insights

Cyber Threats

& AI Risks: Is Your Internal Audit Ready?

2025

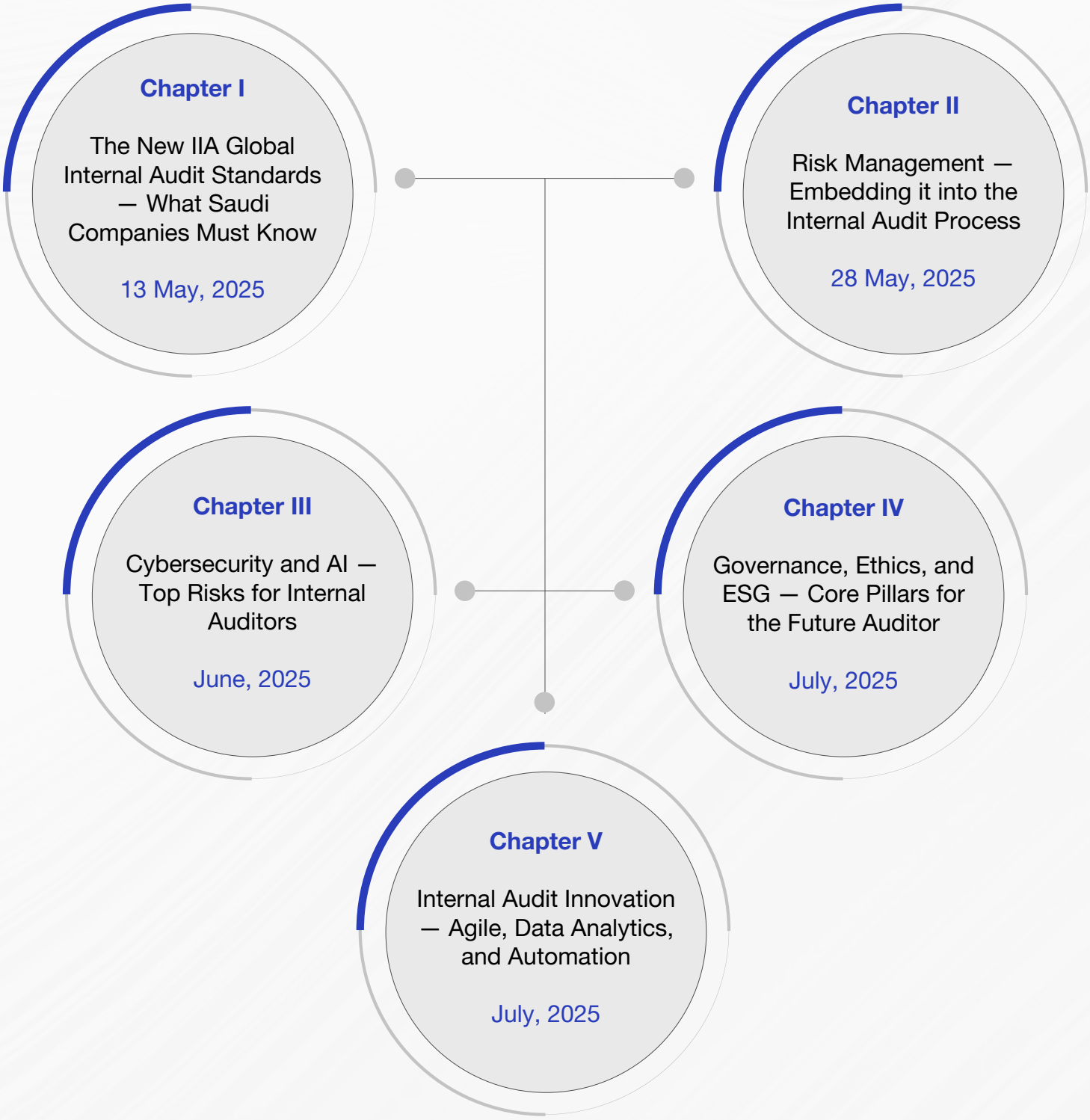
"Redefining Internal Audit's Role in Mitigating AI Misuse and Cyber Vulnerabilities"

