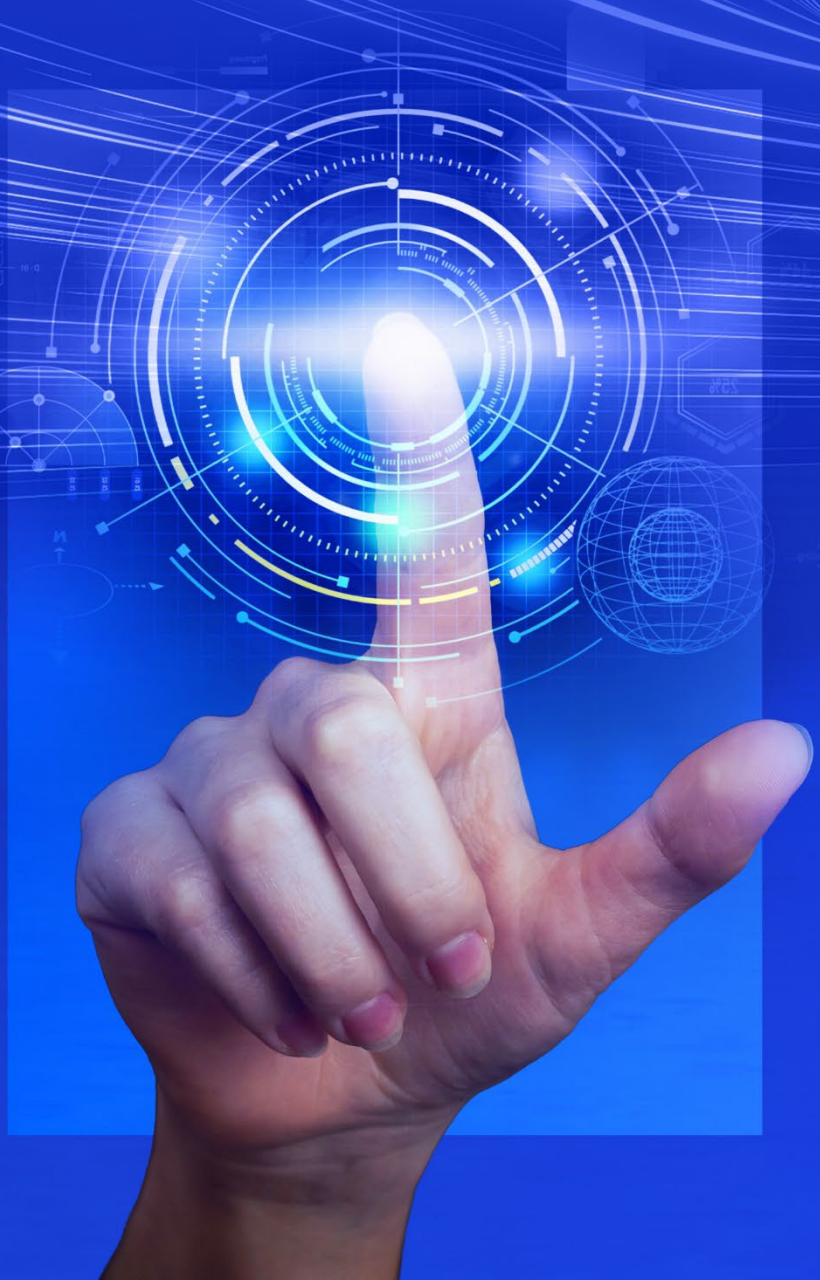
KPMG

Internal audit: Key thematic areas to consider in 2025



October 2024

Key thematic areas to consider in 2025: Overview

Internal audit functions must remain agile and responsive to change when developing their 2025 audit plans as their organisations face evolving challenges.

As organisations continue to navigate a volatile and dynamic risk environment, the depth and breadth of threats being confronted have intensified, exacerbating the stress on organisations' risk and control frameworks. Having endured unprecedent levels of uncertainty and disruption in recent years, most organisations continue to contend with the unceasing threats and challenges posed by prevailing economic and geopolitical conditions, altering stakeholder outlooks, stringent regulatory requirements and heightened digitisation.

To support Heads of Internal Audit, we have identified and compiled the key thematic areas and related risks which internal audit functions should consider. The thematic areas below include both emerging and established risks which internal audit should consider when preparing its agile annual internal audit plan for 2025.

