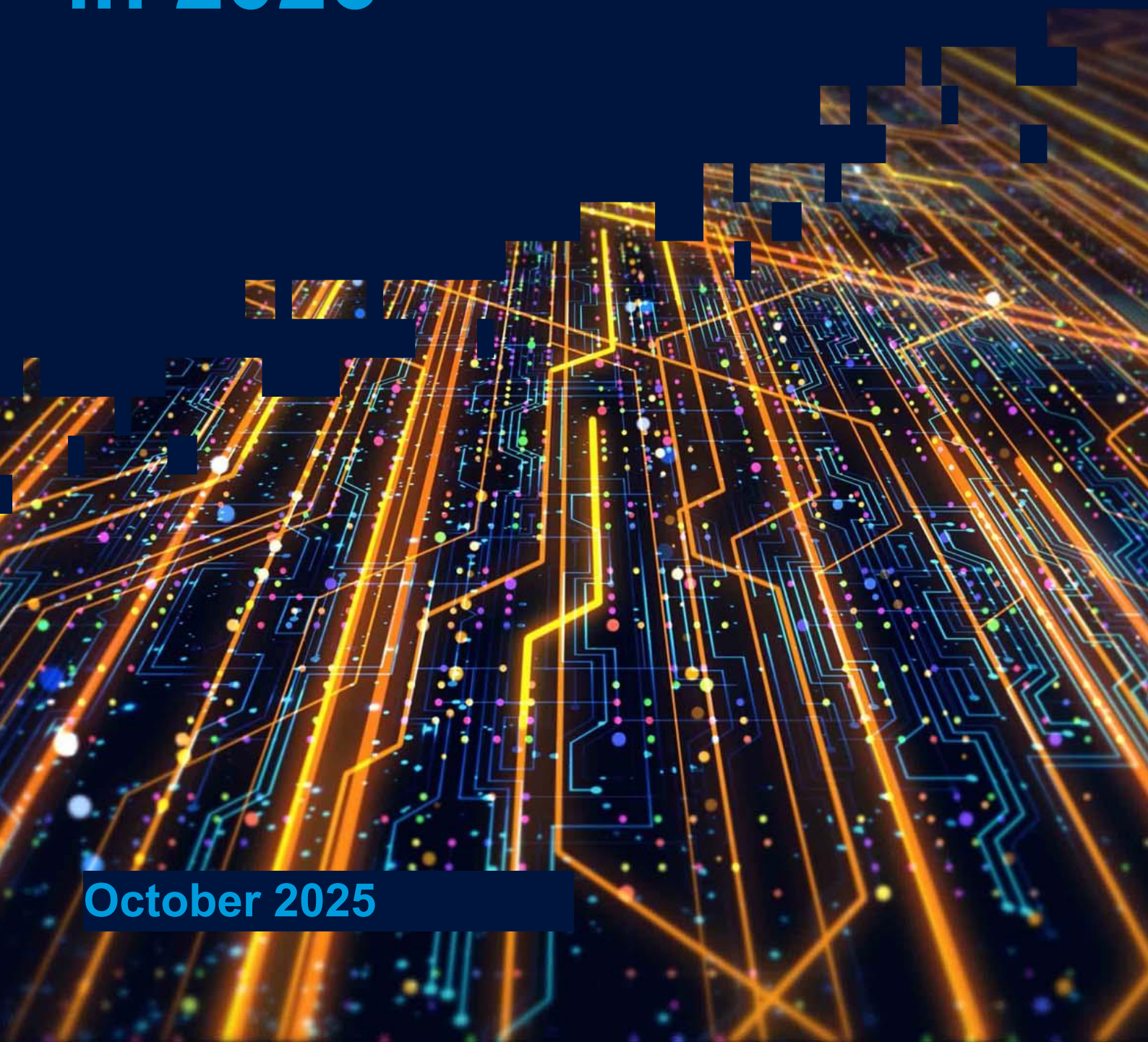
Thematic priorities for internal audit in 2026



October 2025

Thematic priorities

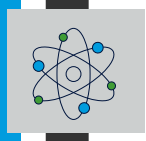
Internal audit functions must remain agile and forward-looking when developing their 2026 audit plans as their organisations face intensifying risk and regulatory complexity.

As organisations continue to operate in a volatile and fast-evolving risk landscape, the convergence of geopolitical instability, digital transformation, regulatory reform and stakeholder scrutiny is reshaping risk profiles and control environments. The pace of change is accelerating, and internal audit functions must evolve to provide timely, strategic assurance across both emerging and established risk domains.

To support Heads of Internal Audit, we have identified the key thematic areas and related risks which internal audit functions should consider when preparing their 2026 audit plans. While not exhaustive, the thematic areas below provide a foundation for internal audit functions to assess their organisation's risk profile and control environment in 2026.

