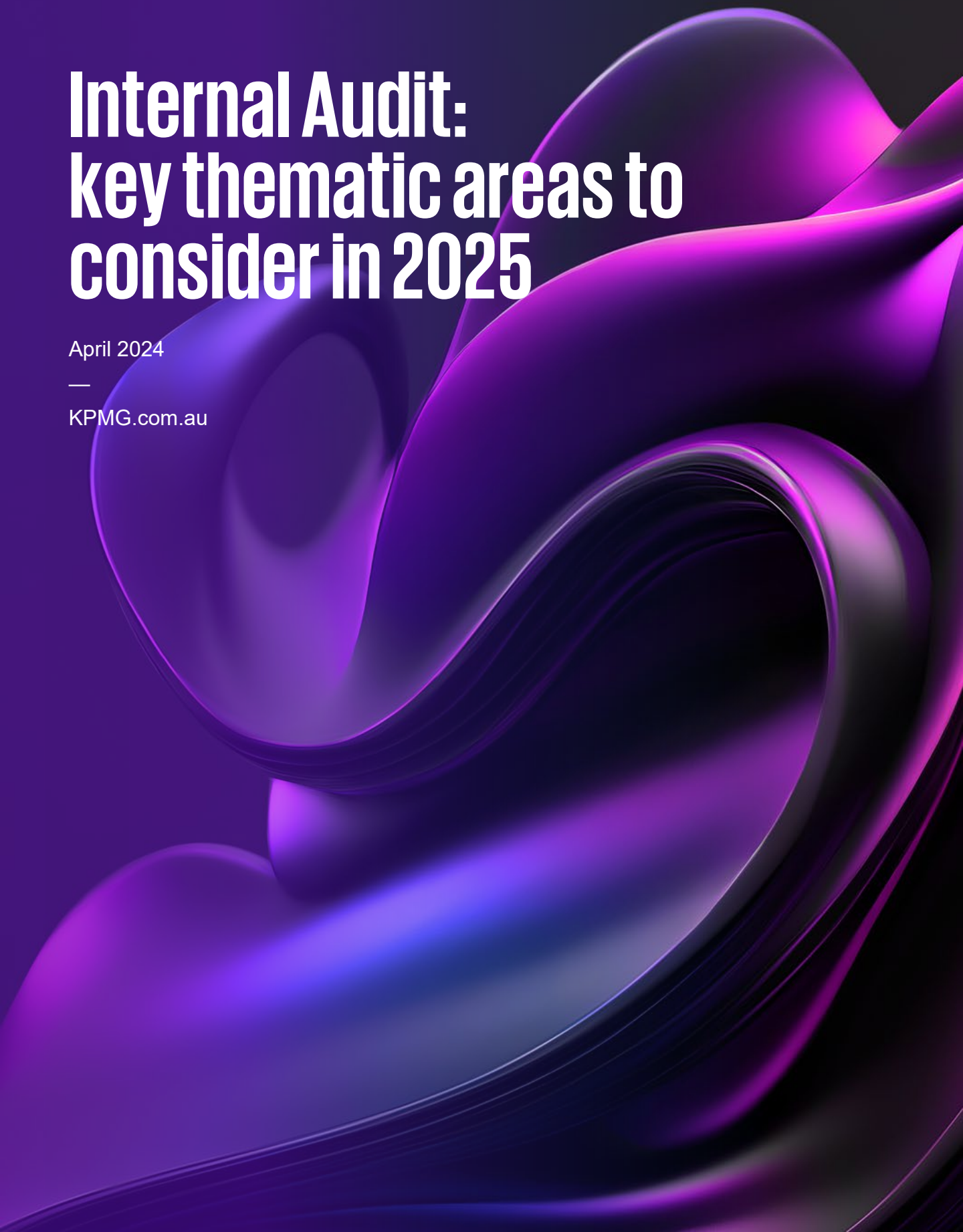
KPMG

Internal Audit: key thematic areas to consider in 2025

April 2024

—

KPMG.com.au



Internal Audit functions are confronting a risk environment that is continually evolving, marked by heightened uncertainty, unpredictability, and volatility. These factors compel Internal Audit to maintain a dynamic posture in the crafting of their 2025 Internal Audit Plans, ensuring agility and responsiveness to change.

The ability to anticipate potential issues and the flexibility to modify audit strategies are essential for safeguarding against such disruptions. The persistent uncertainties and disruptions experienced in recent times – including supply chain challenges, inflationary effects, and geopolitical instability – serve to amplify the stress on organisations' risk and control frameworks, necessitating vigilant and strategic responses.