While the below is not an exhaustive list of thematic areas, these can serve as a starting point from which the internal audit function can leverage when assessing the organisation's risk profile and control environment throughout 2025. We have provided further information on each thematic area overleaf.

External Pressures

- Economic & Geopolitical Uncertainty
- Operational Resilience
- Third-Party Relations & Supply Chain

Operational Challenges

- Talent Management & Retention
- Environmental, Social & Governance (ESG)

Technology

- Fraud & Financial Crime
- Cyber Security
- Data Privacy and Governance
- Digital Disruption and Emerging Technology

Regulatory-driven risk

Organisations have faced unprecedented levels of geopolitical and economic volatility in recent years. Escalating conflicts in the Middle East, the Ukraine War, and government reforms have created new risks and challenges for organisations and continue to impact the Irish economy in many ways, including disruptions in supply chains. The operational resilience of organisations is being pushed to the limit, and organisations must ensure that their risk management functions, operations and supply chains are more agile, durable, and dynamic than ever before in order to navigate and effectively respond to such intense external pressures.

Economic & Geopolitical Uncertainty

Following years of unprecedented levels of economic and geopolitical instability, global economic growth remained resilient in 2024, with further growth and recovery anticipated for 2025. Notwithstanding, the current geopolitical landscape remains unstable and fragmented, with developments including escalating conflicts, flaring trade tensions and widespread political transitions in numerous parts of the world set to pose further risks and uncertainties into 2025.

Whilst proving sticky and stubborn in some countries, inflation is now on a downward trend. Consequently, interest rates in the EU, UK and US have declined throughout 2024, with the most recent third interest rate cut by the European Central Bank (ECB) this year emblematic of this gradual reversal of inflationary pressures which will persist into 2025. Despite this disinflation trend and the easing of monetary policy in recent months as price pressures eased, certain economic areas and sectors remain cautious due to ongoing geopolitical uncertainties and the potential supply chain disruptions.

Organisations must continue to implement long-term strategies to effectively navigate the challenges posed by such externalities and manage the associated risks.

The role of internal audit

Internal audit need to consider how both the first and second lines of defence in their organisation are managing the increased risks and impact on operations associated with the geopolitical factors. Internal audit should be involved in the evaluation of critical risk areas of the organisation. This should include the examination of the following aspects: long-term strategies aimed at mitigating financial and operational risks, third-party suppliers vulnerable to economic fluctuations, capital planning and management procedures.

