

20
25

Risk Management

Evolving Internal Audit for Strategic Impact

“Transforming Risk Into Opportunity – Internal Audit for the Future”

Volume II

Risk Management

Internal Audit 2025

Aligning with New Global Standards and Emerging Risks for 2025

Insights Publication Timeline:



Introduction to A New Era for Internal Audit

The 2024 Global Internal Audit Standards mark a pivotal shift in the internal audit profession, prioritizing strategic alignment, agility, and risk foresight. For auditors, this means moving beyond traditional compliance checks to become active contributors in organizational risk management.

Internal auditors are now expected to contribute to enterprise risk discussions, integrate emerging risks into their work, and operate with agility and foresight. This evolution is especially crucial for organizations navigating Saudi Arabia's ambitious Vision 2030 initiatives.

This publication explores how internal audit functions can embrace Risk Management week 2.

We'll discuss integrating Enterprise Risk Management (ERM), evaluating emerging risks such as cybersecurity, ESG, and AI, and tailoring audit strategies to local complexities — all through the lens of the new IIA standards.

At Insights, we help clients evolve their audit functions to meet these new expectations through tailored strategies, tools, and advisory support.

Three Key Pillars

Strategic Role Elevation:

Internal audit is no longer a back-office function. It is now positioned as a critical advisor supporting governance, risk strategy, and performance enhancement.

Risk-Driven Agility:

Audit plans must be dynamic and responsive, continuously aligned with evolving risk profiles and business priorities.

Vision 2030 Alignment:

With transformational programs and giga projects underway, Saudi companies must align internal audit practices to national goals, regulations, and market shifts.

Emphasis on Risk Management in the 2024 IIA Standards

The 2024 IIA Global Internal Audit Standards place risk management at the center of internal audit strategy. Auditors are now required to assess not just controls, but also how organizations identify, manage, and respond to risks — including those emerging in real-time.

This change empowers audit functions to proactively guide leadership through uncertainty, while ensuring alignment with global governance expectations and regulatory demands.

Mandatory Risk-Based Planning

Internal auditors must now build audit plans from documented, regularly updated risk assessments tied to strategy and objectives.

Stronger Role in Risk Oversight

Auditors are expected to evaluate the effectiveness of risk management processes and offer insight into strategic and emerging risks.

Collaboration Across Risk Lines

The standards promote coordination with ERM, compliance, and operational risk functions to ensure full coverage of the organization's risk landscape.

These updates signal a shift from static, checklist-driven audits to a dynamic, enterprise-wide risk perspective. For Saudi organizations, adapting internal audit to this model is essential for regulatory readiness, strategic alignment, and long-term resilience.

Integrating Enterprise Risk Management (ERM) into Internal Audit

The 2024 IIA Standards emphasize that internal audit should be closely aligned with Enterprise Risk Management (ERM) to ensure comprehensive, proactive assurance across all levels of the organization.

This integration empowers internal audit to support decision-making, strengthen governance structures, and remain agile in response to emerging risks. Internal audit must both leverage and evaluate ERM — enabling smarter audit planning and identifying organizational blind spots before they materialize.

The 2024 IIA Standards Support Stronger ERM-Audit Integration:	
Risk-Aligned Planning	Use ERM tools — such as the risk register, heatmaps, and risk appetite statements — to prioritize high-risk areas and shape the annual audit plan. This ensures audit efforts are tied to what truly threatens strategic objectives.
ERM Effectiveness Reviews	Internal audit is expected to independently assess the maturity, design, and operational effectiveness of ERM frameworks. Weaknesses must be reported, and audit recommendations can drive continuous improvement.
Coordinated Assurance Across the 3 Lines	Auditors should work in harmony with compliance, legal, IT security, and risk owners to coordinate risk coverage and avoid duplication — a core principle of the IIA’s Three Lines Model.
Advisory Role — Without Compromising Independence	The standards allow audit to support ERM implementation by advising on frameworks, facilitating workshops, and sharing insights — as long as it does not own risk decisions.
Real-Time Risk Intelligence	By integrating with ERM dashboards and Key Risk Indicators (KRIs), audit functions can adjust focus areas mid-cycle, enabling agile audits that respond to fast-changing risks.

This integrated approach not only aligns with the IIA’s Three Lines Model but also strengthens audit's ability to act as a strategic advisor. In Saudi Arabia, where Vision 2030 has accelerated risk complexity, ERM-audit synergy is essential to supporting giga projects, digital transformation, and regulatory reform.

ERM integration enables continuous risk sensing and forward-looking assurance — precisely the direction emphasized by the 2024 IIA Standards. Within the context of Saudi Arabia’s Vision 2030 and the execution of large-scale giga projects, close alignment between ERM and internal audit ensures that high-risk national initiatives receive the oversight they demand. Internal audit plays a critical role as a second layer of validation, independently confirming whether management’s risk treatments are effective and aligned with strategic goals.

Evaluating Emerging Risks

To become proactive strategic partners, internal audit teams must align closely with Enterprise Risk Management (ERM). This integration enhances visibility into top risks and strengthens audit focus on what matters most.