Volume III

Aligning with 2024 IIA Standards and Vision 2030 Priorities

Internal Audit 2025

Aligning with New Global Standards and Emerging Risks for 2025



Internal Audit at the Frontline of Digital Risk

The 2024 Global Internal Audit Standards elevate cybersecurity to a core audit priority. Internal auditors are now expected to assess the adequacy of cyber governance (aligned with Domain V: Performing Internal Audit Services – Principles 13 & 14), test the effectiveness of controls, and evaluate incident preparedness, ensuring these efforts align with enterprise risk objectives and national cybersecurity frameworks.

In today's environment, cyber threats are dynamic and deeply intertwined with strategy, compliance, and reputation. For organizations advancing under Saudi Arabia's Vision 2030, the internal audit function plays a pivotal role in reinforcing digital trust, mitigating cyber risk, and ensuring resilience across critical systems as follows:

- Cybersecurity as a strategic risk
- Alignment with Vision 2030
- Role of internal audit in digital trust

This section outlines how internal audit functions should respond to cybersecurity demands under the new standards. We examine risk-based planning, cyber competence, and data protection expectations, enabling audit teams to offer meaningful assurance in an increasingly digital world.

At **INSIGHTS**, we support organizations in embedding cybersecurity into internal audit strategy through tailored frameworks, skill-building, and advisory solutions grounded in the latest global and national standards.

Three Key Focus Areas

Risk-Aligned Focus: Auditors must treat cybersecurity as a strategic enterprise risk-ensuring governance and controls support evolving threat landscapes.

Skill-Backed Integrity: Cyber audits require current risk knowledge and unbiased execution, free from prior involvement or conflicts.

Resilience & Trust: Evaluate breach readiness while ensuring data confidentiality and compliance throughout engagements.

Internal Audit's Role in Cybersecurity per IIA Standard Alignment

The 2024 IIA Global Internal Audit Standards redefine internal audit's role in cybersecurity, recognizing it as a strategic risk central to performance, resilience, and trust. Internal auditors must move from reactive assurance to proactive evaluation, integrating cyber risks into governance and ensuring effective oversight.

Under the new standards, internal audit plays a key role in supporting leadership by evaluating whether cybersecurity governance and practices are comprehensive, dynamic, and strategically aligned.

Auditing the Risk Dimensions of Digital Innovation: Audit reviews controls for emerging risks in AI, automation, IoT, and cloud projects.

Developing In-House and Strategic Cyber Expertise: Audit builds or accesses cyber expertise to assess critical controls effectively.

Embedding Cybersecurity in Governance Structures: Audit evaluates how cybersecurity is integrated into governance and risk management, ensuring risks are prioritized and reported to leadership.

The 2024 IIA Standards promote agile, technology-enabled audit approaches to address fast-evolving cyber and AI risks. Internal auditors are expected to use tools like threat intelligence, security analytics, and automated testing to deliver real-time assurance.

Internal audit functions must ensure their cybersecurity assessments align with KSA regulatory requirements, including NCA frameworks and PDPL obligations. Beyond assurance, internal auditors play an advisory role by translating complex cyber risk issues into actionable recommendations, thereby helping boards and executives make informed decisions to protect critical assets.

AI Governance Audits: Managing Control, Bias, and Ethics Risks

The 2024 IIA Global Internal Audit Standards recognize artificial intelligence (AI) as a transformative force and a complex risk area requiring proactive oversight. Internal audit is now expected to assess whether AI governance frameworks are ethically grounded, well-controlled, and transparently managed. This includes evaluating risks tied to data integrity, model bias, and decision accountability.

As organizations accelerate digital transformation, internal audit plays a key role in ensuring AI systems align with purpose, protect stakeholder trust, and comply with evolving regulatory expectations.