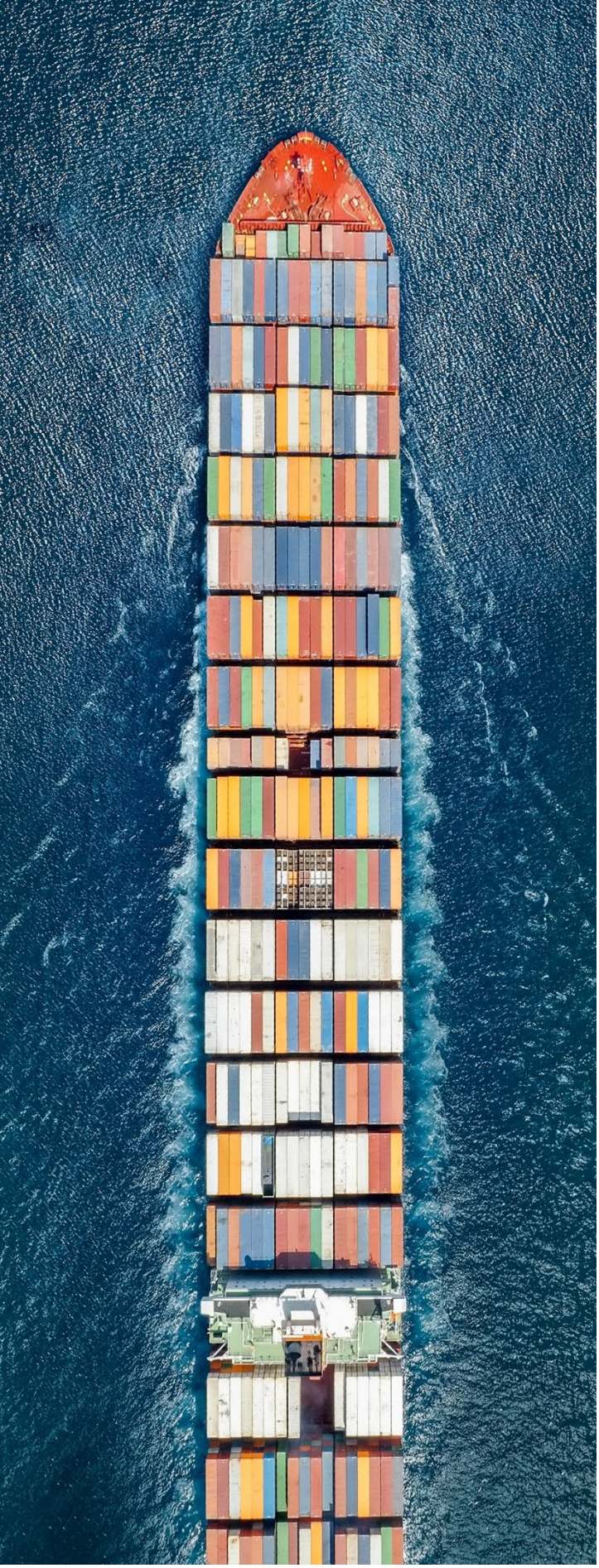
Operational Resilience

Mounting levels of global interdependency, the proliferation of technology-led organisation transformation, as well as recent high-profile instances of service outages have heightened the focus on the threat of disruption to organisations. These trends, along with current levels of economic, geopolitical and environmental instability, stress the importance of, and need for, organisations to manage their operational risk, plan for contingencies and maintain comprehensive and up-to-date Business Continuity (BC), Disaster Recovery (DR), and Cyber Response (CR) plans.

Additionally, the Digital Operational Resilience Act (DORA) will formally apply to both financial entities and, by extension, their ICT third-party service providers from January 2025. Published by the EU Commission, DORA unifies and builds upon existing regulations and requirements relating to digital risks in the financial sector to create a detailed and comprehensive framework whereby EU financial firms ensure they can endure ICT-related disruptions and risks and remain operational. The focus of DORA concerns maintaining resilient business operations and related processes and services, with the regulation prescribing a series of objectives aiming to strengthen and enhance the collective digital resilience of the European financial sector.

The role of internal audit

Internal audit should assess the design and operating effectiveness of operational resilience and crisis management protocols, frameworks and associated systems to ensure that key threats have been determined and adequate response plans exist and are fit for purpose. Moreover, internal audit should review business continuity measures to ascertain whether emerging risks and evolving threats have, and continue to be, considered by management.



Third-Party Relations & Supply Chain

Supply chain risks are currently heightened as organisations attempt to navigate the fragmented geopolitical landscape arising from the impacts of conflicts in Ukraine and the Middle East, mounting protectionism, policy interventions, and shifting consumer expectations. These developments continue to influence supply chain strategies and investment decisions, with prevailing volatility increasing the complexity and costs associated with mitigating supply chain risks. The effects of these developments underscore the need for robust risk management of outsourced relationships and stress the criticality of supplier diversification. In addition, amid intensifying stakeholder scrutiny and an evolving regulatory environment, organisations must also assess and enhance the transparency, ethics and ESG implications inherent in their supply chains, including performing risk assessments and due diligence of third-parties. Furthermore, organisations are increasingly automating supply chains and supply chain management by integrating technologies such as Artificial Intelligence (AI), blockchain and machine learning into traditional supply chain activities.

The role of internal audit

Internal audit should assess the maturity and resilience of supply chains and provide advice on the suitability of the supply chain operating model to ascertain if due consideration has been given to the risks associated with the current macroeconomic and geopolitical conditions.

In addition to the threats and challenges posed by prevailing externalities and the proliferation of digitised business models, organisations are having to contend with the risks and obstacles arising from dynamic and shifting stakeholder preferences and expectations. Organisations are struggling to attract and retain skilled talent, with changing consumer preferences further exacerbating the pressure and stress being exerted on organisations.

Talent management & retention

Recruitment and retention of skilled talent remains a significant hurdle for organisations with businesses encountering considerable issues in finding suitable candidates to fill vacant positions. Factors such as the availability and affordability of residential accommodation, salary expectations, flexible working arrangements, and intensified competition for talent are but some of the factors contributing to the challenges that management will have to confront and manage into 2025.

We have also seen a perceptible shift regarding hybrid working arrangements whereby a myriad of organisations have progressively reverted to pre-pandemic ways of working, with the general trends and overarching sentiment suggesting more businesses will follow suit in 2025.

