Exposure Draft

Standard on Internal Audit (SIA) 160
Compliance with Laws and Regulations

The Internal Audit Standards Board of The Institute of Chartered Accountants of India (ICAI) invites comments on the draft Standard on Internal Audit (SIA) 160, Compliance With Laws and Regulations.

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/T7ekVvrRCucJJfPE8

Last date for sending comments is October 23, 2025.

Standard on Internal Audit (SIA) 160

Compliance with Laws and Regulations**

Contents

This Standard on Internal Audit (SIA) 160, "Compliance with Laws and Regulations" issued by the Council of the Institute of Chartered Accountants of India should be read in conjunction with the "Preface to the Standards on Internal Audit," issued by the Institute.

** Note: This Standard on Internal Audit (SIA) supersedes Standard on Internal Audit (SIA) 150, Compliance with Laws and Regulations was, originally, issued by the Board in September 2022 which was recommendatory in nature.

1

1. Introduction

1.1 Compliance with applicable laws and regulations is a fundamental pillar of sound governance and sustainable business operations.

1.2 This Standard seeks to clarify both the concept of compliance with laws and regulations and the responsibility of the Internal Auditor, Management and other Stakeholders, with respect to Compliance with Laws and Regulations (CLR), in line with their professional obligations.

1.3 Definition of Internal Audit in the "Preface to the Standards on Internal Audit" (Refer Para. 3.2) and SIA 120, Terms of Internal Audit Engagement indicate providing independent assurance on the effectiveness of internal controls and risk management processes to enhance governance and achieve organisational objectives as a key expectation from internal audit. This definition elaborates on the term Governance by clarifying how it includes "compliance with laws and regulations".

1.4 Scope: This Standard applies to all internal audits conducted where compliance activities and framework is subject matter of an audit, and is being assessed, evaluated and reported on by the Internal Auditor.

2. Effective Date

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

3. Objectives

3.1 The objective of this Standard is to:

(a) Provide a common terminology by defining compliance to prevent ambiguity or confusion on the subject matter.

(b) Explain the responsibilities of the Board of Directors and management with regard to compliance, as mandated by law and regulations, and

(c) Specify responsibilities of the Internal Auditor, especially, when providing independent assurance on the compliance framework.

4. Definition

4.1 Compliance is a term used to describe the process of following, in letter and spirit, the applicable laws and regulations, Standards and Guidelines, Policies and Procedures. Any act contrary to the laid down laws and regulations, either through omission or commission and performed intentionally or unintentionally, is a Non-Compliance (or violation) and may result in fines, penalties, litigation, reputational damage or other such consequences.

4.2 Compliance framework refers to the whole structure, systems and processes put in place to organize, implement and execute the various compliance activities and to integrate them seamlessly into the organization to provide strategy, leadership and direction on compliance.

4.3 Compliance activities forming part of the framework, that are designed to enhance the organisation's ability, includes to:

(a) Establish a culture of compliance throughout the organisation.

(b) Appointing Team and Leadership to effectively handle and monitor litigations and assessment issues arising out of compliances done and/or non-compliance in the organization.

(c) Provide an organisation structure for assigning compliance resources and defining their responsibilities.

(d) Capture and maintain a comprehensive database updated status of all compliance requirements.

(e) Encourage risk-based time prioritisation and effective completion of all compliance requirements.

(f) Ensure expertise and competence in the area of compliance.

(g) Initiate compliance programs and exercise continuous monitoring and oversight on compliance completion; including fixing responsibility for issues arising out of non-compliance and

(h) Periodic communication of compliance matters and formal reporting of compliance status and litigation status to management and those charged with governance.

5. Responsibility of the Board and Management

5.1 The responsibility of the Board of Directors in the area of compliance is generally established by the prevailing laws of the nation. The responsibility of the management is established by both the prevailing laws and the oversight of the Board of Directors.

5.2 Hence, compliance is seen as an essential element of business functioning, with severe consequences and penalties for non-compliance. Therefore, the overall responsibility for developing, implementing and monitoring the compliance framework rests with the Board of Directors and Management.

6. Responsibility of the Internal Auditor

6.1 **Auditing the Compliance Framework (Refer Para. A1)**

The nature and extent of internal audit procedures to be conducted in the area of compliance is dependent on the framework in place and the maturity of the processes. Where management has implemented a formal compliance framework, and unless specifically excluded from the audit scope (or technically not feasible), the Internal Auditor shall plan and perform internal audit procedures to evaluate the design, implementation and operating effectiveness of such framework to provide independent assurance to management and to those charged with governance.

6.2 **Auditing Compliance Activities and Processes (Refer Para. A2)**

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

6.3 **Independent Assurance over Compliance Framework (Refer Para. A3)**

Where the independent assurance requires the issuance of an audit opinion over the design, implementation and operating effectiveness over compliance, 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 compliance framework in place, which shall form the basis of such an assurance.

6.4 **Compliance Audit in the Absence of a Formal Compliance Framework (Refer Para. A4)**

While the primary objective of an internal audit is to enhance and strengthen the systems and processes of compliance. However, there may be instances where the Internal Auditor is specifically requested to undertake compliance audit assignments with the primary objective of identifying any instances of non- compliances. In such situations, and where no formal compliance framework exists, the Internal Auditor may not be able to provide a written opinion in line with requirements of SIA 120, Terms of Internal Audit Engagement. Never-the-less, the Internal Auditor may present a Summary of Findings highlighting any instances of non-compliance identified during the internal audit procedures.

These findings shall be reported along with the following:

- the scope, listing all the specific laws and regulations tested.
- audit procedures performed, sample selected, and population covered.
- summary of the work performed, and
- limitations, if any, on the responsibilities assumed by the internal Auditor, such as inherent limitations in sample selection, or that a court of law is the ultimate authority in establishing legal interpretation of non-compliance etc.

