KPMG

Internal Audit

Key risk areas to consider in 2024

Internal Audit: Key risk areas to consider in 2024

The continuing uncertainty and disruption across the economic landscape over the recent years are intensifying the pressures on businesses and these have resulted in a number of evolving challenges and risks.

The recent geopolitical events introduce economic uncertainties, necessitating strategic financial planning amid global dynamics. The repercussions span over disruptions in supply chains, adjustments in EU monetary policy, and evolving stakeholder expectations. Organizations must closely monitor and respond to these policy shifts to align financial strategies with the evolving economic landscape.

Besides this, emerging risks due to disruptive technologies and cybersecurity threats, wherein safeguarding digital assets against breaches is imperative for financial integrity. Regulatory changes on the hand pose financial compliance challenges, demanding astute adaptation to evolving legal frameworks.

In light of these multifaceted challenges, organizations find themselves navigating uncharted territory, requiring a more proactive and dynamic approach. On the other hand, the unprecedented nature of the challenges has elevated stakeholder expectations. Organizations must engage in transparent communication, demonstrate resilience, and align their strategies with societal and environmental expectations.

Overall, the current confluence of crisis requires a forward-thinking and adaptive approach to risk management. Organizations in the Belgian economy need to proactively address the challenges posed by these interconnected factors to foster resilience and sustainable growth.

Internal Audit must remain agile and take into consideration all the potential risks when developing with their 2024 internal audit plans. To support the Chief Audit Executives we have compiled the key risks that Internal Audit should consider in developing their Internal Audit plans for 2024. The risks include both emerging and established risks.

The below is not an exhaustive list of key risks and could serve as a basis for Internal Audit functions to assess the organisations risk profile and control environment throughout 2024.

01 Economical and geopolitical uncertainty

02 Operational Resilience

03 Talent management, retention and wellbeing

04 Organizational culture and behaviour

05 ESG (Environmental, Social and Governance) reporting

06 Climate change

07 Cyber security and data privacy

08 Digital disruption and new technologies

09 Third-party relationships and supply chain

10 Regulatory risk

01 Economical and geopolitical uncertainty

In recent years, the global economy experienced some of the most significant rises in inflation and interest rates since the early 2000s.

Belgium's economy has shown resilience over the past years and the recovery from the COVID-19 pandemic has been robust thanks to extensive policy support. There were many other macro-economic shockwaves in 2023, namely the tighter monetary policy by central banks which have generated significant inflationary pressures and strong upward cost pressures related to wage increases. These are expected to weigh on business investment in the coming quarters.

It is important to consider the significant emerging risks such as the conflict in the Middle East which comes on top of disruptions caused by the Russian invasion of Ukraine. The impact of these combination of these risks varies from the commercial, logistical, legal and broader geological level including the complex sanctions regime. Any further increase in energy, gas, oil and commodity prices will exacerbate inflation, the supply and labour market shortages.

Internal Audit response

Internal Audit must remain vigilant to emerging risks and ensure that the first and second lines are identifying and evaluating the risks and potential impact on the organisation. Internal Audit should also participate in top management discussions with respect to (emerging) risks, maturity of the three lines model and governance related matters.

Internal Audit could also review third-party suppliers exposed to economic shifts, and more broadly consider the organization's long-term strategies aimed at mitigating financial and operational risks.

Internal Audit could play a role in identifying and assessing potential immediate gaps or control weaknesses in relation to compliance with the current international sanctions regime and ensuring that a robust framework is in place with appropriate risk mitigation measures that can be applied on an ongoing basis.

02 Operational Resilience

The current economic, geopolitical and environmental risks organisations are facing, highlights the importance of robust and resilient systems. Events such as the pandemic and Ukraine conflict demonstrate the interconnectedness of risks and the concentration of risk when events occur. Preparedness for disruption is critical to not only survive disruption but thrive through it. Organisational resilience can be further reinforced through investment in people, data and technology.

The pandemic placed pressure on the resilience, flexibility and skills of workforces to maintain operations safely. Many organisations subsequently developed a disaster recovery plan and business continuity procedure. Similarly, organizations need to ensure that their business continuity planning and crisis management processes are adequate and continuously updated in order to respond to other threats, such as cyber threats, natural disasters, other disease outbreaks, or political instability. Failure to do so could result in high-level disruptions.