When ERM and internal audit operate in sync, organizations gain better oversight, reduce duplication, and improve their ability to respond to uncertainty. Insights helps clients develop emerging risk audit programs — including ESG audit frameworks, cybersecurity readiness, and AI governance assurance. Here are the key emerging risks highlighted below:

Key Emerging Risks Requiring Audit Attention		
Risk Category	Why It Matters	Audit Focus
Cybersecurity	With escalating digital threats and increased regulatory scrutiny, internal audit must assess the organization's cybersecurity posture.	<ul style="list-style-type: none">• Governance structures and board oversight of cyber risk• Alignment with NIST Cybersecurity Framework or ISO 27001• Incident response readiness and cyber incident logging• Third-party cyber risk and access control audits
Environmental, Social, and Governance (ESG)	As ESG disclosures become mandatory and investor expectations increase, audit must validate the quality and reliability of ESG data and programs.	<ul style="list-style-type: none">• ESG reporting accuracy and data traceability (e.g. GRI, SASB frameworks)• Climate risk integration into enterprise risk assessments• Anti-bribery, labor standards, and diversity program compliance• Greenwashing risks in public ESG statements
Artificial Intelligence (AI)	The rise of AI in decision-making brings risks related to bias, explainability, and compliance. Internal audit must ensure responsible AI governance is in place.	<ul style="list-style-type: none">• Validation and testing of machine learning models• Data privacy and source integrity for training data• Bias and fairness controls in automated decisions• Alignment with ethical AI principles and upcoming regulations
Data Privacy & Protection	Stricter regulations (e.g., GDPR-like laws) and growing data-driven operations.	<ul style="list-style-type: none">• Compliance with data regulations• Data handling processes• Breach prevention• Privacy governance
Digital Transformation	Accelerated adoption of cloud, automation, and emerging tech.	<ul style="list-style-type: none">• IT change management• Vendor risks• Cloud governance• Tech investment assurance
Third-Party & Supply Chain Risk	Reliance on external partners increases vulnerability to disruption and misconduct.	<ul style="list-style-type: none">• Due diligence• Monitoring• Contract compliance• Cyber/vendor risk frameworks
Financial Resilience	Inflation, interest rate shifts, and economic volatility impact solvency and planning.	<ul style="list-style-type: none">• Liquidity risk,• Scenario planning• Stress testing of financial assumptions and controls

KSA-Specific Risk Factors: Vision 2030, Giga Projects, and Regulatory Risks

Saudi Arabia's transformation under Vision 2030 introduces a unique and dynamic risk environment. As public and private sectors undergo rapid change, internal audit functions must adapt to oversee new types of strategic, operational, and compliance risks.

01

Vision 2030 Transformation

Vision 2030 represents a nationwide push toward economic diversification, digitalization, and privatization. This introduces transformation risks across all sectors. Internal audit must ensure that governance structures support these strategic shifts and that programs are being executed with clear controls, measurable outcomes, and transparent accountability. Auditors should assess the alignment of internal initiatives with Vision 2030 objectives and evaluate whether key transformation projects are achieving their intended impact.

02

Giga Projects Oversight

Giga projects such as NEOM, Qiddiya, and The Red Sea Project are multi-billion-dollar national investments that carry significant execution risk. These projects are complex, long-term, and involve multiple stakeholders — both public and private. Internal audit functions must provide independent oversight over project governance, procurement, contractor performance, risk mitigation plans, and milestone delivery. Ensuring that these initiatives are managed efficiently and ethically is critical to maintaining public trust and attracting global investment.

03

Regulatory Compliance and Reform

Saudi Arabia's regulatory landscape is rapidly evolving. Authorities like the Capital Market Authority (CMA), the Saudi Central Bank (SAMA), and the Digital Government Authority (DGA) are issuing new requirements related to ESG reporting, data protection, cybersecurity, and internal controls. Internal audit must stay up to date with these developments, assess organizational readiness for compliance, and help identify and close regulatory gaps before enforcement actions occur. In this new era of reform, internal audit plays a pivotal role in ensuring governance maturity and credibility.

04

Emerging Risk Readiness

The pace of change in Saudi Arabia brings not only opportunity but also volatility. With increased reliance on technology, artificial intelligence, and digital infrastructure, organizations face emerging risks that are often under-assessed. Internal audit functions must help organizations identify and prepare for these risks before they materialize. This includes evaluating the organization's ability to manage cyber threats, ESG exposure, AI governance, and geopolitical uncertainty. Proactive scenario planning and horizon scanning are essential tools to future-proof the audit approach.

05

Stakeholder Confidence and Accountability

As Saudi Arabia positions itself as a global economic and innovation hub, the role of internal audit in maintaining transparency and accountability becomes even more crucial. Stakeholders — including government bodies, investors, and the public — expect high standards of ethics, performance monitoring, and risk assurance. Internal auditors must reinforce ethical culture, support transparent reporting, and provide clear, actionable insights to boards and audit committees. Their work will directly influence organizational credibility and the success of national-level programs.

