



# **Internal Audit Key risk areas 2023**

In a continuously changing world full of uncertainties, Chief Audit Executives and Internal Audit functions must remain agile when establishing their risk landscape and developing their 2023 audit plan.

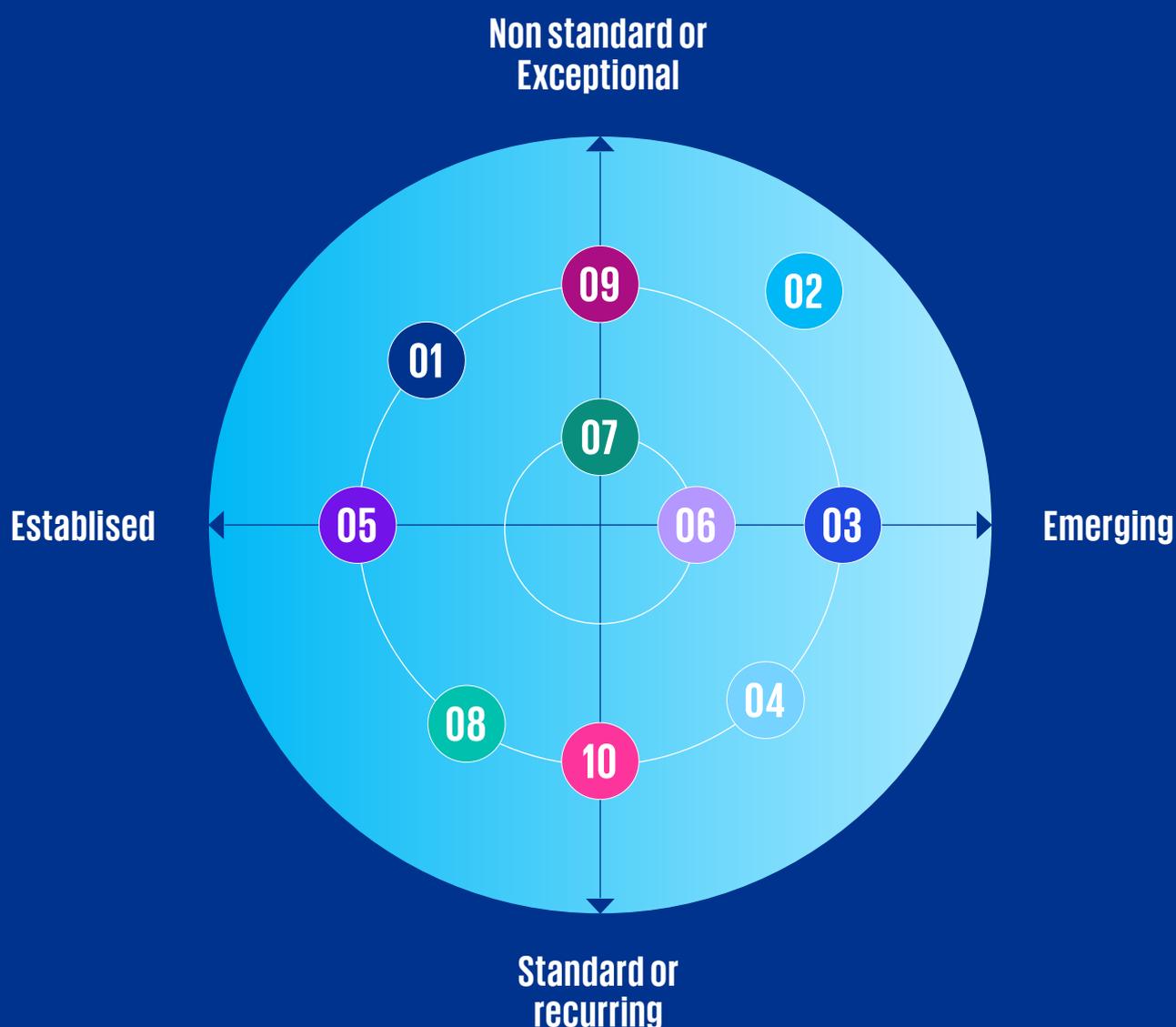
In a post COVID-19 world, where organizations are still facing several challenges (e.g., supply chain issues, changing workforce mindset, etc.), the last few months have shown that we should always be on the lookout for new threats and challenges. The skyrocketing inflation as well as geopolitical issues will be impacting many organizations.