Overview

To assist Heads of Internal Audit, we have compiled a portfolio of key thematic areas and their associated risks that Internal Audit functions should consider during the formulation of forward-looking Internal Audit Plans for 2025.

These themes encompass a spectrum of both emerging and established risks that should be applied in the creation of a responsive and agile Internal Audit Plan.

Below is a selective list of thematic areas – while not comprehensive, it is intended to provide a foundation upon which Internal Audit may base its evaluation of the organisation's risk and control standing for the forthcoming year.

Detailed insights on each identified thematic area are presented in the subsequent pages.

Key thematic areas to consider in 2025

External Pressures

Recent years have been termed the age of the 'polycrisis'.

The World Economic Forum (WEF) uses the term "polycrisis" to capture the essence of how a set of interconnected global risks and their compounding effects interact in a way that the total impact exceeds the sum of the individual parts. In light of the escalating levels of economic, geopolitical, and environmental uncertainty, the frequency, intensity, interconnectedness, and velocity of existing risks and threats are evolving, while new risks, once thought improbable, are coming to the forefront, substantially impacting on the Australian economy. These influences encompass a spectrum of factors including disruptions in supply chains, surges in inflation and rising costs, spikes in energy expenditures, tightening regulatory requirements, shifts in monetary policy, and evolving stakeholder expectations. Consequently, it is essential that the risk management frameworks of organisations become more predictive and agile than ever to effectively confront these challenges. We have highlighted the three main areas of focus:

Economic Uncertainty and Geopolitical Volatility

In recent times, the global economy has been experiencing an unprecedented degree of volatility, primarily driven by geopolitical issues. Events such as regional conflicts, persistent wars in Ukraine and Gaza, and the fragmentation of trade agreements are fuelling substantial inflationary pressures. Such geopolitical complexities have helped to perpetuate the elevated prices of commodities like gas and oil, leading to a persistent cost of living crisis. In an attempt to curb this inflationary trend, central banks across the globe, including Australia's, have resorted to raising interest rates to their highest levels in recent times. Nonetheless, despite the initial signs of inflation stabilisation and projections of a decline following the tightening of monetary policies, it is expected that geopolitical volatility will persist as a key driver of macroeconomic uncertainty into 2024 and beyond. Recognising that this state of economic flux and geopolitical volatility will constitute the 'new normal', organisations must adopt robust, forward-looking, and adaptable long-term strategies to successfully navigate the complexities that lie ahead.

The role of Internal Audit

Internal Audit is obliged to evolve in response, integrating geopolitical risk assessment as a core element in audit planning and risk evaluation. This integration should provide Internal Audit with the scope to comprehend and appraise how the organisation's first and second lines of defence are addressing and managing the amplified risks and operational impacts associated with geopolitical volatility. Employing advanced tools like Dynamic Risk Assessment (multi-faceted risk assessment solutions) and scenario modelling may enable an internal audit function to move beyond a standard two-dimensional risk analysis to investigate the connections between risks, their velocity and impact.

Environmental, Social and Governance

ESG is now integral for long-term sustainability. There are now multiple mandatory reporting requirements for ESG globally and following the issue of the ISSB standard (IFRS S1 and IFRS S2), the Australian Accounting Standards Board (AASB) recently published an exposure draft of Australian Sustainability Reporting Standard (ASRS) relating to disclosure of climate-related information. The release of this Exposure Draft marks an important step towards mandatory climate reporting in Australia, expected to commence from FY25 for some larger companies. These changes will improve transparency and will assist investors make more informed investments decisions. As such, compliance is requiring transformational changes in business activities so that organisations can define their ESG disclosures and metrics. However, an ESG risk and reporting program should not be implemented in isolation. organisations should recognize the value creation potential by connecting ESG efforts with long-term strategic goals, whereby committing to a bigger vision that encourages transformation to drive sustainability and resilience.

The role of Internal Audit

Internal Audit plays a crucial role in supporting organisations by assessing readiness for reporting requirements, offering guidance on governance and controls, and reviewing processes related to ESG metrics reporting.

They also provide advice on aligning risk management capabilities with ESG risks and organisational goals, while continuously ensuring the effectiveness and efficiency of ESG risk management, internal controls, and governance.

Additionally, Internal Audit evaluates data governance and control mechanisms to ensure accurate and thorough reporting.

Third-party relations & supply chain

The COVID-19 pandemic and the wars in Ukraine and Gaza have created volatile macroeconomic conditions and exerted great strain on global supply chains. Whilst the impacts of these events are easing, they, along with other pressures such as extreme weather and inflation, highlight the need for robust risk management in outsourcing relationships, emphasizing the imperative to diversify supplier portfolios and avoid undue dependence on a single source.