Operational resilience is an important and frequent discussion for management boards, with many organizations having to navigate difficult times through recent global crises. However, organizations should seek a long-term model that allows them to not only ''keep the lights on'' and survive a crisis, but to grow despite unfavourable conditions.

The role of Internal Audit

Including operational resilience in the Internal Audit scope will ensure the organisation is aligned with the best practices to prevent, respond and recover from crisis.

Internal Audit could assess the quality of the overall crisis management system, by ensuring that key threats have been identified and appropriate response plans are in place and tested during emergency exercises. Another aspect for Internal Audits to consider is the governance around crisis decision-making and the integrity of data and information reported to crisis committees.

Internal Audit reviews whether the business continuity or crisis response plans are fit for purpose and whether emerging risks and evolving key threats have been considered.

The objective will be to help the organisation better understand the impact of the disruption and to determine the corresponding mitigating/resilience response.

Pre Crisis

- Recurrent update of crisis management framework and contact list
- Recurrent update of BCP (BIA, RTO's and control measures)*
- Raising awareness in the organization &recurrent training of key persons
- Recurrent crisis simulations

Crisis

- Notification
- Facts gathering
- Evaluation matrix
- Activation of the appropriate governance body

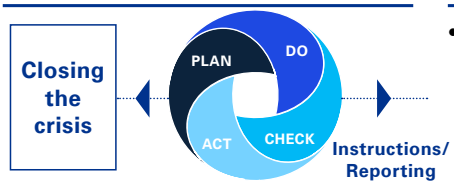
Post Crisis

- Implementing recovery measures
- Crisis evaluation
- Implementing improvement actions

Composition

- Managing director
- Process owner
- Internal / external advisor
- Crisis Management Team
  - Chairman CMT
  - Communication
  - Logistics & infrastructure
  - HRM
  - ICT
  - Secretary

Strategic Governance



Operational

- Execution of tasks
  - by departments
  - by taskforces
  - crisis communication

03 Talent management, retention and wellbeing

The availability and retention of talent remains a key risk area in the aftermath of the COVID-19 pandemic, where people move at an accelerating pace in the labour market. Whilst uncertainty exists around potential macro-economic impacts talent remains a key issue for organisations.

In Belgium, the risk of talent acquisition persists due to low unemployment resulting in a continued skills and talent shortage. Organisations are faced with a smaller pool of talent who increasingly demand flexible work, attractive remuneration and personal alignment with the organisation's purpose and social responsibility agenda.

With the adoption of new ways of working, the risks associated with talent are increasing and these include hybrid working, culture and wellbeing.

According to the Belgian FPS Employment, Labour and Social Dialogue, work-related psychosocial risks affect both the mental and physical health of workers impacting on productivity, along with the erosion of purpose and culture. These risks stem from the working conditions and interpersonal relations at work. These risks could be mitigated through measures to prevent psychosocial risks at work, prevent any harm that results from these risks or limit this harm.

Technological advancements give rise to a new set of risks such as new learning methods, talent upskilling to meet a more digitised future and other exposures to due remote working.

The role of Internal Audit

Internal Audit could assess the risks that the organisations face in terms of workforce planning and future skill demand, talent acquisition, and talent retention strategies. These should incorporate succession planning, capability management, remuneration benchmarking, wellbeing programs and training and development.

Internal Audit must understand the ramifications of employee departures and hiring freezes on the internal control landscape and how these factors may affect the organization. Additionally, Internal Audit should evaluate how management oversees and plans to enhance the employee-centric factors.

Internal Audit could assist the organization in developing talent metrics that are consistent with the relevant business risks.

When developing the audit plan the risks around people and talent could be integrated in other audits or tackled in a more agile way and by demonstrating leadership and empathy to work through solutions with management.

04 Organizational culture and behaviour

A culture of trust within an organisation and towards its internal and external stakeholders is fundamental for its success. It is critical for organisations to understand and implement an appropriate culture and standards of integrity.

In recent years there was been a shift in the mindset and companies that ignore HR insights and focus solely on making money without building a strong organization and culture could face problems in the long run.

One example is that employees are choosing the employers on choice based on factors such as flexibility, workplace culture and existence of strong social values rather than solely renumeration.

The health of a company's culture is often better indicated by shared values, communication, trust, and openness. Soft controls, like these intangible aspects, have a big impact on how individual employees behave and perform. Paying attention to these softer elements not only keeps a company's culture strong but also predicts the organisation success in the long run.