6.5 **Compliance related to Related Party Transactions (RPTs) (Refer Para. A5)**

Related Party transactions (RPTs) is a critical aspect of the overall governance structure. Internal auditors must ensure that RPTs are disclosed, reviewed, and approved in accordance with applicable laws such as the Companies Act, 2013 and SEBI (LODR) Regulations. RPTs compliance helps prevent conflicts of interest, ensures transparency in financial reporting, and protects shareholder value.

6.6 **Boundaries of the Internal Auditor's Role in Compliance (Refer**

Para. A6)

The Internal Auditor shall not assume any responsibility to manage or operate the compliance framework or to take compliance-related decisions. It is not the responsibility of the Internal Auditor to execute or resolve compliance-related risks.

****

Application and Other Explanatory Material

A1. Auditing the Compliance Framework (Refer Para. 6.1): Where there is a formal compliance framework in place, the work of the Internal Auditor shall be directed to ensure that, amongst others:

(a) The organisation has designed the framework consistent with best-in-class and globally recognised frameworks.

(b) The organisation has established and implemented various enabling mechanisms, including:

(i) Issuing compliance policies and implementing supporting procedures.

(ii) Setting the right "tone at the top" through constant leadership communication and supporting activities.

(iii) Designing a structured compliance framework, appointing designated compliance officers and assigning specifies responsibilities to identified compliance owners.

(iv) Identifying all laws and regulations applicable to the entity, creating and maintaining compliance database, assessing associated significant risks and embedding them into the relevant business processes.

(v) Conducting training programs regularly for compliance officers and owners, covering knowledge and competency for effective compliance.

(vi) Implementing robust compliance systems, deploying technology (where possible), monitoring their progress

and tracking their status, documenting timely completion with relevant proofs and artefacts and supporting timely escalations in case of slippages.

(vii) Tracking performance continuously against compliance targets and goals with sufficient reviews and oversight mechanisms.

(viii) Establishing timely communication and periodic reporting systems and protocols, including self- assessment and compliance certificates.

(c) The compliance system and processes in place operate in an effective and efficient manner and help to ensure full compliance.

Any shortcoming shall result in recommendations for improvement and suggestions on how to make the compliance framework more efficient and effective in line with stated objectives.

A2. Auditing Compliance Activities and Processes (Refer Para. 6.2): Where management has not implemented any formal compliance framework, the Internal Auditor will conduct audit procedures over various compliance related activities which may be present (similar to those indicated under Para. 6.2). These activities may be supported by certain enabling systems and processes (similar to those indicated under Para. 6.1) and which may be recommended as desirable actions to be undertaken to establish a formal framework.

A3. Independent Assurance over Compliance Framework (Refer Para. 6.3): In situation where a written assurance report is being issued, the Internal Auditor may consider the following to form his opinion:

(a) The linkage of the compliance framework with other frameworks like the Risk, Governance, Fraud, or Information Technology frameworks which may exist.

(b) The process in place of self-assessment and certification from compliance owners is part of a continuous system of compliance.

A4. Compliance Audit in the Absence of a Formal Compliance Framework (Refer Para. 6.4): In several organizations, a formal

compliance framework may not be in place. In such circumstances, management may request the Internal Auditor to undertake a compliance-focused assignment with the primary objectives of identifying instances of non-compliance. Since such an engagement does not involve the design or operation of a structured compliance system, the Internal Auditor is not in a position to provide a written assurance opinion as per SIA 110 "Terms of Internal Audit Engagement". In such cases, reports should be limited to a fact-based Summary of Findings. This report should clearly set out the scope of work, the specific laws and regulations tested, the audit procedures performed, the sample and population covered, and a summary of work carried out. It should also explicitly highlight the limitations of the exercise, such as inherent restrictions in sample testing and the principle that the final legal interpretation of compliance matters rests with the courts or regulators. The emphasis is on communicating factual observations rather than forming a legal or assurance opinion, thereby safeguarding the Internal Auditor from unintended liability or misinterpretation of the nature of the engagement.

A5. Compliance related to Related Party Transactions (RPTs) (Refer Para. 6.5): Related Party Transactions (RPTs) form an integral component of the corporate governance framework, as they directly impact transparency, accountability, and stakeholder confidence. It is the responsibility of internal auditors to verify that all RPTs are appropriately identified, disclosed, reviewed, and approved in strict compliance with applicable statutory provisions, including the Companies Act, 2013, and the SEBI (Listing Obligations and Disclosure Requirements) Regulations. Effective oversight of RPTs not only mitigates the risk of conflicts of interest but also enhances the credibility of financial reporting and safeguards the interests of shareholders by ensuring fairness in business dealings.

A6. Boundaries of the Internal Auditor's Role in Compliance (Refer Para. 6.6): The responsibilities of the Internal Auditor in the area of compliance are primarily independent assessment-oriented and must not extend into management or operational functions. Specifically, the Internal Auditor is not expected to act as a compliance officer, maintain or operate compliance monitoring systems, or take responsibility for compliance-related decisions. The Internal Auditor

may also avoid direct interaction with regulators or involvement in implementing or resolution of compliance risks. The role remains restricted to examining the adequacy and effectiveness of compliance framework, identifying gaps or deviations, and reporting them to those charged with governance. Any involvement beyond this scope and risks compromising the independence. Any involvement beyond this scope may impair the internal auditor's independence and objective. The responsibility for establishing and maintaining compliance ultimately rests with management, while the Internal Auditor's contribution is limited to providing an independent evaluation and highlighting areas requiring corrective action.