These new developments are accompanied by emerging risks that the Internal Audit function should take into consideration in its risk assessment and (dynamic) annual plan, without neglecting the key established risks. As a result, we present you our recommended key areas for focus for FY23.

- |           |   |           |   |
|-----------|---|-----------|---|
| <b>01</b> | <b>Economical and geopolitical uncertainty</b>              | <b>06</b> | <b>Organizational culture and behavior</b>        |
| <b>02</b> | <b>Climate change</b>                                       | <b>07</b> | <b>Third-Party relationships and supply chain</b> |
| <b>03</b> | <b>Talent acquisition and retention</b>                     | <b>08</b> | <b>Digital disruption and new technologies</b>    |
| <b>04</b> | <b>ESG (Environmental, Social and Governance) reporting</b> | <b>09</b> | <b>Business continuity and crisis response</b>    |
| <b>05</b> | <b>Cyber security and data privacy</b>                      | <b>10</b> | <b>Mergers and acquisitions</b>                   |

We believe that this publication serves to provide insights to Chief Audit Executives on the key risk areas to take into consideration when developing their 2023 audit plan. As further guidance, we have mapped the top 10 risk areas on a Risk Radar (refer to visual 1). The Radar presents two spectrums:

- 1 **Established key risk areas** that should have been identified and understood by the IAF, versus **emerging risk areas** that are developing, but whose full understanding has yet to be obtained.
- 2 **Non-standard/exceptional risk areas** that should be considered for a one-time audit, versus **standard/recurring risk areas** that should be considered on an ongoing basis.



# Internal Audit: key risk areas to consider in 2023

## 01 Economical and geopolitical uncertainty



The strength of recovery in the global economy, the shift in spending patterns to goods rather than services, and the COVID-19-related disruptions in logistics networks have generated significant inflationary pressures. These pressures have not eased in recent months; the war in Ukraine has caused severe economic consequences in Europe and in case the Netherlands with global ramifications. It is important to consider its various commercial, logistical, legal and broader geological impacts (including the complex sanctions regime). Furthermore, due to the unprecedented increase in gas and oil prices, but also in commodity prices, the inflation continues to rise and the purchasing power of many households is declining. As a controlling measure, the different central banks have started to raise interest rates. These ongoing global developments are creating new day-to-day risks in the commercial agenda of global organizations.

### The role of Internal Audit

Consider how the first and second lines of responsibilities (based on the 'Three Lines model') are identifying and assessing where these risks and pressures are likely to impact the organization. Internal Audit should also review third-party suppliers exposed to economic shifts, and more broadly consider the organization's capital planning and management, net interest margins, credit/default risk and debt recovery, claims management and business cases for future investments.

Internal Audit can also 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 to help maintain compliance. Last but not least, Internal Audit can play a role as sparringspartner for senior management with respect to (emerging) risks, maturity of the 3 Lines model and governance related matters.

## 02 Climate change



Recent years have shown that the direct consequences of climate change are impacting the global population as well as organizations. This summer, extreme temperatures have caused new issues such as reduced container ship transport due to alarming declines in river flows, reduced agricultural yields, and even direct damage to infrastructure. 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.

## 03 Talent management and retention



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 labor market. High employee turnover rates are causing disruptions for many organizations, and competition to secure the talent they need is fierce. Employee wellbeing remains under severe strain, increasing the risk of talent loss, fatigue and the associated impact on productivity, along with the erosion of purpose and culture.

Every employee's voluntary departure is extremely costly to the organization in terms of business disruption, recruiting and onboarding. Organizations

need to understand the changing workforce mindset and design long-term incentive and compensation programs to increase retention.