External pressures

- Geopolitical risk
- Operational resilience
- Third-party risk and supply chain



Technology

- Cyber security
- Artificial intelligence governance
- Data governance and privacy
- Digital transformation and cloud risk

Operational challenges

- Talent, culture and skills
- ESG and sustainability

Regulatory-driven risk

- AI, ESG, resilience, and financial crime

External pressures

Organisations continue to face significant external pressures as geopolitical instability, economic uncertainty, and supply chain disruption persist across global markets. These pressures are compounded by evolving regulatory expectations, increased scrutiny from stakeholders, and the need for greater agility in risk management and strategic planning. Internal audit functions must assess how their organisations are responding to these challenges, ensuring that resilience frameworks, third-party oversight and strategic risk management are sufficiently robust, integrated and future-proofed.

Geopolitical risk

Geopolitical volatility remains a defining feature of the global risk landscape. The rise of regionalism, the decline of multilateralism, and the proliferation of grey-zone threats, such as cyber sabotage, disinformation campaigns, and infrastructure attacks, are reshaping global alliances, trade flows, and supply chain dependencies. Political transitions across major economies, including the EU, UK and US, are driving regulatory divergence and uncertainty, while emerging coalitions and alternative governance models challenge the traditional Western-led order.

Internal audit should assess how geopolitical risks are identified, monitored and integrated into enterprise risk management frameworks. This includes evaluating the effectiveness of horizon scanning, scenario planning, and stress testing capabilities, as well as the agility of governance structures to respond to external shocks. Assurance should extend to the resilience of critical third parties, the robustness of contingency planning, and the organisation's ability to adapt to shifting regulatory and economic conditions across jurisdictions.

Operational resilience

Following the implementation deadlines for DORA and UK resilience regimes, regulators now expect firms to embed operational resilience into business-as-usual activities. This marks a shift from compliance-driven programmes to strategic resilience capabilities that support continuity, adaptability and long-term sustainability. The focus is now on maturity, integration and continuous improvement.

Internal audit should assess the design and operating effectiveness of resilience frameworks, including business continuity planning, ICT recovery strategies, and crisis response protocols. Assurance should cover the quality of management information, the sophistication of resilience testing (including threat-led penetration testing), and the alignment of resilience activities with broader risk and change management programmes. Internal audit must also evaluate how resilience is embedded into outsourcing arrangements, product development, and strategic initiatives, ensuring that resilience is treated as a core business capability rather than a regulatory obligation.

Third-party risk and supply chain

Third-party risk continues to escalate as organisations deepen their reliance on outsourcing, cloud services, and digital ecosystems. This dependency is amplified by geopolitical fragmentation, economic volatility, and increasingly complex global supply chains. Regulatory scrutiny is intensifying, with frameworks such as DORA, PRA SS2/21, and the UK's Critical Third Party regime requiring firms to demonstrate robust governance, resilience, and accountability across their extended enterprise. These developments reflect a shift from transactional vendor management to strategic oversight of critical service providers.

Beyond operational and financial considerations, organisations must now address data sovereignty, cross-border compliance, and ESG-related risks within their supply chains. Stakeholders expect transparency on ethical sourcing, environmental impact, and human rights practices, while regulators demand evidence of due diligence and continuous monitoring. The integration of AI-driven tools and automation into supply chain operations introduces additional risks around algorithmic bias, cyber vulnerabilities, and regulatory compliance.

Internal audit should evaluate the maturity and effectiveness of third-party governance frameworks, including onboarding, due diligence, contract terms, and performance monitoring. Assurance should extend to resilience testing of critical suppliers, oversight of subcontractors, and integration of ESG and AI risk considerations. Internal audit must also review contingency planning, supplier diversification strategies, and the organisation's ability to respond to disruptions, ensuring resilience is embedded as a strategic capability rather than a compliance exercise.

Operational challenges

Organisations are facing mounting internal pressures as they adapt to shifting workforce expectations, evolving ESG obligations, and the need for continuous transformation. Talent shortages, hybrid working dynamics, and cultural alignment are now strategic concerns, while sustainability reporting and climate risk integration are becoming regulatory imperatives. Internal audit must provide assurance over how these challenges are being addressed, with a focus on governance, data quality, and alignment to long-term organisational objectives.

