Exposure Draft

Standard on Internal Audit (SIA) 150

Risk Management

The Internal Audit Standards Board of The Institute of Chartered Accountants of India (ICAI) invites comments on the draft Standard on Internal Audit (SIA) 150, Risk Management.

Comments are most helpful if they indicate relevant paragraph number, a clear rationale and, where applicable, provide a suggestion for alternative wording.

Comments can be submitted at link:
https://forms.gle/pVdUuaXZazbuLoWJ7

Last date for sending comments is October 23, 2025.

Standard on Internal Audit (SIA) 150

Risk Management**

Contents

This Standard on Internal Audit (SIA) 150, "Risk Management," issued by the Council of the Institute of Chartered Accountants of India (ICAI) should be read in conjunction with the "Preface to Standards on Internal Audit" issued by the Institute.

** Note: This Standard on Internal Audit (SIA) supersedes Standard on Internal Audit (SIA) 130 "Risk Management" issued in September 2022.

1. Introduction

1.1 Risk management is a critical component in ensuring that an organization identifies, assesses, mitigates, monitors and reports risks that could impact its objectives, including Strategic, financial, operational, compliance, and safeguarding of assets.

1.2 This Standard seeks to clarify the concept of Risk Management and also the responsibility of the Internal Auditor, Management and other Stakeholders with respect to risk management, keeping in mind, the legal, regulatory and professional obligations.

1.3 Definition of Internal Audit (Refer Para. 3.1 in the "Preface to the Standards on Internal Audit") and SIA 120, Terms of Internal Audit Engagement indicate providing independent assurance on the effectiveness of risk management processes as a basic expectation from internal audit. The definition on Internal Audit elaborates on the term "Risk Management" by clarifying how this is an integral part of management function and business operations.

1.4 Scope: This Standard applies to all internal audits and where risk management is subject of audit review and are being assessed, evaluated and reported upon.

2. Effective Date

2.1 This Standard is applicable for internal audits beginning on or after a date to be notified by the Council of the Institute.

3. Objectives

3.1 The objectives of this Standard are to:

(a) Provide a common terminology on risk, risk management and its framework to prevent ambiguity and provide clarity on the subject matter.

(b) To evaluate whether the organization has risk management framework & strategy in place that identifies and mitigates key risks (internal and external risks) on a continuous basis.

(c) To assess whether governance structures, including the Board of Directors and relevant Committees (such as Risk Committee

or audit Committee) are actively overseeing the risk management process to assess if risk management has been integrated into various organizational processes.

(d) Specify the requirements which need to be met to be able to provide an independent assurance of risk management framework in the organization under review.

4. Definition

4.1 Risk can be defined as a threat exploiting vulnerability of business assets or processes or controls by occurrence of an event which could prevent the organization from achieving its goals and objectives or which can significantly impact the business operations, internal controls and business continuity of the organization. Areas which can be impacted by risk are broadly classified into strategic, reputational, operational, financial, legal, environmental, etc.

4.2 Risk Management is a process with a series of steps, taken on a continuous basis to identify the threats and vulnerabilities, assess them for severity and likelihood, monitor risks, prioritize them for action and minimize their possible negative impact through mitigation actions.

4.3 Risk Management Framework is the combination of structure, systems and processes put in place to organise the various risk management activities and to integrate them seamlessly into the organisation. Risk management activities, forming part of the framework, are designed to enhance the organisation's ability to, amongst others:

(a) Provide strategy, leadership and direction on risk management.

(b) Establish a culture of risk awareness and management throughout the organisation.

(c) Provide an organisation structure for assigning risk management resources and defining their roles and responsibilities.

(d) Capture and maintain a comprehensive database of all risks with periodic updation of risk inventory.

(e) Ensure expertise and competence in the area of risk management.

(f) Exercise continuous monitoring and oversight on risk management.

(g) Identifying areas where Internal Control are weak or impaired, which leads high risk to the business.

(h) Categorise risk based on organisation's risk policy.

(i) Periodic communication of risk management matters and formal reporting of risk status to management and those charged with governance.

4.4 Enterprise Risk Management is a term used to refer to various risk management frameworks uniformly applied on an entity-wide basis towards a comprehensive approach to manage organisational risks. It usually involves a separate and dedicated risk management function or department, led by a (Chief) Risk Officer to support those charged with governance in achieving organisation objectives through risk management.

4.5 In the Standard on Auditing (SA) 315," Identifying and Assessing the Risks of Material Misstatements Through Undertaking the entity and Its Environment) issued by the ICAI, Business Risk is defined as follows:

"A risk resulting from significant conditions, events, circumstances, actions or inactions that could adversely affect an entity's ability to achieve its objectives and execute its strategies, or from the setting of inappropriate objectives and strategies."