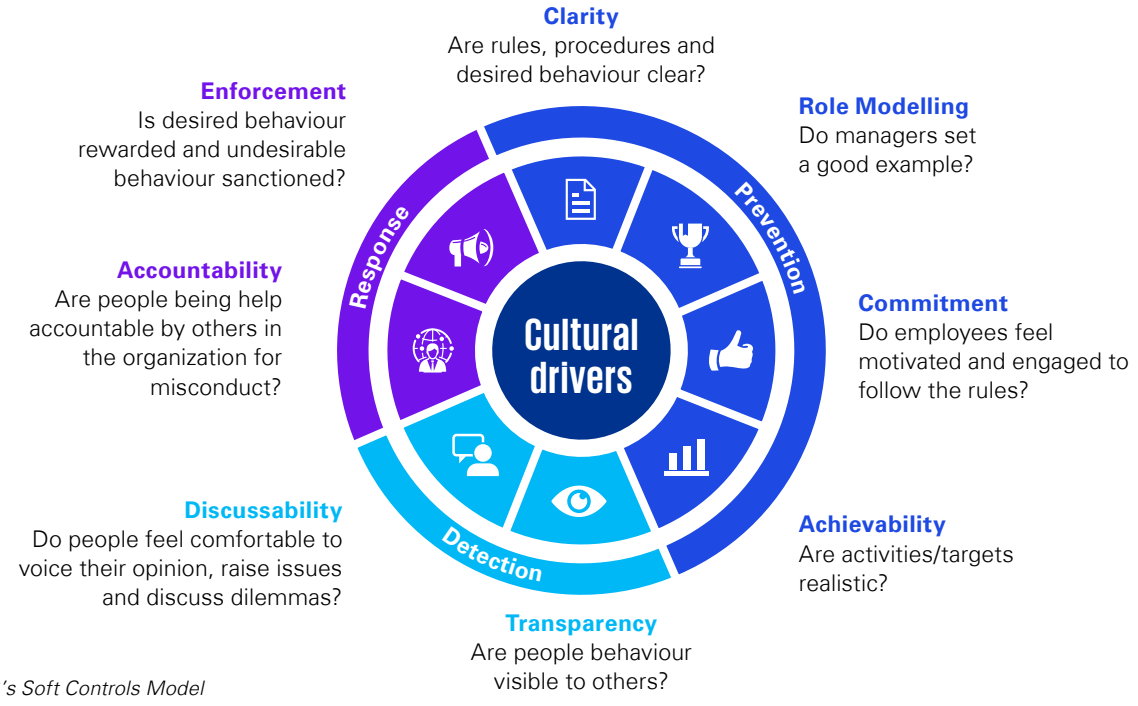
The role of Internal Audit

Internal Audit could assess whether the policies on diversity, equity and inclusion are compliant with applicable regulations and the effectiveness of controls are in place.

Internal Audit can also assess the current level of employee alignment with the organization's values and identify potential fraud risk. Alternatively Internal Audit could perform staff surveys, supplemented by interviews with leaders, key individuals and second line professionals in order to assess the perceived corporate culture.

Besides this, it could review the effectiveness of the soft controls instruments, which are measures in place to support the effectiveness of an organization's culture.

Culture audits should be a recurring topic in the internal audit plan to continuously assess the effectiveness of soft controls.



KPMG's Soft Controls Model

05 ESG (Environmental, Social and Governance) reporting

ESG is now fundamental for long-term financial success and the biggest evolution is the inception of the EU Corporate Sustainability Reporting Directive (CSRD) in corporate reporting.
With the first CSRD reports due in 2025 — for companies with year-ending 31 December 2024 —the clock is ticking. Organisations are required to implement appropriate governance structures to respond to ESG-related topics and to provide reliable and useful information on their ESG risks and opportunities.

The extent of the obligations is proportional to the company's size and resources, and nature of business, with larger companies and those operating in high-risk sectors and/or regions facing greater demands.

The role of Internal Audit

A potent and integrated ESG governance structure serves as a vital catalyst for sustained organizational success in the ESG domain.