The 2024 IIA Standards Strengthen Oversight of AI Governance and Ethical Risks:	
AI Ethics Integration	Internal audit is expected to review whether ethical AI principles such as fairness, accountability, and transparency are embedded in policy and practice, and whether they guide AI model design and deployment.
Bias Monitoring Mechanisms	Auditors should evaluate the presence and effectiveness of controls designed to detect and mitigate algorithmic bias, ensuring decisions do not unfairly disadvantage specific individuals or groups.
Data Governance in AI	Internal audit must assess data inputs used in AI models for quality, accuracy, relevance, and compliance with data privacy laws (such as Saudi PDPL), as poor data leads to unreliable outputs and reputational risk.
Accountability Structures	Internal auditors are responsible for verifying that AI-related responsibilities are clearly defined across business, IT, and compliance teams, and that ownership of AI risks is traceable at all stages.
Auditability and Transparency	Internal audit should assess whether AI systems are explainable and their outputs traceable ensuring models can be audited, decisions justified, and governance upheld even in automated environments.

Internal audit's oversight of AI governance aligns with the IIA's Three Lines Model, enhancing its role as a strategic advisor on emerging technology risks. In Saudi Arabia, where Vision 2030 accelerates AI adoption and digital innovation, internal audit is critical in ensuring AI systems operate within ethical, control, and regulatory frameworks. The 2024 IIA Standards emphasize continuous monitoring and forward-looking assurance, enabling auditors to identify and address AI-related risks such as bias, data integrity, and transparency.

This alignment supports Saudi Arabia's digital transformation and regulatory reforms by confirming that AI governance practices are robust and effective. Internal audit acts as an independent reviewer, validating management's controls and recommending improvements where AI governance frameworks are still developing. Through this role, internal audit helps organizations balance innovation with ethical responsibility and compliance with Saudi regulations like the PDPL and NCA cybersecurity standards.

Third-Party (Vendor) Cyber Risk Management

To effectively manage cyber risks from third parties, internal audit must align closely with Enterprise Risk Management (ERM) to gain comprehensive visibility into vendor-related threats. This collaboration sharpens audit focus on critical third-party risks, improves oversight of vendor security controls, and helps organizations respond swiftly to supply chain vulnerabilities. Insights supports clients in developing robust third-party cyber risk audit programs, ensuring compliance with regulatory standards and strengthening vendor governance. Below are the key areas of focus for managing third-party cyber risks:

Key Emerging Cyber Risks Requiring Audit Attention		
Risk Area	**Description**	**Internal Audit Focus**
Vendor Access Management	Risks related to how third parties access systems and data.	• Access controls review • Privilege management • Authentication checks
Data Protection & Privacy	Risks of data breaches or non-compliance with data privacy laws.	• Privacy compliance checks • Data handling audits • Confidentiality safeguards
Incident Response & Recovery	Risks tied to vendor preparedness for cyber incidents.	• Crisis preparedness assessment • Incident response testing • Communication audits
Contractual Security Clauses	Risks from inadequate security requirements in vendor contracts.	• Contract terms audit • SLA compliance • Enforcement monitoring
Continuous Monitoring	Risks from lack of ongoing oversight of vendor security posture.	• Risk assessment reviews • Security audit schedules • Performance tracking
Supply Chain Vulnerabilities	Risks from interconnected third-party ecosystems.	• Supply chain risk mapping • Interdependency analysis • Mitigation controls review
Regulatory Compliance	Risks of vendor non-compliance with local cybersecurity laws.	• Regulatory adherence review • Compliance reporting • Policy alignment checks
Technology and Tool Risks	Risks associated with vendor-provided software or hardware.	• Technology vetting audits • Security testing • Batch management verification

Cybersecurity Audit Checklist Based on Saudi NCA Standards

Saudi Arabia's Vision 2030 drives significant digital transformation, creating a complex cybersecurity risk landscape. As organizations adopt advanced technologies and face stricter regulatory requirements from the National Cybersecurity Authority (NCA), internal audit functions must evolve to provide targeted oversight. Understanding the NCA's cybersecurity framework and local compliance mandates is crucial for delivering effective, risk-based cybersecurity assurance aligned with the Kingdom's strategic objectives.

