

EXPOSURE DRAFT
Standard on Internal Audit (SIA)
INTERNAL AUDIT IN AN INFORMATION
TECHNOLOGY ENVIRONMENT

Invitation to Comments

The Internal Audit Standards Board (hitherto known as the Committee on Internal Audit), of the Institute of Chartered Accountants of India invites comments on the Exposure Draft of the Standard on Internal Audit (SIA), *Internal Audit in an Information Technology Environment*. Comments are most helpful if they indicate the specific paragraph(s) to which they relate, contain a clear rationale and, where applicable, provide a suggestion for alternative wording.

Comments should be submitted in writing to:

Secretary, Internal Audit Standards Board,
The Institute of Chartered Accountants of India,
ICAI Bhawan,
C-1, Sector-1, Noida – 201 301.

*The last date for receiving comments is **January 29, 2009**. Comments can also be emailed at cia@icai.in.*

The following is the text of the Standard on Internal Audit (SIA), “Internal Audit in An Information Technology 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 Standards and Guidance Notes on Internal Audit”, issued by the Institute.

Introduction

1. The purpose of this Standard on Internal Audit (SIA) is to establish standards on procedures to be followed when an internal audit is conducted in an information technology (IT) environment. An information technology 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, and other types of information processing whether those computers are operated by the entity or by a third party. An IT system is a system that uses technology to capture, classify, summarize and report data in a meaningful manner to interested users, including an enterprise resource planning (ERP) system.

2. The overall objective and scope of an internal audit does not change in an IT environment. However, the use of a computer changes the processing, storage, retrieval and communication of financial information and the interplay of processes, systems and control procedures. This may affect the internal control systems employed by the entity. Accordingly, a IT environment may affect:

- a) the procedures followed by the internal auditor in obtaining a sufficient understanding of the processes, systems and internal control system; and
- b) the auditor's review of the entity's risk management and continuity systems.

3. The internal auditor should consider the effect of an IT environment on the internal audit engagement, *inter alia*, :

- a. the extent to which the IT environment is used to record, compile, process and analyse information; and**
- b. the system of internal control in existence in the entity with regard to:**
 - **the flow of authorised, correct and complete data to the processing centre;**
 - **the 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.**

Skills and Competence

4. **The internal auditor should have sufficient knowledge of the information technology systems to plan, direct, supervise, control and review the work performed.** The sufficiency of knowledge would depend on the nature and extent of the IT environment. **The internal auditor should consider whether any specialised IT skills are needed in the conduct of the**

audit, for example , the operating knowledge of a specialised ERP system. Specialised skills may be needed, for example, to:

- a) obtain sufficient understanding of the effect of the IT environment on systems, processes, internal control and risk management systems;
- b) design and perform appropriate tests of control and substantive procedures; and
- c) determine the effect of the IT environment on assessment of overall audit risk.

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

Planning

6. The internal auditor should obtain an understanding of the systems, processes, control environment, risk-response activities and internal control systems sufficient to plan the internal audit and to determine the nature, timing and extent of the audit procedures, in accordance with SIA 1 *Planning an Internal Audit*. Such an understanding would help the internal auditor to develop an effective audit approach..

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

- i) the information technology infrastructure [hardware, operating system(s), etc., and application software(s)] used by the entity, including changes, if any, therein since last audit.
- ii) the significance and complexity of computerised processing in each significant application. An application may be considered to be complex when, for example:
 - a) the volume and materiality of transactions is such that users would find it difficult to identify and correct errors in processing.
 - b) the computer automatically generates material transactions or entries directly to another application.
 - c) the computer performs complicated computations of financial information and/or automatically generates material transactions or entries that cannot be (or are not) validated independently.
 - d) transactions are exchanged electronically with other organisations [as in electronic data interchange (EDI) systems] without manual review for propriety or reasonableness.
- iii) determination of the organisational structure of the client's IT activities and the extent of concentration or distribution of computer processing throughout the entity, particularly, as they may affect segregation of duties.

iv) determination of the availability of data. Source documents, computer files, and other evidential matter that may be required by the internal auditor may exist for only a short period or only in machine-readable form. Information Technology 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 internal audit procedures, or may enable the auditor to economically apply certain procedures to the entire population of transactions.

8. When the information technology systems are significant, the internal auditor should also obtain an understanding of the IT environment and whether it influences the assessment of inherent and control risks. The nature of the risks and the internal control characteristics in IT environments include the following:

- a. *Lack of transaction trails* : Some IT 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.
- b. *Uniform processing of transactions*: Computer processing uniformly processes like transactions with the same processing instructions. Thus, the 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.
- c. *Lack of segregation of functions*: Many control procedures that would ordinarily be performed by separate individuals in manual systems may become concentrated in a IT environment. Thus, an individual who has access to computer programs, processing or data may be in a position to perform incompatible functions.
- d. *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 IT 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.
- e. *Initiation or execution of transactions*: Information Technology 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 information technology systems and subsequent modification.