Building an **Agile, Risk-Based Audit Plan**

To comply with the 2024 IIA Standards and respond effectively to a rapidly changing risk environment, internal audit functions must adopt an agile, risk-based approach. This transformation enables timely assurance, strategic alignment, and greater responsiveness to emerging threats.

At Insights, we design and implement agile audit planning models tailored to your risk profile and organizational strategy.

01 Planning Must Be Risk-Aligned and Dynamic

The audit plan must be driven by current enterprise risks, not by legacy schedules. This requires:

- Aligning audits with strategic priorities and risk appetite
- Updating the risk assessment regularly (e.g., quarterly)
- Reallocating audit resources as risks evolve
- Prioritizing high-impact areas rather than evenly distributing efforts

02 Agility Requires Flexible Tools and Collaboration

To support agile planning and execution, audit teams must:

- Leverage data analytics and real-time dashboards for risk sensing
- Use continuous auditing tools to monitor controls dynamically
- Collaborate with ERM, compliance, and business units to share insights
- Maintain an audit backlog that can be reshuffled as needed

03 Audit Plans Must Enable Strategic Value

To support agile planning and execution, audit teams must:

- Leverage data analytics and real-time dashboards for risk sensing
- Use continuous auditing tools to monitor controls dynamically
- Collaborate with ERM, compliance, and business units to share insights
- Maintain an audit backlog that can be reshuffled as needed

Transforming Audit Planning for a Dynamic Risk Environment

As business models shift and regulatory expectations rise, audit functions must abandon static annual plans in favor of dynamic, risk-responsive strategies. The 2024 IIA Standards reinforce the importance of planning that evolves in real time, supports enterprise objectives, and adapts quickly to disruption. In Saudi Arabia, where Vision 2030 initiatives demand transparency and agility, internal audit must modernize its planning approach to stay relevant and valuable.

Strategic Alignment as the Foundation

Planning begins with a clear line of sight to the organization's mission, priorities, and risk appetite. Internal audit must focus on areas of strategic significance, ensuring that resources are not spread thin but concentrated where risk exposure is greatest and where value can be added.

STEP 01

Responsive, Not Rigid

Effective audit planning is fluid. Risks evolve quickly — from new regulations to sudden cyber threats. Audit plans should be reviewed frequently, with clear mechanisms to reprioritize and reallocate resources. Flexibility in execution ensures internal audit can pivot when needed without sacrificing quality or independence.

STEP 02

Data-Driven Planning with Technology

Analytics and automation allow internal auditors to monitor risk indicators continuously. From dashboards to predictive models, these tools provide insights that inform smarter planning decisions and more timely interventions. Technology isn't a supplement — it's the engine of agile audit planning.

STEP 03

Risk Intelligence through Collaboration

Internal audit cannot plan in isolation. Ongoing collaboration with ERM, compliance, and functional leaders ensures audit priorities reflect the real-time risk landscape. Participating in enterprise risk forums and contributing to strategic risk dialogue enhances the plan's accuracy and relevance.

STEP 04

Ongoing Calibration for Maximum Impact

A forward-looking audit plan must be iterative. Regular reassessment based on stakeholder feedback, external developments, and internal changes is critical. Audit leaders should be ready to add, drop, or reframe engagements to maintain alignment with business risk and deliver lasting value.

Why It Matters Now

The internal audit profession is shifting — and standing still is no longer an option. With the 2024 IIA Standards in effect and Vision 2030 accelerating regulatory reform and public scrutiny, organizations must act quickly to modernize audit functions.

Audit functions that evolve now will be tomorrow's strategic advisors.

01

The new standards are live — legacy frameworks risk non-compliance.

02

Vision 2030's high-profile initiatives demand stronger governance and audit oversight.

03

ESG, cyber, and AI risks require new expertise and assurance strategies.

04

Investors, regulators, and boards now expect internal audit to deliver strategic insight — not just findings.



How Can Insights Help

At Insights Financial Management & Consultancy, we don't just inform — we help transform. Our advisory services are designed to help internal audit functions evolve from control-focused to strategy-driven, fully aligned with the 2024 IIA Standards and Saudi Arabia’s Vision 2030 objectives.

Transformation Pathway



Contacts Us

For further information, clarification and discussion concerning the contents, please contact

Khawaja Soha Butt

Partner - Financial & Risk Advisory

✉ : sbutt@insightss.co

Ehtesham Malik

SVP - Financial & Risk Advisory

✉ : emalik@insightss.co

Nicholas Whitford

SVP – Business Growth

✉ : nwhitford@insightss.co



Riyadh Office :

107 Legend Tower,
King Fahd Road, Riyadh - KSA.

Jeddah Office :

Royal Plaza, Prince Sultan Street,
Jeddah 23615 - KSA.

Dubai Office :

Office 711, Iris Bay Building,
Business Bay, Dubai - UAE.

UK Office :

37th Floor, 1 Canada Square,
London E14 5AA

Adelaide Office :

P.O. Box 6387, Halifax Street,
Adelaide South Australia 5000

New York Office :

14, Wall Street, 20th Floor,
New York 10005 USA.

Insights

☎ : +966 53 963 3882

☎ : + 966 11 2930 665

✉ : info@insightss.co

🌐 : www.insightss.co