internal control systems, the auditor would consider whether these systems, inter alia:

(a) ensure that authorised, correct and complete data is made available for processing;

(b) provide for timely detection and correction of errors;

(c) ensure that in case of interruption in the working of the CIS environment due to power, mechanical or processing failures, the system restarts without distorting the completion of the entries and records;

(d) ensure the accuracy and completeness of output;

(e) provide adequate data security against fire and other calamities, wrong processing, frauds etc.;

(f) prevent unauthorised amendments to the programs; and

(g) provide for safe custody of source code of application software and data files.
9. The auditor should make an assessment of inherent and control risks for material financial statement assertions, in accordance with AAS 6 (Revised), "Risk Assessments and Internal Control".

10. The inherent risks and control risks in a CIS environment may have both a pervasive effect and an account-specific effect on the likelihood of material misstatements, as follows:

- The risks may result from deficiencies in pervasive CIS activities such as program development and maintenance, system software support, operations, physical CIS security, and control over access to special-privilege utility programs. These deficiencies would tend to have a pervasive impact on all application systems that are processed on the computer.
- The risks may increase the potential for errors or fraudulent activities in specific applications, in specific databases or master files, or in specific processing activities. For example, errors are not uncommon in systems that perform complex logic or calculations, or that must deal with many different exception conditions. Systems that control cash disbursements or other liquid assets are susceptible to fraudulent actions by users or by CIS personnel.

11. As new CIS technologies emerge for data processing, they are frequently employed by clients to build increasingly complex computer systems that may include micro-to-mainframe links, distributed data bases, end-user processing, and business management systems that feed information directly into the accounting systems. Such systems increase the overall sophistication of computer information systems and the complexity of the specific applications that they affect. As a result, they may increase risk and require further consideration.

12. In accordance with AAS 6 (Revised) "Risk Assessments and Internal Control"; the auditor should consider the CIS environment in designing audit procedures to reduce audit risk to an acceptably low level. He should make enquiries and particularly satisfy himself whether:

(a) adequate procedures exist to ensure that the data transmitted is correct and complete; and
(b) cross-verification of records, reconciliation statements and control systems between primary and subsidiary ledgers do exist and are operative and that accuracy of computer compiled records are not assumed.

13. The auditor's specific audit objectives do not change whether accounting data is processed manually or by computer. However, the methods of applying audit procedures to gather evidence may be influenced by the methods of computer processing. The auditor can use manual audit procedures, or computer-assisted audit techniques, or a combination of both to obtain sufficient evidential matter. However, in some accounting systems that use a computer for processing significant applications, it may be difficult or impossible for the auditor to obtain certain data for inspection, inquiry, or confirmation without computer assistance.

14. The auditor should document the audit plan, the nature, timing and extent of audit procedures performed and the conclusions drawn from the evidence obtained. In an audit in CIS environment, some of the audit evidence may be in the electronic form. The auditor should satisfy himself that such evidence is adequately and safely stored and is retrievable in its entirety as and when required.

15. This Auditing and Assurance Standard (AAS) becomes operative for all audits related to accounting periods beginning on or after 1st April 2003.

Compatibility with International Standard on Auditing (ISA) 401

The auditing standards established in this Auditing and Assurance Standard are generally consistent in all material respects with those set out in International Standard on Auditing (ISA) 401 on Auditing in a Computer Information Systems Environment except for the additional requirement related to "Documentation" [see paragraph 14]. ISA 401 does not contain any requirement related to documentation.