NCA Cybersecurity Compliance	As Saudi Arabia advances its digital infrastructure, compliance with NCA cybersecurity standards is vital to safeguard national interests and critical assets. Internal audit plays a pivotal role in verifying adherence to these mandates, ensuring organizations uphold rigorous security controls. This compliance not only protects sensitive information but also strengthens stakeholder confidence in the organization's cybersecurity posture and regulatory alignment.
Risk-Based Control Assessment	In the face of evolving cyber threats, internal audit must prioritize controls based on dynamic risk assessments that reflect the organization's unique threat landscape. By focusing on the most critical vulnerabilities and security measures, auditors help optimize resource allocation and risk mitigation efforts. This targeted approach enhances resilience and aligns cybersecurity practices with Saudi Arabia's strategic risk management goals.
Incident Response and Reporting	Timely detection and management of cybersecurity incidents are essential to minimize impact and support regulatory transparency. Internal audit ensures that incident response frameworks are robust, tested, and compliant with NCA reporting requirements. Effective oversight of these processes builds organizational agility and assures stakeholders that risks are being managed proactively and responsibly.
Third-Party Cybersecurity Oversight	As organizations increasingly rely on vendors and partners, managing third-party cyber risk becomes a strategic priority. Internal audit evaluates how well these risks are identified, controlled, and monitored throughout the vendor lifecycle. This oversight protects the organization's extended digital ecosystem, bolsters supply chain security, and upholds regulatory expectations.
Continuous Monitoring & Awareness	Cybersecurity is a constantly evolving challenge requiring persistent vigilance. Internal audit's role in validating continuous monitoring and cybersecurity training programs is critical to maintaining a proactive security posture. By promoting ongoing awareness and real-time risk detection, audit helps ensure that organizations remain resilient against emerging threats and aligned with national cybersecurity objectives.

Understanding cybersecurity risks and compliance requirements is essential—but the real value lies in effective action. Insights shall assist Saudi organizations in aligning their audit practices with NCA cybersecurity standards, ensuring regulatory compliance, and providing robust assurance over critical digital infrastructure protection.

Real-Life Audit Examples: Cyber Risks and Response in KSA Companies

As cyber threats continue to evolve rapidly, organizations in Saudi Arabia face increasing challenges in safeguarding their digital assets. Internal audit plays a vital role in identifying, assessing, and mitigating these risks while ensuring compliance with national cybersecurity regulations. By examining real-life audit findings and responses, companies can strengthen their cybersecurity posture and enhance resilience against emerging threats. Below are key cyber risks encountered in KSA companies alongside typical internal audit actions taken to address them:

Cyber Risks

Phishing and Email Compromise

Responses and Actions

Internal audit recommended multi-factor authentication (MFA) and simulated phishing training. In response, the organization adopted a zero-trust approach for email verification and introduced mandatory awareness sessions, drastically reducing click-through rates on malicious emails.

Cyber Risks

Cloud Security Misconfigurations

Responses and Actions

The audit revealed that cloud governance policies were outdated. The company revised access rights, implemented automated configuration checks, and aligned cloud architecture with the NCA Cloud Cybersecurity Controls to prevent data leakage and regulatory breaches.

Cyber Risks

Third-Party Vendor Breaches

Responses and Actions

Following the audit, the organization established a third-party risk management framework. This included regular audits of critical vendors, onboarding risk scoring, and cyber-SLAs. This step enabled faster threat detection and ensured vendor accountability in line with PDPL obligations.

Cyber Risks

Shadow IT and Unauthorized Applications

Responses and Actions

Internal audit prompted the development of an enterprise-wide application inventory and the implementation of endpoint monitoring tools. The response ensured that only vetted applications were used, reducing attack vectors and enforcing policy compliance.