5. Responsibility of the Board and Management4

5.1 The overall responsibility for developing, implementing and monitoring of risk management rests with the Board of Directors, risk management committee and Management and should be appropriately covered in the internal audit scope.

6. Responsibility of the Internal Auditor

6.1 Adoption of Risk-Based Internal Audit Approach (Refer Para. A1)

Unless specially excluded from the audit approach, the Internal Auditor shall plan and conduct risk based internal audits. This requires the application of risk management concepts to ensure that the audits are

prioritised in areas of urgency and importance, appropriate resources are allocated effectively where needed most, audit procedures are designed to give due attention to important matters and issues identified and reported are significant in nature.

6.2 Audit Procedures Based on Risk Management Maturity (Refer Para. A2)

The nature and extent of audit procedures to be conducted in risk management is dependent on the maturity of the risk management processes and the framework in place. Where management has implemented a risk management framework, the Internal Auditor shall plan and perform audit procedures to evaluate the design, implementation and operating effectiveness of the organisation's risk management framework to provide independent assurance to management and those charged with governance.

6.3 Audit Role in Absence of Formal Risk Management Framework (Refer Para. A3)

Where no formal risk management framework exists, the Internal Auditor shall design and conduct audit procedures with a view to highlight any exposures arising from weak or absent risk management activities, make recommendations to implement and strengthen related processes and thereby improve risk management and mitigation.

6.4 Assurance Engagements on Risk Management Framework (Refer Para. A4)

Where the independent assurance requires the issuance of an audit opinion over the design, implementation and operating effectiveness of risk management, this shall be undertaken in line with the requirements of SIA 120, "Terms of Internal Audit Engagement", especially with regard to the need to have a formal Risk Management Framework in place, which shall form the basis of such an assurance.

6.5 Limitation of Auditor's Role in Risk Management (Refer Para. A5)

The Internal Auditor shall not assume any responsibility to manage the risks or to execute risk management decisions. It is not the responsibility of the Internal Auditor to mitigate or resolve the risks.

****

Application and Other Explanatory Material

A1. Adoption of Risk-Based Internal Audit Approach (Refer Para. 6.1): The requirement to conduct audits on a risk-based approach underscores the principle that internal audit must focus its attention on areas of greatest importance to the achievement of organizational objectives. Unless specifically excluded, the internal auditor is expected to apply risk management concepts to prioritize internal audit activities, ensuring that urgent and high-risk areas receive greater coverage. This also facilitates efficient allocation of resources and ensures that audit findings are relevant, material, and add tangible value to governance and oversight processes. Standard on Internal Audit (SIA) 220, Internal Audit Planning emphasizes that internal audit planning may be in line with organizational risk.

A2. Audit Procedures Based on Risk Management Maturity (Refer Para. 6.2): The nature, depth, and extent of internal audit procedures are directly influenced by the maturity of the entity's risk management framework. Where a formal risk management system exists, the internal auditor must evaluate its design, implementation, and operating effectiveness to provide independent assurance to management and those charged with governance. This evaluation strengthens stakeholder confidence in the reliability of the organization's risk management processes. Standard on Internal Audit (SIA) 310, Reporting and Conformance with Standards on Internal Audit states that internal auditor must evaluate the effectiveness of the organization's risk management processes.

A3. Audit Role in Absence of Formal Risk Management Framework (Refer Para. 6.3): Where no formalized risk management structure exists, the internal auditor should adopt a proactive role by identifying potential exposures resulting from weak or absent processes. The auditor is expected to highlight such deficiencies, recommend appropriate measures for instituting a risk management framework, and assist management in enhancing overall risk culture through constructive recommendations. This approach not only mitigates immediate risks but also contributes to long-term organizational resilience.

A4 Assurance Engagements on Risk Management Framework (Refer Para. 6.4): Where management or the Board requires independent assurance in the form of an opinion over the adequacy and effectiveness of risk management practices, the internal auditor must conduct such an engagement strictly in accordance with SIA 120, *Terms of Internal Audit Engagement.* A formal risk management framework is a prerequisite for expressing such an opinion, as it provides the basis on which the auditor can evaluate design, implementation, and operating effectiveness. This ensures the opinion is both credible and defensible.

A5. Limitation of Auditor's Role in Risk Management (Refer Para. 6.5) It is essential to clearly delineate the responsibilities of the internal auditor vis-à-vis management. While the auditor may evaluate, recommend, and provide assurance on risk-related processes, the responsibility for risk ownership, management, and mitigation lies exclusively with management and the Board. The internal auditor must not assume operational responsibility for managing risks, as doing so would impair independence, objectivity, and assurance credibility.