In addition, given the evolving regulatory landscape and increasing stakeholder expectations, organisations are compelled to assess the transparency, ethics, and ESG implications inherent in their collaborations with third parties that support their operational activities.

Consequently, many organisations have realigned their supply chain objectives from a focus on cost and efficiency to prioritizing flexibility and continuity. We expect to see this continued focus on resilience and sustainability of supply chains.

The role of Internal Audit

Internal Audit should go beyond contract management and assess the maturity and resilience (and concentration) of supply chains, as well as providing advice on the suitability of the supply chain operating model, and determine if sufficient consideration has been given to the risks associated with current macroeconomic and geopolitical conditions.

Operational challenges

Securing success: Operational challenges in the digital age

In navigating the operational landscape of 2025, organisations must anticipate and address a myriad of thematic areas to stay resilient and competitive. The heightened levels of economic, geopolitical, and environmental uncertainty are creating new risks, threats and opportunities at an unprecedented rate and impacting the Australian economy.

Amidst the priority for escalating digital transformation, it has become apparent that functions need to be more progressive and dynamic than ever before to navigate concerns surrounding operational challenges. Below, we have included the three main areas of focus:

Profitability, inflation and liquidity

With inflation and interest rates reaching highs not seen since the early 2000s, 2023 has been particularly marked by an intense macroeconomic volatility, which has placed considerable financial pressure on organisations worldwide. As these organisations peer into the horizon of 2024 and beyond, the expectation is not for a swift return to stability but rather for a continued oscillation that companies must adeptly manage.

The augmentation of risks related to corporate assets and cash flows presents an onerous challenge to long-term financial performance—threatening not just immediate fiscal health but also the strategic fortitude organisations have cultivated over time. In response, key internal functions are called upon to carefully evaluate the extent of these risks and their potential ramifications. The spectrum of these considerations spans the direct impact of inflated expenses that may erode profitability margins, to the intricacies of liquidity management in a climate where credit could become both more expensive and limited.

The role of Internal Audit

Organisations must recognise the heightened strain on their finance teams due to challenging macroeconomic conditions. Internal Audit teams should conduct thorough reviews of investment and financing decisions, as well as supply chain and procurement practises. Additionally, Internal Audit should assess management's approaches to identifying, evaluating, and mitigating risks associated with inflation and interest rates, which includes undertaking scenario analyses to prepare for potential adverse scenarios.

Operational resilience

The persistent flux in economic, geopolitical, and environmental conditions present new threats and opportunities to organisations, highlighting the need for robust and resilient systems.

These systems must adapt to disruptions while protecting stakeholders, maintaining critical business processes and safeguarding the performance of key technology and information systems. Australia's evolving regulatory environment also demands greater focus on resilience. For example, the Security of Critical Infrastructure Act 2018 (SOCI) reflects Government's expectations for the continuity of essential services, and provides a framework designed to uplift security and resilience across all hazards – both natural and human induced.

Organisations are investing in people, processes, data, and technology to enhance resilience and take preventative measures against disruption risks. They must also maintain a 'final line of defence' through Crisis Management, Business Continuity, Emergency Management, Incident Management, IT Disaster Recovery and IT Service Continuity Management.

The role of Internal Audit

Internal Audit is tasked with evaluating the effectiveness of the organisation's operational resilience and crisis management frameworks. This involves verifying that significant threats have been identified, that suitable response plans are established and effective, and that the consideration of emerging risks and the evolution of key threats is ongoing. Additionally, Internal Audit should ensure that organisations comprehend the impacts of disruptions, determine intolerable levels of risk, and examine the cost-benefit analysis of mitigation and resilience measures.

Talent management and retention

Effective talent management is crucial for organisational success, involving the attraction, retention, and development of skilled individuals. Challenges, such as adapting to hybrid work models, talent acquisition, and employee well-being are at the forefront. In the coming years, emphasis on employee-centric initiatives is expected, including a focus on enhancing employee experiences, engagement, mental health, work-life balance, and professional development. Remote working options and flexibility are increasingly regarded as essential components of employee satisfaction. A strong Employee Value Proposition (EVP) is vital for talent retention, with younger employees particularly seeking alignment between their values and their employer's mission. Furthermore, new legislation from Safe Work Australia under the Work Health and Safety Act 2011 (NSW) (the WHS Act) highlights the importance of managing psychosocial hazards and ensuring resilience in workforce through effective work and role design. Strategic HR planning and organisational design are integral to achieving business objectives and mitigating risks. Additionally, the rapid evolution of AI is set to influence job roles, operational methods, required skills, and overall organisational culture.