Talent, culture and skills

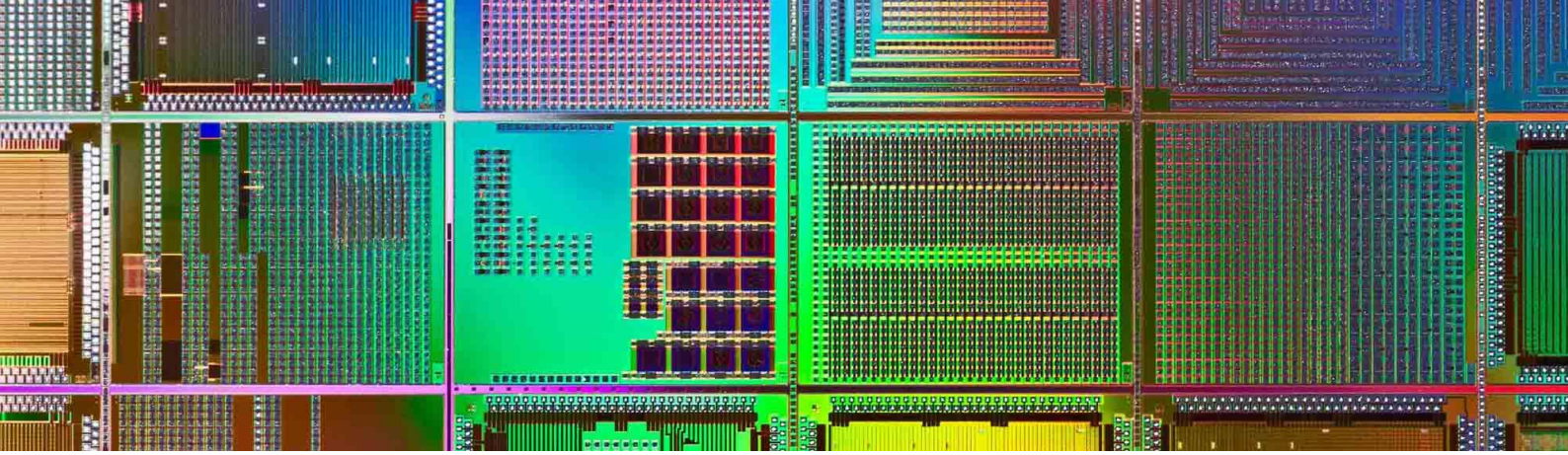
The skills required for internal audit are evolving rapidly. The adoption of GenAI, advanced analytics, and agile assurance methodologies is reshaping the profession, demanding new capabilities and mindsets. At the same time, organisations face persistent challenges in attracting and retaining talent, with hybrid working arrangements, DE&I expectations, and employee value propositions under increasing scrutiny.

Internal audit should assess workforce planning, talent acquisition strategies, and upskilling initiatives across the organisation. This includes evaluating the organisation's readiness for AI adoption, the maturity of behavioural risk frameworks, and the effectiveness of staff engagement mechanisms such as surveys, feedback loops, and cultural assessments. Assurance should also cover succession planning, leadership development, and the alignment of workforce strategies with long-term business objectives and regulatory expectations.

ESG and sustainability

Sustainability reporting and climate risk management are entering a new phase of maturity and regulatory scrutiny. The UK Sustainability Reporting Standards (UK SRS), CSRD, and ISSB frameworks are driving convergence and increased assurance expectations. Organisations are expected to produce credible transition plans, integrate climate risks into financial planning, and demonstrate alignment with net zero commitments.

Internal audit should assess the governance, data quality, and control frameworks underpinning ESG reporting and climate risk management. This includes reviewing CSRD readiness, the integration of climate risks into ORSA, ILAAP (where relevant) and strategic planning, and the effectiveness of sustainability data governance. Assurance should also extend to stakeholder engagement, ESG risk registers, and the alignment of ESG initiatives with broader organisational strategy and regulatory requirements.



Technology

The pace of technological advancement continues to reshape risk landscapes across sectors. From the proliferation of generative and agentic AI to the increasing reliance on cloud infrastructure and data-driven decision-making, organisations are navigating a complex and rapidly evolving digital environment. Internal audit functions must be equipped to assess the governance, resilience and compliance frameworks underpinning these technologies, ensuring that innovation is balanced with robust risk management and regulatory alignment.

Cyber security

Cyber threats continue to evolve in scale, sophistication and impact. AI-powered attacks, ransomware, and supply chain vulnerabilities are now commonplace, with attackers leveraging automation, deepfakes and behavioural analytics to bypass traditional defences. The IIA's Cyber Topical Requirement, effective February 2026, introduces a new baseline for cyber assurance, requiring internal audit functions to assess governance, risk management and control effectiveness across the cyber domain.

Internal audit should evaluate the maturity of cyber security programmes, including threat detection capabilities, incident response plans, and alignment with recognised frameworks such as NIST and COBIT. Assurance should cover phishing simulation results, privileged access management, vulnerability management, and the integration of cyber risk into strategic planning. Internal audit must also assess compliance with the IIA requirements, including documentation, applicability assessments, and evidence of conformance.