Cyber Risks

Outdated Incident Response Plans

Responses and Actions

The audit team highlighted gaps in crisis response testing and documentation. Management updated the incident response plan to align with NCA standards, ran tabletop exercises, and assigned ownership to specific teams—improving speed and clarity in breach situations.

Cyber Risks

Insider Threats and Privileged Access Abuse

Responses and Actions

The audit uncovered that many users had unnecessary administrative rights, increasing the risk of intentional or accidental misuse. The company responded by implementing role-based access controls (RBAC), logging all privileged activity, and integrating user behavior analytics (UBA) tools to flag anomalies. These actions significantly reduced insider risk exposure while enhancing accountability.

Cloud Security Audits: Addressing Risks in Remote Infrastructure

As Saudi organizations accelerate cloud adoption, internal audit plays a critical role in ensuring remote infrastructure is secure, compliant, and resilient. Auditing cloud environments against national standards like the NCA Cloud Cybersecurity Controls helps identify misconfigurations, assess third-party risks, and verify ongoing monitoring.

Below are the key focus areas for internal audit when assessing cloud security in remote infrastructure environments.

01

Analyze the organization's cloud risk management framework to ensure it comprehensively identifies and prioritizes risks associated with remote infrastructure and evolving threat landscapes.

02

Evaluate the design and operational effectiveness of cloud security controls, including identity and access management, data encryption, network segmentation, and incident response protocols.

03

Review the implementation of continuous monitoring and threat detection mechanisms, such as automated alerts and vulnerability scanning, to verify timely identification of security incidents.

04

Analyze the organization's cloud risk management framework to ensure it comprehensively identifies and prioritizes risks associated with remote infrastructure and evolving threat landscapes.

05

Analyze the organization's cloud risk management framework to ensure it comprehensively identifies and prioritizes risks associated with remote infrastructure and evolving threat landscapes.

06

Inspect the configuration management process to verify that cloud resources are securely provisioned, maintained according to best practices, and regularly audited for misconfigurations that could expose vulnerabilities.

07

Validate disaster recovery and business continuity plans related to cloud infrastructure to ensure data availability and system resilience in case of outages or cyber incidents.

Strategic Audit Planning for Emerging Cyber and AI Threats

To meet the demands of the 2024 IIA Standards, internal audit functions must transform from traditional compliance roles to strategic advisory partners.

1. Planning Must Be Risk-Aligned and Dynamic

The audit plan should focus on emerging cyber and AI risks, not on legacy schedules. This requires:

- Aligning audits with current cyber and AI risk assessments and organizational strategy
- Regularly updating risk evaluations (e.g., quarterly or after major incidents)
- Prioritizing audits on areas with the highest potential impact

2. Planning Must Be Risk-Aligned and Dynamic

Effective audit planning involves collaboration with cybersecurity, AI governance, and risk management teams. This includes:

- Engaging relevant stakeholders early in the planning process
- Incorporating the latest threat intelligence and regulatory standards
- Ensuring audit scopes reflect evolving external and internal risk factors

3.Agility and Technology-Enabled Auditing

Audit plans must be flexible and leverage advanced technologies. This involves:

- Using AI and data analytics tools to enhance audit effectiveness
- Incorporating scenario analysis and simulations to test resilience
- Including governance, ethical, and bias considerations related to AI

How Can Insights Help

At Insights Financial Management & Consultancy, we go beyond guidance — we drive transformation. Our advisory services empower internal audit functions to shift from control-centric to strategy-led, aligning seamlessly with the 2024 IIA Standards and supporting the strategic goals of Saudi Arabia's Vision 2030.