The role of Internal Audit

Internal Audit should evaluate the organisation's strategies for workforce planning, future skill requirements, talent acquisition, and retention. It is crucial to comprehend the implications of employee turnover and hiring freezes on the internal control environment and the broader organisational impact. Moreover, assessing management's oversight and plans to improve employee-centric aspects is an essential component of Internal Audit's role.

Key thematic areas to consider in 2025

Technology

Unveiling the Global Evolution of Innovation and Connectivity

In the dynamic landscape of technology in 2025, global developments are catalysing transformative shifts across industries. The rapid advancement of artificial intelligence (AI) and machine learning technologies continues to redefine operational paradigms, enabling unprecedented automation, optimisation, and decision-making capabilities. Regulatory frameworks like the European Union's General Data Protection Regulation (GDPR) and evolving global standards, underscores the imperative for organisations to prioritise robust cybersecurity measures in their technological endeavors.

Holistically, organisations' risk management processes need to be more prognostic and dynamic than ever before to navigate these challenges. Below we have included the three main areas of focus:

Cybersecurity

Cybersecurity will remain a top focus for organisations into 2025 and beyond. This is due to the increasing sophistication of cyber threats, the digitisation of customer channels, the adoption of new technology platforms and the ever-growing volume of sensitive data constantly moving across interconnected and integrated networks.

We have continued to see a rise in cyberattacks and data breaches in 2023-2024, and these attacks can affect organisations of all sizes and industries with a range of security systems. Organisations are recognising the importance of improving cybersecurity and data protection, including increased transparency around data use.

Organisations will need to implement robust IT security measures and increase awareness of cybersecurity risks to their workforce to resist and evade the constant threat of cyberattacks.

The role of Internal Audit

Internal Audit should assess existing controls to mitigate cybersecurity risks and ensure that the first and second line of defence are continuously monitoring cybersecurity controls. This includes undertaking a controls assessment against relevant regulations or industry standards.

Internal Audit can also provide valuable assurances through undertaking targeted reviews around user access management, data management and incident response. A technical assessment, such as a vulnerability assessment or penetration test, will help determine if your organisation has external vulnerabilities that could be exploited in a cyber-attack.

Data privacy and governance

Customers, employees and regulatory bodies have all become more aware of their data privacy rights concerning personal information and the measures taken by organisations to safeguard such data.

Recent high profile data breaches have demonstrated the importance of understanding key data repositories, key controls and use of data. This heightened awareness amplifies the potential risks faced by organisations, necessitating their commitment to compliance with Federal or State based regulations such as the Australian Privacy Act 1988 (Cth), Privacy and Data Protection Act 2014 (VIC), Privacy and Personal Information Protection Act 1998 (NSW).

Failure on the part of an organisation to effectively manage and govern its data practices may result in loss of customer trust, reputational damage, and could lead to the imposition of regulatory actions, financial penalties and sanctions.

The role of Internal Audit

Internal Audit should assess the data privacy and protection controls within an organisation to ensure it is clear what data the organisation has collected and why this occurred as well as where the data will be stored & transferred, if it is secure, how long the data will be retained for and how it is disposed of in line with any regulation & organisational needs..

Internal Audit should also evaluate data breach response plan design, readiness and interlock with third-party data breach response plan.

Additionally, ensure a comprehensive understanding of whether third parties have access to the organisation's data and, if so, how this access is monitored and controlled.

Digital disruption & emerging technology

There has been a current trend incline in the use of AI technology by businesses. AI can be a major business enabler for an organisation through harnessing the power of generative AI and processing complex data.

Nevertheless, it is essential for organisations to be aware of the accompanying risks and to proactively address them, particularly by focusing on the ethical deployment of these emerging technologies within the organisation.

Digital transformation is continuing across industries, with cloud often central to these transformations. If used correctly with strong governance and management controls, it presents many benefits to organisations, such as cost reductions through further system automation reducing human error and facilitating better collaboration within an organisation.

The role of Internal Audit

Internal Audit should assess the digital transformation strategy to further provide advice on governance and control matters. This includes review of the design and controls around emerging technologies, including cloud transition, DevSecOps, zero trust architecture and distributed ledgers.

Internal Audit can review how and why AI is being used by organisations and what controls are in place to mitigate the risks that occur with using AI. This includes data, reliability, accountability, governance, security and privacy. KPMG's Trusted AI Framework outlines our strategic approach to reviewing AI solutions to ensure they are established and controlled in a responsible and ethical manner.

Contact us:

Clare Power
Partner
t: +61 423 024 386
e: clarepower@kpmg.com.au

Craig O'Hagan
Partner
t: +61 414 296 438
e: cohagan@kpmg.com.au

Philip Masters
Associate Director
t: +61 408 337 429
e: pmasters@kpmg.com.au

KPMG.com.au