Assessment Domain Methodology

Prime Initiator

Internal audit function is fully aligned with global internal audit standards, governance frameworks, and organizational strategies. Processes are well established, and methodologies are consistently updated to provide assurance, insight, and foresight.

A robust mechanism is in place, ensuring that any deviations from standards are documented and communicated with alternative actions.

Required Action Steps

Priority is to maintain alignment with global standards, continuously improve processes, engage stakeholders for risk insights, and uphold robust information access controls to sustain excellence in internal audit performance.

1- Foresight Capabilities

- Strengthen the foresight capability by utilizing advanced data analytics, machine learning, and trend analysis to predict emerging risks (cybersecurity, regulatory changes, market shifts). Ensure that auditors are equipped with tools and skills to not only respond to current risks but also anticipate and mitigate future risks.
- Invest in audit technology platforms that provide predictive analytics capabilities. Incorporate periodic environmental scanning and scenario planning as part of the audit planning process.

2- Alignment with Strategy

- Maintain alignment by conducting annual strategic alignment reviews. As the organization evolves (e.g., entering new markets, adopting new technologies), ensure the internal audit strategy remains flexible and adjusts accordingly.
- Schedule an annual strategy review session between the internal audit team and senior management to reassess the alignment of audit priorities with the company's strategic objectives.

Riyadh:
Office 1402, King Abdullah Financial District, Al Aqiq, Riyadh 13519

UK
3 Deneside, Great Yarmouth, England NR 30 2HL

Pakistan
668 Street 42 Main Double Rd, NPF MPCHS E 11/3 E-11

3- Conformance with Global Standards

Conduct periodic reviews of the internal audit methodology to incorporate any updates to global standards or best practices. Ensure the methodology evolves to meet the needs of the organization and global trends.

Establish a review committee to evaluate the methodology annually and benchmark against leading practices. This review should consider evolving global standards (e.g., changes to IIA standards) and technological advancements (e.g., audit automation tools).

Develop a proactive monitoring system to continuously identify any potential conflicts between global standards and local regulations. This ensures that the organization is always compliant and ahead of regulatory changes.

Use an audit management software that tracks any instances of non-conformance and automatically flags them for review. Ensure that these instances are discussed during audit committee meetings.

4- Stakeholder Engagement

Enhance stakeholder engagement by involving external stakeholders (e.g., suppliers, customers) in fraud and risk workshops. This will provide a broader perspective on potential risks.

Organize workshops that include key external partners who may have insights into potential risks (e.g., supply chain vulnerabilities, market changes). Use these inputs to adjust the risk assessment process.

5- Training

Expand the training program to include more advanced auditing techniques, such as cybersecurity audits, data analytics, and ESG (environmental, social, governance) audits.

Develop specialized training modules that focus on emerging risks, audit automation, and the use of technology in audits. Partner with external training providers to ensure auditors stay up-to-date.

6- Benchmarking

Continuously benchmark the organization's governance and risk management maturity against global best practices. Identify areas for improvement and implement targeted enhancement projects.

Use industry-standard maturity models (e.g., COSO or ISO frameworks) to periodically assess governance and risk management processes. Implement improvement initiatives based on the assessment results, focusing on areas like IT governance or data protection.

7- Data Security

Continuously strengthen data security controls by implementing the latest cybersecurity measures (e.g., encryption, AI-driven threat detection). Regularly test these controls through security audits and penetration testing.