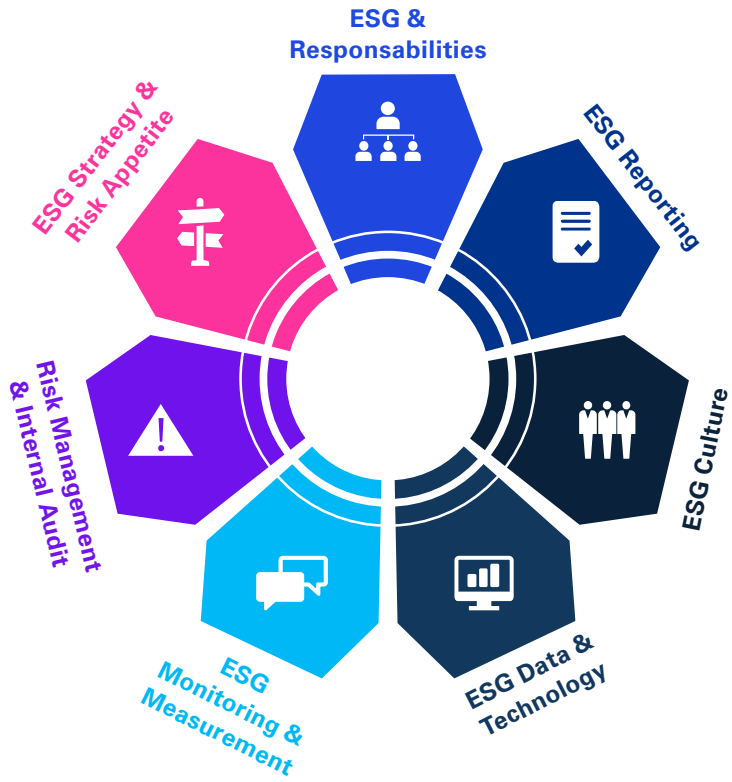
For organisations still at an infancy stage and with no immediate reporting requirements, Internal Audit have numerous roles from consultative assistance to comprehending ESG risks. Internal Audit can simultaneously contribute to shape and fortify the governance frameworks and control ecosystems. This entails the seamless integration of ESG considerations into the day-to-day operational processes of the organization, fostering a comprehensive approach to ESG. Risks and opportunities should be managed alongside other risks throughout the organizational spectrum.

For organisations who are required to be compliant in 2024, Internal Audit should assess CSRD reporting and provide assurance on relevant governance frameworks, organizational strategies, and the integrity of ESG reporting.

ESG Integrated Governance Model

The ESG Integrated Governance Model is a proven methodology to help organizations understanding and managing their risks and opportunities on an integrated manner, and in line with their risk appetite and strategy.

The model can easily be tailored upon the organization's specific needs in order to enhance the existing GRC framework implemented and optimally integrate specific ESG related risk management



06 Climate change

Recent years have shown that the direct consequences of climate change are impacting the global population as well as organizations. This summer for example, extreme temperatures have caused reduced agricultural yields in Belgium. This has impacted, according to a report commissioned by the National Climate Commission, two of Belgium's most iconic products, beer and fries.

The challenges and risks that organizations face in achieving their sustainability goals and minimizing their contribution to climate change will not decrease over the coming years. Coupled with this, investors, regulators, customers and employees are increasingly expecting organizations to operate with a sustainability lens on everything they do.

The role of Internal Audit

Internal Audit has a key role to play in establishing whether the organization is prepared to face a climate crisis and in supporting the organization to effectively manage climate change risks. Internal Audit can examine this area at the operational level, given its deep understanding and knowledge of the processes that relate to and are impacted by sustainability, from materials sourcing to transport and logistics and waste management.

07 Cyber security and data privacy

Cybersecurity will remain a top focus for organizations in 2024. This is due to the ever-growing volume of sensitive data moving across interconnected and integrated networks and the increasing reliance on digital technology to operate efficiently. There is a global consensus that the volume of risk factors is increasing. Remote working and the speed at which new technologies, such as the adoption of cloud-based and recent developments in AI are contributing to this trend.

We have continued to see a rise in cyberattacks and data breaches in 2023, and these attacks can affect organizations of all sizes and industries. The attacks may result in high costs for organizations to fix the problem and repair the damage caused.

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. This heightened awareness amplifies the potential risks faced by organisations, necessitating their commitment to compliance with regulation such as the General Data Protection Regulation (GDPR). Failure on the part of an organisation to effectively manage and govern its data practices may result in reputational damage, and it could also lead to the imposition of financial penalties and sanctions.

