

Assessment Domain Methodology



Active Builder

The internal audit function is in the process of improving alignment with global standards, organizational strategies, and stakeholder expectations, but progress is still ongoing. Methodologies and processes are under consideration or implementation, but consistency and full integration are yet to be achieved.

Efforts are being made to implement surveys, interviews, or workshops, but they are not yet fully functional.

Required Action Steps

Focus should be on finalizing methodology implementation, improving foresight capabilities, enhancing stakeholder engagement, and ensuring audit strategies align with organizational goals.

1- Foresight Integration

- Ensure that foresight (predicting and preparing for future risks and opportunities) is considered in every audit engagement. This means auditing not just current risks but also emerging risks (e.g., technological changes, regulatory updates, economic shifts).
- Introduce scenario analysis, future-focused risk assessments, and environmental scanning into audit planning. Use tools like predictive analytics and risk dashboards to help auditors identify potential future risks.

2- Alignment with Organization Priorities

- Finalize the alignment of the internal audit strategy with the organization's broader strategy. Ensure that audit priorities reflect the company's growth plans, risk appetite, and industry trends.
- Conduct workshops with senior management and the board to understand strategic goals and expectations.
- Establish a mechanism for periodic (e.g., quarterly or bi-annual) review of the internal audit strategy to ensure it remains aligned with any changes in the organization's direction.

IMPACT DRIVEN GOVERNANCE

3- Compliance with Global Standards

Complete the development and rollout of the internal audit methodology according to global internal audit standards. Ensure auditors are trained to use the methodology effectively.

Conduct internal workshops and training to communicate the methodology and set up a compliance tracking system. Integrate the methodology into the audit process through standardized templates, checklists, and tools.

Implement a quality assurance program to periodically assess whether audits are conducted according to the methodology.

4- Non-Conformance

Finalize and implement a formal procedure where the CAE documents any instances of non-conformance with internal audit standards (e.g., due to regulatory restrictions, resource constraints) and communicates this to senior management or the board.

Develop a template for documenting non-conformance, including alternative actions taken, reasons for non-compliance, and potential impacts on the audit. Ensure this documentation is communicated through formal reports to the audit committee.

5- Identification of Fraud Risk

Fully implement a system for gathering input on fraud and risks from internal stakeholders (e.g., through surveys, workshops, or interviews). This will ensure that the internal audit function has a comprehensive understanding of potential risks.

Establish a regular schedule (e.g., annually or bi-annually) to conduct these surveys and workshops with key stakeholders, including department heads, risk owners, and employees.

Use the insights gained from these sessions to inform the audit plan and refine risk assessments.

6- Training

Implement an ongoing training program for internal auditors to ensure they are up to date with the latest audit methodology and standards. This includes both formal training sessions and informal knowledge-sharing activities.

Establish a calendar of training sessions (quarterly or bi-annually) where auditors are refreshed on key methodologies, audit tools, and new regulations. Use case studies, role-playing, and external training where necessary.

7- Information Access

Complete the implementation of controls that restrict access to sensitive information. Ensure data is classified properly and access rights are granted only to authorized personnel.

Implement tools like encryption, access control lists, and multi-factor authentication. Ensure that access is regularly reviewed and updated as needed.

Regularly audit these controls to ensure they are effective and remain compliant with data protection regulations.