Standard on Internal Audit (SIA)
INTERNAL CONTROL EVALUATION

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), Enterprise Risk Management. *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 12, 2009****. Comments can also be emailed at* ***cia@icai.in.***

Contents

Introduction

1. The purpose of this Standard on Internal Audit is to establish standards and provide guidance on the procedures to be followed by the internal auditor in evaluating the system of internal control in an entity and for communicating weaknesses therein to those charged with governance.

Nature, Purpose and types of Internal Controls

2. Internal controls are a system consisting of specific policies and procedures designed to provide management with *reasonable assurance* that the goals and objectives it believes important to the entity will be met. "Internal Control System" means all the policies and procedures (internal controls) adopted by the management of an entity to assist in achieving management's objective of ensuring, as far as practicable, the orderly and efficient conduct of its business, including adherence to management policies, the safeguarding of assets, the prevention and detection of fraud and error, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information. The internal audit function constitutes a separate component of internal control with the objective of determining whether other internal controls are well designed and properly operated. Internal control system consists of interrelated components as follows:

- Control (or Operating) environment
- Risk assessment
- Control Objective setting
- Event identification
- Control activities
- Information and communication
- Monitoring
- Risk response

3. The system of internal control must be under continuing supervision by management to determine that it is functioning as prescribed and is modified, as appropriate, for changes in conditions. The internal control system extends beyond those matters which relate directly to the functions of the accounting system and comprises:

a. "*control environment*" means the overall attitude, awareness and actions of directors and management regarding the internal control system and its importance in the entity. The control environment has an effect on the effectiveness of the specific control procedures and provides the background against which other controls are operated. Factors reflected in the control environment include:

- The entity's organisational structure and methods of assigning authority and responsibility (including segregation of duties and supervisory functions).
- The function of the board of directors and its committees in the case of a company or the corresponding governing body in case of any other entity.
- Management's philosophy and operating style.
- Management's control system including the internal audit function, personnel policies and procedures.
- Integrity and ethical values
- Commitment to competence
- Board of directors or Audit committee
- Organizational structure
- Human resource policies and practices

b. "*control activities*" (or procedures) which means those policies and procedures in addition to the control environment which management has established to achieve the entity's specific objectives. Control activities include approvals, authorizations, verifications, reconciliations, reviews of performance, security of assets, segregation of duties, and controls over information systems.

4. Internal controls may be either preventive or Detective. Preventive controls attempt to deter or prevent undesirable acts from occurring. They are proactive controls that help to prevent a loss. Examples of preventive controls are separation of duties, proper authorization, adequate documentation, and physical control over assets. Detective controls attempt to detect undesirable acts**.** They provide evidence that a loss has occurred but do not prevent a loss from occurring. Examples of detective controls are reviews, analyses, variance analyses, reconciliations, physical inventories, and audits.

5. Internal controls are generally concerned with achieving the following objectives:

- Transactions are executed in accordance with management's general or specific authorisation.
- All transactions and other events are promptly recorded in the correct amount, in the appropriate accounts and in the proper accounting period so as to permit preparation of financial statements in accordance with the applicable accounting standards, other recognised accounting policies and practices and relevant statutory requirements, if any, and to maintain accountability for assets.
- Assets and records are safeguarded from unauthorised access, use or disposition.

- Recorded assets are compared with the existing assets at reasonable intervals and appropriate action is taken with regard to any differences.
- Systems and procedures are effective in design and operation.
- Risks are mitigated to a reasonable extent

6. Internal Control is a process. Internal control can be expected to provide only reasonable assurance, not absolute assurance. Internal control is geared to the achievement of *objectives*. Internal control is effected by *people* and not by policy manuals and forms alone.

Inherent Limitations of Internal Controls

7. Internal control systems are subject to some inherent limitations, such as:

- Management's consideration that the cost of an internal control does not exceed the expected benefits to be derived.
- The fact that most internal controls do not tend to be directed at transactions of unusual nature.
  The potential for human error, such as, due to carelessness, distraction, mistakes of judgement and the misunderstanding of instructions.
- The possibility of circumvention of internal controls through the collusion with employees or with parties outside the entity.
- The possibility that a person responsible for exercising an internal control could abuse that responsibility, for example, a member of management overriding an internal control.
- Manipulations by management with respect to transactions or estimates and judgements required in the preparation of financial statements.

