Exposure Draft
Standard on Internal Audit (SIA) 240
Use of Tools

The Internal Audit Standards Board of The Institute of Chartered Accountants of India (ICAI) invites comments on the draft Standard on Internal Audit (SIA) 240, Use of Tools.

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/t9kXu3jHZjGFtQDC8

Last date for sending comments is October 23, 2025.

Standard on Internal Audit (SIA) 240
Use of Tools

Contents

This Standard on Internal Audit (SIA) 240, "Use of Tools," 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.

1. Introduction

1.1 The growing complexity of business operations, coupled with rapid digital transformation and increased regulatory oversight has significantly enhanced the role of technological tools in internal audit engagements. Technological tools—including data analytics platforms, computer-assisted audit techniques (CAATs), visualization tools, and audit management software as well as emerging technologies such as Artificial Intelligence (AI) and Machine Learning (ML)—enable internal auditors to enhance the efficiency, accuracy, and relevance of their work.

1.2 This Standard provides a structured framework for:

- selection, application, evaluation, and documentation of tools used in internal audit assignment.
- ensuring audit quality and professional judgement remain paramount.

1.3 Scope: This Standard applies to all internal audit assignments.

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:

- Establish a structured and risk-responsive framework for the appropriate use of tools in internal audit.
- Enhance the quality of audit outcomes through the effective deployment of relevant technologies.
- Safeguard data integrity, confidentiality, and compliance with applicable laws while using tools.
- Encourage periodic review and improvement of tools to ensure relevance in dynamic organizational and technological environments.

4. Requirements

4.1 Planning for Use of Tools (Refer Para. A1)

- The internal auditor shall evaluate and record the proposed use of tools at the planning stage, ensuring their alignment with the risk assessment and defined audit objectives.
- Tool selection must consider engagement objectives, complexity of operations, system architecture, and data availability.

4.2 Validation of Tools (Refer Para. A2)

- Tools selected for use in internal audits must be evaluated for relevance, reliability, and security.
- The internal auditor shall validate that the outputs of such tools are complete, accurate, and aligned with audit objectives.

4.3 Competency and Training (Refer Para. A3)

- The audit team must possess the necessary competencies to effectively use selected tools.
- The Chief Internal Auditor shall ensure periodic training and upskilling of team to match evolving tool capabilities.

4.4 Data Security and Confidentiality (Refer Para. A4)

- The internal auditor shall ensure that tools comply with applicable data privacy and cybersecurity regulations.
- Where third-party tools are used, the internal auditor shall verify the existence of adequate confidentiality, ownership, and access controls.

4.5 Documentation and Audit Evidence (Refer Para. A5)

- The use of tools must be thoroughly documented, including rationale, configurations, testing parameters, and outcomes.
- Any limitations or constraints in tool application that affect the internal audit conclusion shall be disclosed.

4.6 Use of Professional Judgement (Refer Para. A6)

- The internal auditor shall not rely solely on automated outputs; professional skepticism and contextual evaluation must be applied to all tool-based findings.

4.7 Monitoring and Continuous Improvement (Refer Para. A7)

- The Chief Internal Auditor shall institute procedures for the periodic assessment of tools to evaluate their effectiveness and continued relevance to the audit function.
- Insights and lessons derived from each internal audit engagement shall be utilized to refine and enhance strategies for tool deployment.

****

Application and Other Explanatory Material

A1. Planning for Use of Tools (Refer Para. 4.1):

- The decision to use tools should be aligned with risk-based audit planning.
- Tools may be most relevant where large volumes of transactions exist or where automation can detect trends, anomalies, or exceptions.

A2. Validation of Tools (Refer Para. 4.2):

- Analytical platforms such as IDEA, ACL, Power BI, Python scripts, and AI-based applications shall be subject to validation to ensure reliability and integrity in data processing.
- Trial runs, benchmarking against known outcomes, and cross-validation with manual procedures help to ensure reliability.

A3. Competency and Training (Refer Para. 4.3):

- Internal audit teams should be trained on using audit-specific features such as filter logic, power BI, pattern detection, pivot analysis, and scripting for automation.
- Continuing education plans should include refresher modules on tool updates and integration techniques.

A4. Data Security and Confidentiality (Refer Para. 4.4):

- Internal auditors shall ensure that the use of tools complies with applicable regulatory, security, and data protection frameworks such as ISO 27001, General Data Protection Regulation (GDPR), Digital Personal Data Protection (DPDP) Act 2023, NIST Cybersecurity Framework, and any other relevant national or international standards.

- Confidentiality agreements with vendors and internal access controls are essential when using cloud-based or third-party tools.

A5. Documentation and Audit Evidence (Refer Para. 4.5):

- Audit workpapers should include:
  - Purpose and scope of tool usage.
  - Inputs and configuration parameters.
  - Screenshots of queries, dashboards or reports.
  - Commentary on interpretations and audit conclusions.
- Exceptions, limitations, and assumptions must be clearly noted.

A6. Use of Professional Judgement (Refer Para. 4.6):

- Anomalies identified by tools must be investigated further through sampling, walkthroughs, or corroborative procedures.
- Internal auditors should avoid over-reliance on tools and remain alert to limitations such as missing data, outdated algorithms, or contextual misinterpretation.

A7. Monitoring and Continuous Improvement (Refer Para. 4.7):

- Post-audit reviews should assess:
  - Whether the tools met their intended objectives.
  - Feedback from internal audit team on ease of use and challenges.
  - Opportunities for upgrades or replacement of outdated systems.
- A centralized tool registry, version control, and usage logs can enhance governance.