Responses and Actions

01 Enterprise Risk Management (ERM) Maturity Reviews

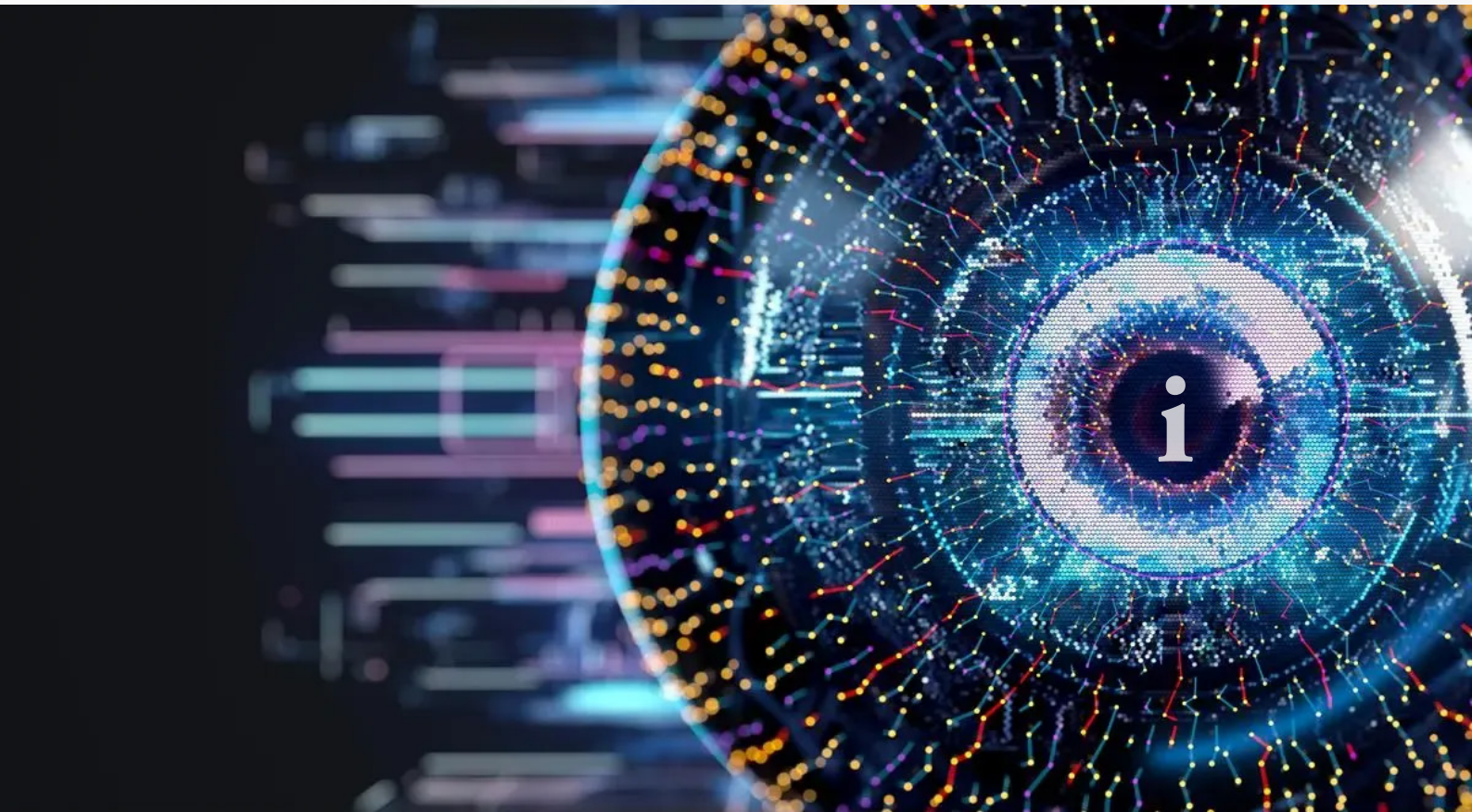
02 Internal Audit Readiness Assessments (aligned with IIA 2024)

03 Board & Audit Committee Workshops on Governance Oversight

04 Agile Audit Planning Models and Toolkits

05 Regulatory Compliance Audits (SAMA, CMA, DGA)

06 ESG, Cybersecurity & AI Risk Audit Frameworks



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

Navigating Complexity, Simplifying Success

insights