STANDARD ON INTERNAL AUDIT (SIA) 13
ENTERPRISE RISK MANAGEMENT

Contents

Paragraph(s)

Introduction 1-2

Risk and Enterprise Risk Management 3-4

Process of Enterprise Risk Management and Internal audit 5-6

Role of the Internal Auditor in Relation to Enterprise Risk Management 7-11

Internal Audit Plan and Risk Assessment 12-15

Effective Date 16

The following is the text of the Standard on Internal Audit (SIA) 13, *Enterprise Risk Management*, issued by the Institute of Chartered Accountants of India. The Standard should be read in the conjunction with the *"Preface to the Standards on Internal Audit"*, issued by the Institute.

In terms of the decision taken by the Council of the Institute at its 260th meeting held in June 2006, the following Standard on Internal Audit shall be recommendatory in nature in the initial period. The Standard shall become mandatory from such date as may be notified by the Council in this regard.

Introduction

1. The purpose of this Standard on Internal Audit is to establish standards and provide guidance on review of an entity's risk management system during an internal audit or such other review exercise with the objective of providing an assurance thereon. This Standard applies where the internal auditor has been requested by the management to provide such an assurance on the effectiveness of its enterprise risk management system.

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 of an event and the financial impact of such occurrence to an enterprise.

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. Operational 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.

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 given 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 scope of the internal auditor's work in assessing the effectiveness of the enterprise risk management would, normally, include:

   (a) assessing the risk maturity level both at the entity level as well as the auditable unit level;

(b) assessing the adequacy of and compliance with the risk management policy and framework; and

(c) for the risks covered by the internal audit plan:

(i) Assessing the efficiency and effectiveness of the risk response; and

(ii) Assessing whether the score of the residual risk is within the risk appetite.

9. The extent of internal auditor'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 auditor'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 auditor has a role only in commenting and advising on risk management and assisting in the effective mitigation of risk.

10. The internal auditor has to review the structure, effectiveness and maturity of an enterprise risk management system. In doing so, he 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 and;

e) creates a system to proactively manage risks.

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 and, not for identifing, prioritizing, and managing 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 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 process conducted by internal auditors will help to determine, *inter alia:*

    a) whether the adopted measures result in what was intended;

    b) whether the procedures adopted and information gathered for undertaking the assessment were appropriate; and

    Further, improved knowledge would help in reaching better decisions and identifying the lessons to improve future assessment and management of risks.

15. The internal auditor should submit his report to the Board or its relevant Committee, delineating the following information:

    - Assurance rating (segregated into High, Medium or Low) as a result of the review;
    - Tests conducted;
    - Samples covered; and
    - Observations and recommendations.

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.