The role of Internal Audit

Robust IT security measures and increased awareness are fundamental to mitigate the risk of cyber-attacks. Internal Audit should assess the existing controls to mitigate cyber security risks and ensure that both the first and the second line defences are continuously monitoring cyber security controls.

This could be done through assessing the veracity of controls to mitigate cyber security risks and consider applying the NIST Cyber Security Framework based around Identify, Protect, Detect, Respond and Recover. Example reviews could include Cyber Security governance, Identity Management, Awareness and Training, Security Assessment of Cyber Controls (including detection and response management), Data Security practices, Incident Response and Recovery strategies.

Internal Audit should assess the Data Privacy and Protection controls in place in an organisation. They to obtain assurance on the reasons that the organisation has collected the data, where the data will be stored, whether it is secure, how long they plan on retaining this data and how it is disposed of in line with any regulation.

Internal Audit should also 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.

08 Digital disruption and new technologies

There was a rapid progression and transformation of digital technologies over the recent years which includes Artificial Intelligence (AI), Predictive Analytics, Cognitive Computing, and Robotic Process Automation. These technologies introduce new and emerging risks which are not necessarily fully understood or taken into account by many organisations.

AI is a major business enabler and is being capitalised in enterprises of various types. On the other side, the organisations should also be aware of the risks associated to proactively address them.

Similarly, the benefits of cloud computing ranges from cost reductions to better collaboration. Accompanied with a strong governance and management controls the risks could be mitigated.

The role of Internal Audit

The internal audit function can contribute to guiding the organization in enhancing the efficiency of its recurrent processes through the incorporation of cutting-edge technologies, while concurrently disseminating insights and expertise concerning the adoption of novel technological advancements throughout the organizational landscape.

With regards to governance and control matters, Internal audit should understand how AI is being used by the organisations to identify the risks and assess the adequacy of controls to mitigate the risks.

09 Third-party relationships and 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, emphasising the imperative to diversify supplier portfolios and avoid undue dependence on a single source.

Organizations are increasingly reliant on third-party suppliers to deliver business-critical products and services to their clients and customers. Organizations are also finding that failures by third parties can significantly impact their ability to operate effectively and can tarnish their societal trust and reputation. In order to mitigate this third-party risk, organizations should develop clear strategies for the selection, approval and management of third parties.

In addition, given the evolving regulatory landscape and increasing stakeholder expectations, organisations are compelled to assess the transparency, ethics, and ESG implications inherent with 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 prioritising flexibility and continuity, we expect to see this continued focus on resilience and sustainability of supply chains.

The role of Internal Audit

Internal audit could assess the end-to-end procurement process, with particular attention to sourcing and third-party risk, supply chain logistics and continuity processes and the distribution of that risk across suppliers.

On top of the above, Internal Audit can review the contract management framework including scorecards to monitor third-party relationships on an ongoing basis and provide a comprehensive overview of all the outsourcing arrangements.

Depending on the size and risk exposure of the organisation Internal Audit can go further to assess the maturity and resilience of supply chains, as well as to provide advice on the suitability of the supply chain operating model. Internal Audit could also determine whether risks associated with current macroeconomic and geopolitical conditions and ESG were considered.

10

Regulatory risk

The regulatory landscape is becoming more and more complex and subject to constant change in areas such as technology, disruption, ESG and data privacy for all organisations irrespective of the industry they are operating in.

The complexity and pace of these regulatory changes exerts significant pressure on top management. Compliance to the regulations can be ensured by adopting an agile approach.

The role of Internal Audit

In order to effectively evaluate an organization's compliance with regulation, the internal audit function must gain a comprehensive understanding of the existing regulatory landscape for the industry the organization currently operates in

Contact us

Olivier Elst
Partner Risk & Assurance
KPMG in Belgium

M: +32 (0)485 17 83 48
E: oelst@kpmg.com

An Vanderhulst
Principal Risk & Assurance - Corporates and Public sector
KPMG in Belgium

M: +32 (0)473 55 43 12
E: avanderhulst@kpmg.com

Muriel Van Loo
Director Risk & Assurance – Financial services
KPMG in Belgium

M: +32 (0)478 87 64 76
E: murielvanloo@kpmg.com

kpmg.com/be