KPMG

Shaping the future: Key thematic areas for Internal Audit in 2025

December 2024

—

www.kpmg.ch/iarcs

Key thematic areas for Internal Audit in 2025

Internal Audit functions face a risk environment that is continually evolving and 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 organizations' risk and control frameworks, necessitating vigilant and strategic responses.

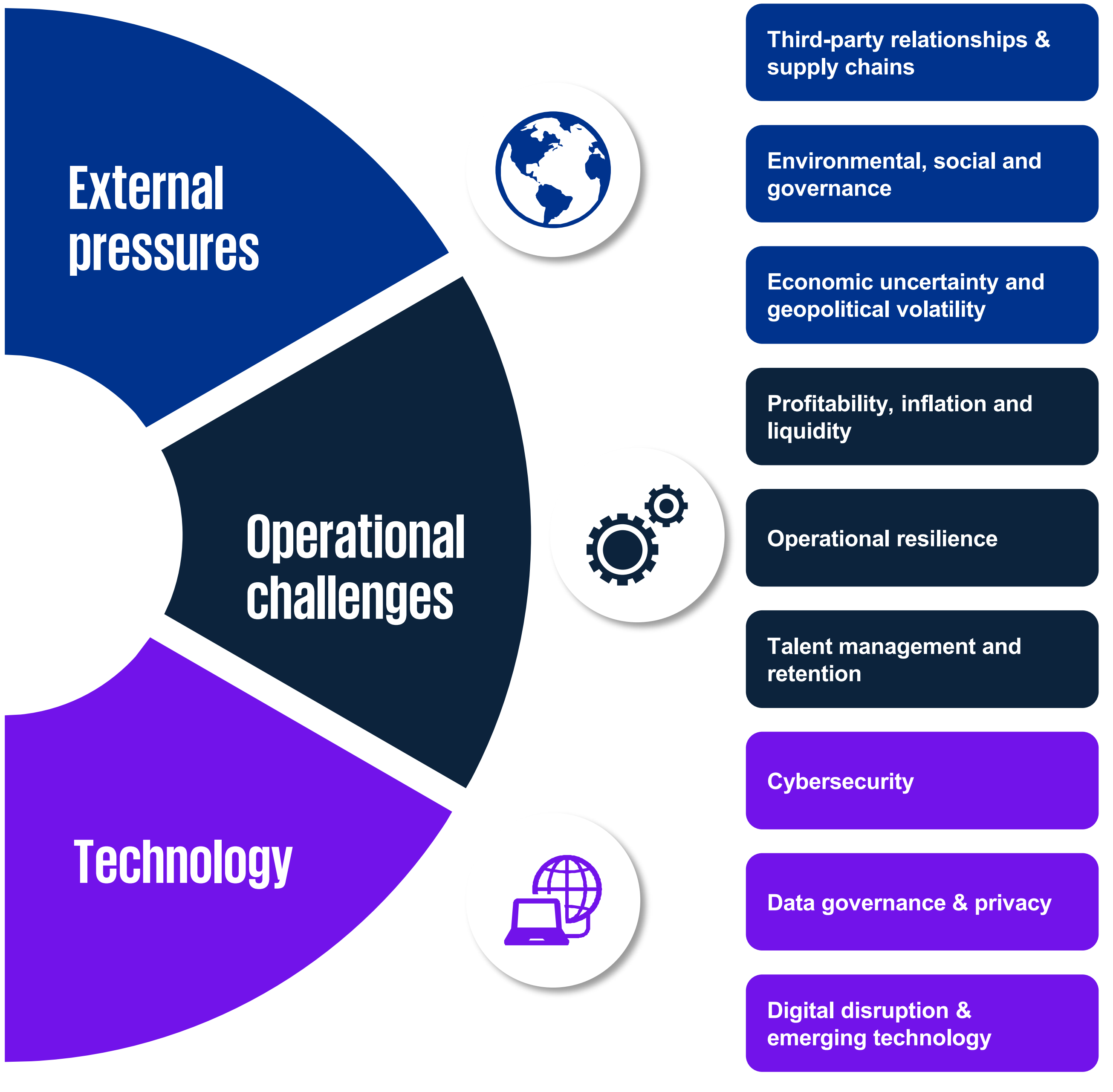
Overview

To assist the heads of Internal Audit, we have compiled a portfolio of the key thematic areas and corresponding risks that Internal Audit functions should consider when formulating forward-looking Internal Audit plans for 2025.