Role of the Internal Auditor in Evaluating Internal Controls

8. The Internal auditor should examine and contribute to the ongoing effectiveness of the internal control system through evaluation and recommendations. However, the internal auditor is not vested with management's primary responsibility for designing, implementing, maintaining and documenting internal control. Internal audit functions add value to an organization's internal control system by bringing a systematic, disciplined approach to the evaluation of risk and by making recommendations to strengthen the effectiveness of risk management efforts. **The internal auditor should focus towards improving the internal control structure and promoting better corporate governance.** The role of the internal auditor encompasses:

- Evaluation of the efficiency and effectiveness of controls
- Recommending new controls where needed – or discontinuing unnecessary controls
- Using control frameworks
- Developing Control self-assessment

9. The internal auditor's evaluation of internal control implies:

- determining the significance and the sensitivity of the risk for which controls are being assessed;
- assessing the susceptibility to misuse of resources, failure to attain objectives regarding ethics, economy, efficiency and effectiveness, or failure to fulfil accountability obligations, and non-compliance with laws and regulations;
- identifying and understanding the design and operation of relevant controls;
- determining the degree of control effectiveness through testing of controls
- assessing the adequacy of the control design;
- reporting on the internal control evaluation and discussing the necessary corrective actions.

10. The broad areas of review by the internal auditor in evaluating the internal control system, *inter alia*, are :

- Mission, vision, ethical and organizational value-system of the entity
- Personnel allocation, appraisal system, and development policies
- Accounting and financial reporting policies and compliance with applicable legal and regulatory standards
- Objective of measurement and key performance indicators
- Documentation standards
- Risk management structure
- Operational framework
- Processes and procedures followed
- Degree of management supervision
- Information systems, communication channels
- Business Continuity and Disaster Recovery Procedures

11. **The internal auditor should obtain an understanding of the significant processes and internal control systems sufficient to plan the internal audit engagement and develop an**

effective audit approach. The internal auditor should use professional judgment to assess and evaluate the maturity of the entity's internal control. The auditor should obtain an understanding of the control environment sufficient to assess management's attitudes, awareness and actions regarding internal controls and their importance in the entity. Such an understanding would also help the internal auditor to make a preliminary assessment of the adequacy of the accounting and internal control systems as a basis for the preparation of the financial statements, and of the likely nature, timing and extent of internal audit procedures. The internal auditors assesses the 'as –is' internal control system within the organization .

12. **The internal auditor should obtain an understanding of the internal control procedures sufficient to develop the audit plan.** In obtaining this understanding, the internal auditor would consider knowledge about the presence or absence of control procedures obtained from the understanding of the control environment, business processes and accounting system in determining whether any additional understanding of control procedures is necessary. **The internal auditor should document and understand the design and operations of internal controls to evaluate the effectiveness of the control environment.** The important procedures to be adopted by the internal auditor for this purpose are:

- Narratives
- Flowcharts
- Questionnaires

13. When obtaining an understanding of the business processes, accounting and internal control systems to plan the audit, the internal auditor obtains a knowledge of the design of the internal control systems and their operation. For example, an internal auditor may perform a "walk-through" test that is, tracing a few transactions through the accounting system. When the transactions selected are typical of those transactions that pass through the system, this procedure may be treated as part of the tests of control.

14. **The internal auditor should consider the following aspects in the evaluation of internal control system in an entity:**

- **Ascertaining whether the entity has a mission statement and written goals and objectives.**
- **Assessing risks at the entity level.**
- **Assessing risks at the activity (or process) level.**
- **Completing a Business Controls worksheet for each significant activity (or process) in each function or department with documentation of the associated controls and their degree of effectiveness (partial or full); prioritizing those activities (or processes) which are most critical to the success of the function or department**

- **Ensuring that all risks identified at the entity and function or department level are addressed in the Business Controls worksheet along with the consolidated documentation of the operating controls.**
- **Ascertaining from the Business Controls worksheet, those risks for which no controls exist or existing controls are inadequate. This process is the stage of 'controls gap' analysis.**

Segregation of Duties

15. Segregation of duties is critical to effective internal control; it reduces the risk of both erroneous and inappropriate actions. **The internal auditor should ensure that in general, the approval function, the accounting/reconciling function, and the asset custody function is separated among employees of the entity**. **When these functions cannot be separated due to small department size, the internal auditor should ensure that a detailed supervisory review of related activities is in practice, as a compensating control activity**. Segregation of duties is a deterrent to fraud because it requires collusion with another person to perpetrate a fraudulent act.

Control Activities for Information Technology

16. In a computer information systems environment, the objectives of tests of control do not change from those in a manual environment; however, some audit procedures may change. The internal auditor may find it necessary, or may prefer, to use computer-assisted audit techniques. The use of such techniques, for example, file interrogation tools or audit test data, may be appropriate when the accounting and internal control systems provide no visible evidence documenting the performance of internal controls which are programmed into a computerised accounting system. There are two broad categories of information systems control - general control and application control. General control applies to all information systems-mainframe, minicomputer, network, and end-user environments. Application control is designed to cover the processing of data within the application software.