- f. *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.
 - g. *Potential for increased management supervision:* IT 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.
 - h. *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 information technology systems have a potential impact on the internal auditor's assessment of risk, and the nature, timing and extent of audit procedures.

9. While evaluating the reliability of the internal control systems, the internal auditor should 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 IT 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.**

Risk Assessment

10. The internal auditor should make an assessment of inherent and control risks for material assertions related to significant processes and systems. These assertions apply to significant processes and systems for example - sales, procurement, inventory management, production, marketing, human resources, logistics .

11. The internal auditor should review whether the information technology system in the entity considers the confidentiality, effectiveness, integrity, availability, compliance and validity of data and information processed. The internal auditor should also review the effectiveness and safeguarding of IT resources, including – people, applications, facilities and data.

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

a. The risks may result from deficiencies in pervasive IT activities such as program development and maintenance, system software support, operations, physical IT 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 IT system.

b. 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 IT personnel

Audit Procedures

13. The internal auditor should consider the IT environment in designing audit procedures to review the systems, processes, controls and risk management framework of the entity.

Review of Information Technology Environment

14. The internal auditor should review the robustness of the IT environment and consider any weakness or deficiency in the design and operation of any IT control within the entity, by reviewing:

a) **System Audit reports of the entity , conducted by independent Information System auditors**

b) **Reports of system breaches , unsuccessful login attempts, passwords compromised, and other Exception reports**

c) **Reports of network failures, virus attacks and threats to perimeter security , if any**

d) **General controls like segregation of duties, physical access records, logical access controls**

e) **Application controls like input, output, processing and run-to-run controls**

f) **Excerpts from the IT Policy of the entity relating to business continuity planning, crisis management and disaster recovery procedures.**

An illustrative checklist of IT controls to be reviewed by the internal auditor is given in the Appendix to this Standard.

15. If the internal auditor is not able to rely on the effectiveness of the IT environment as a result of the review, he may perform such substantive testing or test of IT controls , as deemed fit

in the circumstances. **The internal auditor should apply his professional judgment and skill in reviewing the IT environment and assessing the interfaces of such IT infrastructure with other business processes.**

Outsourced Information Processing

16. The internal auditor should assess and review the reliance which the management of the entity places on the outsourced agency in case where such information processing has been outsourced to the outside party. The risks associated with such outsourced services should be considered by the internal auditor in light of the review of IT controls prevalent in such outside entity. The internal auditor should also review the extent to which the entity's controls provide reasonable assurance regarding the completeness, validity, reliability and availability of the data and information processed by such outsourced agency.

Documentation

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

Effective Date

18. This Standard on Internal Audit is applicable to all internal audits commencing on or after _____. Earlier application of the SIA is encouraged.

Appendices

Illustrative Information Technology controls to be reviewed during Internal Audit in an IT environment

Sr. No.	CONTROL PARAMETERS
	IT Access Control
1	There is a structured IT Policy and facility personnel are aware of the applicable policies.
	IT Back-up & Recovery
2	The network has adequately documented backup and recovery procedures/plans/schedules for critical sites.
3	LAN is supported by an uninterruptible power supply (UPS).
4	UPS tested in the last year (to test the batteries)?
5	For disaster-recovery purposes, LAN applications have been prioritized and scheduled for recovery based on importance to the operation.
	IT Environmental Controls
6	Smoke detection and automatic fire-extinguishing equipments installed for adequate functioning and protection against fire hazards
	IT Inventory
7	There is a complete inventory of the following: Hardware: Computers, File Servers, Printers, Modems, Switches, Routers, Hubs, etc. Software: all software for each Computer is logged with licenses and serial numbers.
8	There are written procedures for keeping LAN inventory. And they identify who (title) is responsible for maintaining the inventory report
9	Unused equipment is properly and securely stored
	IT Operations
10	LAN administrator has a backup person
11	LAN administrator monitors the LAN response time, disk storage space, and LAN utilization
12	LAN administrator is experienced and familiar with operation of the LAN facility
	IT Physical Security
13	Alarms installed at all potential entry and exist points of sensitive areas
	IT Service Agreements
14	Vendor reliability considered before purchasing LAN hardware and software
15	Service log maintained to document vendor support servicing
16	LAN hardware and software purchase contracts include statements regarding vendor support and licensing
	IT Virus Protection Policy

17

The level of virus protection established on servers and workstations is determined and the monitoring of infection are being done by IT administration. Virus Application should be updated on a monthly basis. Laptops if issued should be ensured to have secured internet access.