Artificial intelligence (AI) governance

AI is now a foundational technology, with agentic and generative systems introducing new risks around autonomy, ethics, and accountability. The EU AI Act and UK regulatory developments are setting clearer expectations for responsible AI use, including transparency, explainability, and human oversight.

Internal audit should assess AI governance frameworks, model risk management practices, and regulatory readiness. This includes evaluating the inventory of AI systems, decision boundaries, training data quality, and the effectiveness of human-in-the-loop safeguards. Assurance should also extend to third-party AI tools, ethical risk assessments, and the organisation's internal audit capability to audit AI use cases across the lifecycle, from planning and testing to reporting and continuous monitoring.

Data governance and privacy

Data remains a strategic asset, but poor governance creates significant risk. The UK Data Use and Access Act (DUAA), GDPR, and AI regulations are reshaping data compliance requirements, with increased expectations around transparency, traceability and accountability.

Internal audit should assess the design and operating effectiveness of data governance frameworks, privacy controls, and data resilience strategies. This includes evaluating metadata standards, lineage mapping, dark data risks, and the integration of data risk into the enterprise risk management framework. Assurance should also cover third-party data access, staff awareness and training, and the organisation's ability to respond to regulatory changes and data breach incidents.

Digital transformation and cloud risk

Cloud adoption and digital transformation continue to accelerate, but bring new risks around cost optimisation, resilience, and compliance. ESG considerations and geopolitical tensions are also impacting cloud strategies, with increased scrutiny around data sovereignty, vendor lock-in, and supply chain resilience.

Internal audit should assess cloud governance frameworks, cost management practices, and the resilience of cloud supply chains. This includes evaluating vendor diversification strategies, contract terms, incident response capabilities, and alignment with evolving regulations such as NIS2 and the UK Cyber Security and Resilience Bill. Assurance should also extend to ESG integration, data privacy controls, and the effectiveness of cloud sustainability initiatives.

Regulatory-driven risk

The regulatory landscape is expanding across AI, ESG, resilience, and financial crime. Internal audit must assess the effectiveness of regulatory change programmes, the organisation's compliance culture, and its readiness for new obligations. This includes evaluating integrated assurance models, governance structures, and alignment with strategic objectives. Assurance should also cover horizon scanning, stakeholder engagement, and the organisation's ability to adapt to regulatory divergence across jurisdictions.

RSM delivers internal audit services that drive assurance, insight, and strategic value. With deep sectoral expertise, we help clients strengthen governance, manage risk, and enhance control environments. Our offerings span outsourced and co-sourced delivery, SME support, EQAs, QAIPs, and technology-enabled audits. We deploy cutting edge data analytics and AI to elevate performance.

Please contacts us to discuss further.

Colm Laird
Partner, Risk and Governance
colm.laird@rsmireland.ie

Colm Laird is a leading voice on internal audit, risk, and governance in Ireland. He delivers ICT and business audits that strengthen resilience and compliance. A Chartered Accountant and CIA, CFA, CISA holder, Colm combines sector insight with AI technology-enabled approaches to drive strategic assurance.

Ian McCartney
Director, Risk and Governance
ian.mccartney@rsmuk.com

Ian McCartney is a leading voice on internal audit in Northern Ireland with over 25 years' experience. An FCA, he delivers assurance to boards and regulators, specialising in governance, risk management, and regulatory compliance for financial services and public bodies.

Syed Haque
Director, Financial Services
syed.haque@rsmireland.ie

Syed Haque has nearly 20 years' experience in financial services, including Head of Internal Audit (PCF-13) and senior leadership roles. An FCA and ACCA member, Syed specialises in internal audit, SOC1 reviews, and regulatory assurance for global financial institutions.

Catherine Keenan
Associate Director, Risk and Governance
catherine.keenan@rsmuk.com

Catherine Keenan is an FCCA with expertise in internal audit, risk assurance, and forensic investigations. She co-leads RSM's all-Ireland internal audit portfolio, advising public sector and regulated clients on governance, compliance, and process improvement.

Yevgen Shuvalov
Consultant, Risk and Governance
yshuvalov@rsmireland.ie

Yevgen, former Head of Internal Audit at Ukraine's Central Bank, brings 15 years' experience in public sector and financial services audits. He focuses on governance, cultural risk, and irregularities, delivering assurance that strengthens resilience.

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

RSM Ireland

Block D, Iveagh Court,
Harcourt Rd,
Dublin 2,
D02 VH94
T +353 (0)1 496 5388
www.rsmireland.ie