EXPOSURE DRAFT
Standard on Internal Audit (SIA)
ENTERPRISE RISK MANAGEMENT

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 for review of an entity's risk management initiatives during an internal audit or such other review exercise with the objective of providing an assurance thereon.

2. Enterprise risk management enables management to effectively deal with risk, associated uncertainty and enhancing the capacity to build value to the entity or enterprise and its stakeholders. Internal auditor may review each of these activities and focus on the processes used by management to report and monitor the risks identified.

Risk and Enterprise Risk Management

3. Risk is an event which can prevent, hinder, fail to further or otherwise obstruct the enterprise in achieving its objectives. A business risk is the threat that an event or action will adversely affect an enterprise's ability to maximize stakeholder value and to achieve its business objectives. Risk can cause financial disadvantage, for example, additional costs or loss of funds or assets. It can result in damage, loss of value and /or loss of an opportunity to enhance the enterprise operations or activities. Risk is the product of probability of occurrence and the financial impact of such occurrence.

4. Risk may be broadly classified into Strategic, Operational, Financial and Knowledge. *Strategic Risks* are associated with the primary long-term purpose, objectives and direction of the business. *Operations Risks* are associated with the on-going, day-to-day operations of the enterprise. *Financial Risks* are related specifically to the processes, techniques and instruments utilised to manage the finances of the enterprise, as well as those processes involved in sustaining effective financial relationships with customers and third parties. *Knowledge Risks* are associated with the management and protection of knowledge and information within the enterprise.

Process of Enterprise Risk Management and Internal audit

5. Enterprise Risk Management is a structured, consistent and continuous process of measuring or assessing risk and developing strategies to manage risk within the risk appetite. It involves identification, assessment, mitigation, planning and implementation of Risk and developing an appropriate Risk Response policy. Management is responsible for establishing and operating the risk management framework on behalf of the board.

6. The Enterprise Risk Management Process consists of Risk identification, prioritization and reporting, Risk mitigation, Risk monitoring and assurance**.** Internal audit is a key part of the lifecycle of risk management. The corporate risk function establishes the policies and procedures, and the assurance phase is accomplished by internal audit.

Role of the Internal Auditor in Relation to Enterprise Risk Management

7. The role of the internal auditor in relation to Enterprise Risk Management is to provide assurance to management on the effectiveness of risk management. **Due consideration should be taken to ensure that the internal auditor protects his independence and objectivity of the assurance provided**. The role of the internal auditor is to ascertain that risks are appropriately defined and managed.

8. The extent of internal audit's role in enterprise risk management will depend on other resources, internal and external, available to the board and on the risk maturity of the organisation. **The nature of internal audit's responsibilities should be adequately documented and approved by those charged with governance. The internal auditor should not manage any of the risks on behalf of the management or take risk management decisions. The internal auditor should not assume any accountability for risk management decisions taken by the management.** Internal audit has a role only in commenting and advising on risk management and assisting in the effective mitigation of risk.

9. The Internal Auditor has to review the structure, effectiveness and maturity of an enterprise risk management system and in doing so, should consider whether the enterprise has developed a Risk management policy setting out Roles and responsibilities and framing a Risk management activity calendar. **The Internal Auditor should review the maturity of an Enterprise Risk Management structure by considering whether the framework so developed*, inter alia*:**

a) Protects the enterprise against surprises

b) Stabilizes overall performance with less volatile earnings

c) Operates within established risk appetite

d) Protects ability of the enterprise to attend to its core business

e) Creates a system to proactively manage risks

10. The internal auditor would be responsible for the following activities:

a) Review of compliance to the enterprise risk management process with regard to the existing internal control systems and procedures followed.

b) Defining risk tolerances where none have been identified, based on internal auditor's

experience, judgment, and consultation with management.

c) Developing a detailed assurance calendar as a part of their annual audit plan and submit the review report to the Committee of the Board.

d) Reviewing key risk evaluation, assessment of exposure, recording and reporting.

e) Expanding assurance activities to cover overlooked risk areas.

f) Strengthen risk coverage of technology, fraud and strategic areas of significant importance and priority.

g) Coordinate with other risk and control functions to ensure that risks are efficiently managed and controlled.

h) Leveraging and identifying Key Risk Indicators (KRI) to effectively monitor risk conditions.

i) Reviewing whether Enterprise Risk Management structure is designed to identify opportunities to improve performance by taking maximum advantage of risk opportunities, focus on risk control/ risk transfer/ risk finance and exploit technological advantages.

j) Providing advice on the design, implementation and operation of control systems, identify opportunities to make control cost savings.

k) Reviewing and commenting on the extent of residual risk.

l) Promoting a risk and control culture within the enterprise.

11. The internal auditor should review whether the enterprise risk management coordinators in the entity report on the results of the assessment of key risks at the appropriate levels, which are, *inter alia*:

- **Risk management committee**
- **Enterprise Business and Unit heads**
- **Audit Committee**

Internal Audit plan and Risk Assessment

12. The internal auditor will normally perform an annual risk assessment of the enterprise, to develop a plan of audit engagements for the subsequent period. This plan will be reviewed at various frequencies in practice. This typically involves review of the various risk assessments performed by the enterprise (e.g., strategic plans, competitive benchmarking, etc.), consideration of prior audits, and interviews with a variety of

senior management. It is designed for identifying internal audit key areas, not to identify, prioritize, and manage risks directly for the enterprise. **The internal audit plan, which should be approved by the audit committee, should be based on risk assessment as well as on issues highlighted by the audit committee and senior management. The risk assessment process should be of a continuous nature so as to identify not only residual or existing risks, but also emerging risks. The risk assessment should be conducted formally at least annually, but more often in complex enterprises. To serve this objective, the internal auditor should design the audit work plan by aligning it with the objectives and risks of the enterprise and concentrate on those issues where assurance is sought by those charged with governance.**

13. The risk review and assurance process to be carried out by the internal auditor provides the assurance that there are appropriate controls in place for the risk management activities and that the procedures are understood and followed. Effective enterprise risk management requires a monitoring structure to ensure that the risks are effectively identified and assessed and that the appropriate mitigation plans are in place.

14. The review and assurance process conducted by internal auditors will help to determine, *inter alia*

a) The adopted measures results in what was intended;
b) The procedures adopted and information gathered for undertaking the assessment were appropriate;
c) Improved knowledge would help in reaching better decisions and identify what lessons should be learnt to improve future assessment and management of risks.

15. The internal auditor should submit his report to the Committee of the Board delineating the following information:

- **Assurance rating;**
- **Test conducted;**
- **Sample covered; and**
- **Detailed assurance comments.**

Effective Date

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