Expectations for employee value propositions are ever expanding. Employees are seeking more meaning, purpose, fulfilment and flexibility in their jobs. Those organisations who fail to adapt and evolve their value propositions may find it difficult to attract and retain talented personnel.

The role of internal audit

Internal audit should appraise workforce planning practices and future skill demand, talent acquisition and employee retention strategies. Internal audit must understand and seek to mitigate the impacts of staff and skill shortages and increased turnover on organisations and the internal control environments therein. Additionally, internal audit should assess the adequacy and effectiveness of management oversight and initiatives being planned and undertaken to enhance employee value propositions, including the business approach to solicitation of employee input and feedback (staff surveys, focus groups, etc).

Environmental, Social & Governance (ESG)

Organisations continue to see ESG as being beyond merely complying with regulatory requirements, but a means to enhance value, attract the next generation of talent, strengthen employee engagement and employee value proposition whilst also driving financial performance. The recently effective reporting requirements under the European Union Corporate Sustainability Reporting Directive (CSRD) mandate in-scope organisations to be more transparent and accountable with regards ESG matters. For the first time in 2025, those companies first in-scope for CSRD will providing detailed disclosures on ESG matters for 2024, in compliance with European Sustainability Reporting Standards (ESRS), with more organisations also falling within scope of CSRD in 2025. The expectation for companies to contribute positively to society is paramount, with increased non-financial reporting requirements and stakeholder outlooks compelling organisations to integrate ESG considerations into their core strategies. Companies must consider their impact on people and the environment from an inside out perspective, and the risks and opportunities that may impact the organisation from an outside in perspective.

The role of internal audit

Internal audit should review CSRD reporting in 2025, where applicable, and prepare a CSRD readiness assessment for entities due to fall in scope, by providing advice and assurance over the governance and control frameworks for non-financial reporting. Additionally, internal audit should review the effectiveness of processes and controls for the acquisition, aggregation, quantification and reporting of ESG metrics. Internal audit can also provide advice on broader risk management capabilities to align ESG risks, strategies, and organisational objectives to ESG initiatives, such as the UN Sustainability Goals and the European Green Deal.

The ever-evolving world of emerging technologies has brought with it immense opportunities for organisations. As with all good things, however, these technological advancements are not without challenges. The advent of digitised business models leaves organisations exposed to new risks and subject to heightened regulation. Organisations are more connected than ever before, with vast amounts of personal data being processed, stored and shared globally. Organisations will have to enhance the robustness and rigour of their data privacy and cyber security controls and be proactive in their efforts to implement appropriate guardrails to protect against the escalating threat and incidences of fraud, financial crime and cyber incidents.

Fraud & Financial Crime

The prevalence and potency of fraud and financial crime is escalating globally. The development and employment of increasingly sophisticated techniques has intensified the velocity, veracity and volume of fraud and financial crime instances, heightening the level of risk posed to organisations as traditional processes and technologies struggle to keep pace.

Rapid integration of technological advancements has better enabled and better equipped criminal actors to exploit vulnerabilities within organisations as entities continue to recognise and identify the need for more robust, adaptive and technologically advanced approaches to combat and address rising fraud and financial crime threats.

Furthermore, fraud and financial crime transcends borders which increases the complexity and challenges associated with investigating and prosecuting criminal actors. Deepened levels of global connectivity further exacerbates the significant threats of fraud and financial crime posed to organisations worldwide, as geopolitical and economic instability in one region can have consequential implications on global markets and systems.

The role of internal audit

Internal audit should assess strategies and associated tools and technologies employed to manage the risk of fraud and financial crime and can subsequently provide advice on governance and control matters.

Cyber Security

As we look ahead to 2025, cyber security remains a key area of focus for organisations. We have witnessed a continuation of the persisting increase in cyber-attacks and data breaches in 2024, as the prevalence of cyber threats fails to falter. The velocity, volume and sophistication of cyber-attacks have intensified in recent years, further exacerbating the threat to business continuity, and heightening the risk of reputational damage and financial loss.

The continued digitisation of business models and operational processes globally, allied with the increasingly advanced technology at the disposal of cybercriminals, requires robust cyber security measures for maintaining operational capabilities, safeguarding stakeholder trust, and, fundamentally, alleviating the effects of future attacks.

Organisations will need to embed cyber security in core business processes and increase awareness of cyber security risks within their workforce to support reduce the impacts of now seemingly inevitable cyber-attacks.