17. While evaluating the information technology controls in a system-driven environment, the internal auditor should determine whether the entity, *inter alia*, uses:

• encryption tools, protocols, or similar features of software applications that protect confidential or sensitive information from unauthorized individuals;

• back-up and restore features of software applications that reduce the risk of lost data;

• virus protection software;

• passwords that restrict user access to networks, data and applications.

18. The nature, timing and extent of the procedures performed by the internal auditor to obtain an understanding of the internal control systems will vary with, among other things:

- The size and complexity of the entity and of its information system.
- Materiality considerations.
- The type of internal controls involved.
- The nature of the entity's documentation of specific internal controls.
- The internal auditor's assessment of inherent risk.

19. Ordinarily, the internal auditor's understanding of the internal control systems significant to the audit is obtained through previous experience with the entity and is supplemented by:

a. inquiries of appropriate management, supervisory and other personnel at various organisational levels within the entity, together with reference to documentation, such as procedures manuals, job descriptions, systems descriptions and flow charts;

b. inspection of documents and records produced by the accounting and internal control systems;

c. observation of the entity's activities and operations, including observation of the organisation of computer operations, personnel performing control procedures and the nature of transaction processing.

Test of Controls

20. Tests of control are performed to obtain audit evidence about the effectiveness of the:

a. design of the internal control systems, that is, whether they are suitably designed to prevent or detect and correct material misstatements;

b. operation of the internal controls throughout the period.

c. Cost of a control vis a vis the benefit obtained from the same

21. Tests of control normally include:

- Inspection of documents supporting transactions and other events to gain audit evidence that internal controls have operated properly, for example, verifying that a transaction has been authorised.

- Inquiries about, and observation of, internal controls which leave no audit trail, for example, determining who actually performs each function and not merely who is supposed to perform it.
- Re-performance of internal controls, for example, reconciliation of bank accounts, to ensure they were correctly performed by the entity.
- Testing of internal control operating on specific computerised applications or over the overall information technology function, for example, access or program change controls.

22. **Based on the results of the tests of control, the internal auditor should evaluate whether the internal controls are designed and operating as contemplated in the preliminary assessment of control risk.** The evaluation of deviations may result in the internal auditor concluding that the assessed level of control risk needs to be revised. In such cases, the internal auditor would modify the nature, timing and extent of planned substantive procedures.

23. **The internal auditor should consider whether the internal controls were in use throughout the period.** If substantially different controls were used at different times during the period, the auditor would consider each separately. A breakdown in internal controls for a specific portion of the period requires separate consideration of the nature, timing and extent of the audit procedures to be applied to the transactions and other events of that period. The internal auditor would obtain audit evidence as to the nature, timing and extent of any changes in the entity's accounting and internal control systems since such procedures were performed and assess their impact on the auditor's intended reliance.

Monitoring Internal Audit findings

24. The internal auditor should identify internal control weaknesses that have not been corrected and make recommendations to correct those weaknesses. The internal auditor should document the rationale in deciding which audit recommendations should be followed up on and when, in contrast with recommendations where no follow-up is needed. The internal auditor should also follow up with management to document either that audit recommendations have been effectively implemented, or that senior management has accepted the risk of not implementing the recommendations.

Communication of continuing Internal Control weaknesses

25. When internal controls are found to contain continuing weaknesses, the internal auditor should consider whether:

- **Management has increased supervision and monitoring;**
- **Additional or compensating controls have been instituted; and/or**

- **Management accepts the risk inherent with the control weakness .**

26. The internal auditor should evaluate identified control deficiencies and then determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses. The auditor should communicate significant deficiencies and material weaknesses to management and those charged with governance. This communication includes significant deficiencies and material weaknesses identified and communicated to management and those charged with governance in prior audits but not yet remediated.

27. Some examples of common weaknesses in internal controls are:

- Corporate philosophy is understood but not written, open to misinterpretation;
- Roles and responsibilities are not explicit throughout the entity;
- Lack of performance appetite and understanding of the entity's appetite for risk taking;
- Management or boards do not receive the right information at the right time
- Disincentives exist which lead employees to behave in a dysfunctional manner.

28. As a result of obtaining an understanding of the internal control systems and tests of control, the internal auditor may become aware of weaknesses in the systems. **The internal auditor should make management aware, as soon as practical and at an appropriate level of responsibility, of material weaknesses in the design or operation of the internal control systems, which have come to the internal auditor's attention**. The communication to management of material weaknesses would ordinarily be in writing, as part of the internal audit report. However, if the internal auditor judges that oral communication is appropriate, such communication would be documented in the audit working papers. It is important to indicate in the communication that only weaknesses which have come to the internal auditor's attention as a result of the audit have been reported and that the examination has not been designed to determine the adequacy of internal control for management purposes.

29. The internal auditor in his report to the management, should provide:

- **A description of the significant deficiency or material weakness in internal control.**
- **His opinion on the possible effect of such weakness on the entity’s control environment.**

Effective Date

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