These themes encompass a range of both emerging and established risks that should be applied when creating 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 organization's risk and control status for the forthcoming year.

Detailed insights on each identified thematic area are presented on the next few pages.



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 the economy. These influences encompass a range of factors including disruptions in supply chains, surges in inflation, 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 organizations become more predictive and agile than ever to effectively face these challenges. We have highlighted the three main areas of focus:

Third-party relationships & supply chains

Geopolitical uncertainties have created volatile macroeconomic conditions and exerted great strain on global supply chains. While the impact of these events is 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, organizations are compelled to assess the transparency, ethics and ESG implications inherent in their collaborations with third parties that support their operational activities.

The role of Internal Audit

Internal Audit should go beyond contract management and assess the maturity and resilience (and concentration) of supply chains, provide 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.

Environmental, social and governance

Switzerland has made significant progress toward sustainability by amending its Code of Obligations to introduce non-financial reporting and due diligence requirements. These regulations, inspired by international standards such as the EU's Non-Financial Reporting Directive (NFRD), require public interest entities and large companies that exceed specific thresholds regarding FTEs, revenue, or balance sheet total to report annually on various ESG topics. These include environmental, social and governance factors, as well as compliance with specific due diligence obligations, such as those related to conflict minerals and child labor.

Although Switzerland is not part of the EU, its approach aligns with global trends. The Federal Council encourages companies to integrate recommendations like the Task Force on Climate-related Financial Disclosures (TCFD) into their reporting. However, this remains largely voluntary. Furthermore, Switzerland is closely monitoring the EU's Corporate Sustainability Reporting Directive (CSRD) and its adoption of the European Sustainability Reporting Standards (ESRS). While there are no immediate plans for Switzerland to fully implement ESRS, discussions are ongoing about strengthening sustainability reporting frameworks. These regulatory changes require Swiss companies to adapt their business operations to incorporate ESG reporting into their long-term strategic objectives.

The role of Internal Audit

Internal Audit plays a vital role in supporting organizations as they navigate new reporting requirements. It helps assess their readiness for compliance, providing guidance on governance, controls and processes related to ESG metrics reporting.

Additionally, Internal Audit offers strategic advice on aligning risk management capabilities with ESG risks and organizational objectives, while continuously ensuring the effectiveness and efficiency of ESG risk management, internal controls and governance frameworks.

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 and the fragmentation of trade agreements are fueling substantial inflationary pressures. Such geopolitical complexities have helped to perpetuate the elevated prices of commodities like gas and oil. Despite the initial signs of inflation stabilization 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 2025 and beyond. Recognizing that this state of economic flux and geopolitical volatility will constitute the "new normal", organizations 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 must 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 organization's first and second lines of defense are addressing and managing the amplified risks and operational impacts associated with geopolitical volatility.

Operational challenges

Securing success: operational challenges in the digital age

As organizations navigate the operational landscape of 2025, they must anticipate and address a multitude of thematic areas to remain resilient and competitive. The heightened economic, geopolitical and environmental uncertainties are generating new risks, threats and opportunities at an unprecedented pace, impacting the Swiss economy.

Amid the escalating priority of digital transformation, it has become clear that functions need to be more progressive and dynamic than ever before to tackle concerns surrounding operational challenges. The three main areas of focus are:

Profitability, inflation and liquidity

With inflation and interest rates reaching highs not seen since the early 2000s, 2024 has been marked in particular by intense macroeconomic volatility, which has placed considerable financial pressure on organizations worldwide. As these organizations peer toward the horizon of 2025 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 that organizations 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 extends from 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

Organizations must recognize 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 practices. Additionally, Internal Audit should assess management's approaches to identifying, evaluating and mitigating risks associated with inflation and interest rates, which includes performing scenario analyses to prepare for potential adverse scenarios.

Operational resilience

The ongoing changes in economic, geopolitical and environmental conditions present both new threats and opportunities for organizations, underscoring the need for robust and resilient systems. These systems must be agile enough to adapt to disruptions while protecting stakeholders, preserving critical business processes and ensuring the performance of key technology and information systems. Switzerland's evolving regulatory landscape also emphasizes the importance of resilience. For example, the Swiss Federal Act on Data Protection (FADP) and other regulatory frameworks require organizations to prioritize the continuity of essential services and to enhance their security and resilience in the face of both natural and human-induced hazards.