The role of internal audit

Internal audit should assess the existing controls to mitigate cyber security risks and provide assurance on governance and oversight structures across the three lines of defence.

Data Privacy and Governance

In a technology-enabled environment, organisations must prioritise data privacy and data protection. The General Data Protection Regulation (GDPR) governs the protection of personal data, enforcing strict regulations for organisations to adhere to whilst simultaneously granting individuals unprecedented control over their personal information. The regulation applies universally, encompassing all organisations that handle personal data and necessitates organisations review their data privacy framework and ensure compliance with the requirements of GDPR. Non-compliance with GDPR, and ineffective management and governance of data practices generally, not only violates regulatory requirements, but also amplifies legal and financial risks, and exposes organisations to potential reputational damage.

Heightened levels of global interconnectedness also magnifies the significance of complying with rules around international data transfers for organisations. Furthermore, findings published this year in the Data Protection Commission Annual Report 2023 called attention to the matters of unauthorised access and disclosure of personal data, largely driven by a lack of understanding on the behalf of employees regarding their role and responsibilities in safeguarding personal data.

The role of internal audit

Assess the Data Privacy and Protection framework and associated controls in place in the organisation and ensure the adequacy and effectiveness of privacy structures with regard to relevant regulatory requirements in areas including data collection, retention, disclosure and transfer, as well as staff awareness and training initiatives.

Perform reviews to ascertain the identify of third-party processors and ensure a comprehensive understanding these parties that have access to the organisation's data and how this access is monitored and controlled.

Digital Disruption & Emerging Technology

Levels of exposure and excitement with regards AI have surged over the past few years with eyes opened to the undeniable potential and imminent transformative effects such technologies will have on how we live our lives and conduct business. However, amidst the global advent of AI in both business and personal life, concerns about the risks and appropriate usage of AI have emerged. In response, in March this year, the European Parliament formally approved the EU AI Act. The Act came into force on the 1st of August 2024, as the EU aims to strike a delicate balance between encouraging AI adoption and safeguarding against significant new risks regarding the responsible and ethical use, development and distribution of AI. The Act establishes a tiered system of regulatory requirements for different AI applications, depending on their level of risk, in recognition of AI as a product with potential threats to safety and fundamental rights. Prohibitions on certain AI systems will commence in February 2025, with the Act's requirements becoming effective on a gradual, phased basis with most general provisions applying from August 2026.

Organisations will need a fully integrated response and approach across their legal, compliance, IT and product delivery functions to navigate the increasingly complex and technical regulatory environment and proactively address the risks associated with emerging technologies.

The role of internal audit

Internal audit can advise on governance and control matters relating to an organisation's digital transformation strategy.

Internal audit should engage with management to define and enhance, where appropriate, a fit-for-purpose AI governance framework as well as a suite of internal controls to mitigate the risks that come with using AI.

Regulatory-Driven Risk

Organisations are continually having to contend with increasing regulation, the volume, breadth and depth of which is at an unprecedented level as we approach 2025. Regulatory environments and requirements continue to evolve and expand, with organisations of all sizes and industries required to comply with regulations in areas including ICT, AI, ESG and data privacy and security. This heightened regulatory burden poses significant challenges and exerts pressure on executive management who must ensure that their organisations, not only comply with prevailing regulations, but are also sufficiently agile and flexible to adopt and adapt to new obligations, as and when required.

The role of internal audit

Internal audit must analyse and develop a comprehensive understanding of the regulatory landscape in which the organisation operates in order to assess governance structures and controls to support compliance with relevant laws and regulations. Additionally, internal audit should review the level of management oversight and monitoring and control structure in place to evaluate the organisation's preparedness for future compliance requirements.

2024 Global Internal Audit Standards

Internal Audit functions must also remember that the Institute of Internal Auditors (IIA) released the 2024 Global Internal Audit Standards (Standards) on January 9, 2024. The Standards are the main component of the International Professional Practices Framework (IPPF) and will be effective from 9 January 2025.

Contact us:

Patrick Farrell
Partner
Risk Consulting

t: +353 870504029
e: patrick.farrell@kpmg.ie

Colm Laird
Director
Risk Consulting

t: +353 87 1115949
e: colm.laird@kpmg.ie

Maria McAnearney
Senior Consultant
Risk Consulting

t: +353 86 1040019
e: maria.mcanearney@kpmg.ie

Cian Mullen
Consultant
Risk Consulting

t: +353 86 0319747
e: cian.mullen@kpmg.ie

kpmg.ie