The role of Internal Audit

Internal Audit is tasked with 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 organizations 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 essential for organizational success and includes the attraction, retention and development of skilled individuals. In the coming years, an emphasis on employee-centric initiatives is expected, which includes a focus on enhancing employee experiences, engagement, mental health, work-life balance and professional development. Furthermore, Switzerland's evolving labor laws, such as the Federal Act on Gender Equality, highlight the importance of fostering a supportive work environment and ensuring resilience through effective job design. Strategic HR planning and organizational design play a crucial role in achieving business objectives while mitigating risks. Furthermore, the rapid development of AI and digital transformation will continue to influence job roles, operational methods, required skills and overall organizational structures.

The role of Internal Audit

Internal Audit should evaluate the organization'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 as well as their broader organizational impact. Moreover, assessing management's oversight and plans to improve employee-centric aspects is an essential component of Internal Audit's role.

Technology

Unveiling the global evolution of innovation and connectivity

In the dynamic landscape of technology in 2025, global developments are catalyzing transformative shifts across industries. The rapid advancement of artificial intelligence (AI) and machine learning technologies continues to redefine operational paradigms, enabling unprecedented automation, optimization and decision-making capabilities.

Regulatory frameworks like the European Union's General Data Protection Regulation (GDPR) and evolving global standards underscore the imperative for organizations to prioritize robust cybersecurity measures in their technological endeavors. Holistically, organizations' risk management processes need to be more prognostic and dynamic than ever before to navigate these challenges. The three main areas of focus are:

Cybersecurity

Cybersecurity will remain a top focus for organizations into 2025 and beyond. This is due to the increasing sophistication of cyber threats, the digitalization 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 organizations of all sizes and industries employing a wide range of different security systems. Organizations are recognizing the importance of improving cybersecurity and data protection, which also includes increasing transparency surrounding data use.

Organizations will need to implement robust IT security measures and increase the awareness of cybersecurity risks within their workforce in order 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 lines of defense are continuously monitoring cybersecurity controls. This includes performing a controls assessment against relevant regulations or industry standards.

Internal Audit can also provide valuable assurance by performing targeted reviews of user access management, data management and incident responses.

Data privacy and governance

Customers, employees and regulatory bodies have become increasingly aware of their data privacy rights concerning personal information and the measures taken by organizations to protect such data. Recent high-profile data breaches have highlighted the critical importance of understanding key data repositories, controls and the use of data. This heightened awareness raises the potential risks faced by organizations, necessitating their commitment to compliance with Swiss regulations such as the Federal Act on Data Protection (FADP) and the EU General Data Protection Regulation (GDPR), which also applies to Swiss companies handling data of EU citizens.

Failure to effectively manage and govern data practices can lead to a loss of customer trust, reputational damage and the imposition of regulatory actions, financial penalties and sanctions. Organizations must ensure they have robust data protection measures in place to mitigate risks and maintain compliance with these stringent data privacy laws.

The role of Internal Audit

Internal Audit should assess the data privacy and protection controls within an organization to ensure clarity regarding which data the organization has collected and why as well as where the data will be stored and transferred, whether it is secure, how long the data will be retained and how it is disposed of in accordance with regulatory & organizational requirements.

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

Digital disruption & emerging technology

There has been an upward trend in the use of AI technology by businesses. AI can be a major business enabler by enabling an organization to harness the power of generative AI and process complex data.

Nevertheless, it is essential for organizations 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 organization.

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

The role of Internal Audit

Internal Audit should assess the digital transformation strategy to additionally provide advice on governance and control matters. Furthermore, Internal Audit can review how and why AI is being used by organizations and which controls are in place to mitigate the risks that arise when using AI. KPMG's Trusted AI Framework outlines our strategic approach to reviewing AI solutions to ensure that they are established and controlled in a responsible and ethical manner.

Martin Rohrbach
Partner, Internal Audit, Risk and Compliance Services (IARCS)

KPMG Switzerland
T +41 58 249 71 28
M +41 79 249 85 27
martinrohrbach@kpmg.com

Robin Gerber
Director, IARCS

KPMG Switzerland
T +41 58 249 77 42
M +41 79 675 93 62
robingerber@kpmg.com

Alessandro Gabriele
Senior Manager, Head IARCS Western Switzerland

KPMG Switzerland
T +41 58 249 28 39
M +41 79 870 41 20
alessandrogabriele@kpmg.com

kpmg.ch