### The role of Internal Audit

Assess the organization's workforce planning and future skill demand, talent acquisition, and talent retention strategies. These should include succession planning, capability management, remuneration benchmarking, wellbeing programs, and training and development. Internal Audit should assist the organization in developing talent metrics that are consistent with relevant business risks.

## 04 ESG (Environmental, Social and Governance) reporting



While specific ESG reporting is in its infancy, like the EU Taxonomy, there is a rapid movement that ESG reporting requirements will be broader and all-encompassing. The EU Corporate Sustainability Reporting Directive (CSRD) amends the current Non-Financial Reporting Directive (NFRD) and from 2024 onwards, under the CSRD, companies will



start reporting according to the mandatory EU sustainability reporting standards. Therefore, all organizations are already encouraged to ensure they have appropriate governance structures in place to properly respond to ESG-related topics, and to provide reliable and useful information on their ESG risks and opportunities.

Organizations should define their ESG disclosures and metrics and identify the data to be captured and curated in order to comply with new European and local ESG regulations in a timely manner.

### The role of Internal Audit

For organizations that are in the early stages of their ESG journey, internal audit should provide advisory support in understanding ESG risks, and support the design and development of robust governance frameworks and control environments.

For organizations further progressed on their ESG journey, internal audit should provide assurance on relevant governance frameworks, organizational strategies, and the integrity of ESG reporting. Compliance with ESG risk management and applicable legislative requirements should be assessed.

## 05

## Cyber security and data privacy



Remote working and the speed at which new technologies, such as cloud-based platforms, are being adopted, coupled with global players increasingly using cyber disruption as a critical tool in their arsenal, means that organizations must remain vigilant to their cyber security risk. This accentuates the need for greater scrutiny of IT security and increased workforce awareness of malicious and non-malicious cyber attacks.

In a data-driven world powered by digitization, regulators continue to increase their vigilance, and data privacy and protection continue to pose significant challenges to organizations. The European Union General Data Protection Regulation (EU-GDPR), in force since May 2018, should not be overlooked by organizations. Continued focus on compliance with the EU-GDPR will prevent large penalties and reputational risks.

#### The role of Internal Audit

Assess the veracity of controls to mitigate cyber security risks and consider applying the NIST Cyber Security Framework: 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), Post Covid-19 New Ways of Working Review, Data Security practices, Incident Response and Recovery strategies.

Assess privacy and data protection controls with respect to how and what data is collected, used, stored, secured, retained and disposed of. This should be in accordance with regulatory requirements and industry-leading practices. Consider the management of organizational data to which third-party providers have access. Perform a gap analysis against proposed legislative reforms, or a maturity assessment against the EU-GDPR (or AVG in the Netherlands).

## 06

## Organizational culture and behavior



Organizations are held accountable by their internal and external stakeholders for encouraging an appropriate culture and standards of integrity. In order to achieve this, there is a need to define a set of values to which employees should adhere within the organizations. For example in the banking industry, weak culture has been linked to many historic incidents of loss or fraud. That has led European banking supervisors to increase their focus on risk culture. De Nederlandsche Bank (DNB), which began assessing banks' behaviour and culture in 2011, was a pioneer in this area. Furthermore, management needs to provide adequate oversight and set clear policies (e.g., Anti-bribery and Corruption) and expectations. Because ultimately, it is the behavior of the people that drives decision-making and thus influences the performance of the organization and the effectiveness of the controls in place.

#### The role of Internal Audit

Soft controls audits aim to generate discussion, share best practice and enhance 'in control' activities. Internal audit typically look for evidence that diverse views are being aired, that those voices are heard, that robust debate is taking place and that leaders are open to challenge. Audit make use of staff surveys, supplemented by interviews with leaders, key individuals, and second line professionals. Internal Audit should continue to conduct soft control audits to provide assurance on the current culture in the organization and its impact on the effectiveness of the controls in place.

Asses the current level of employee alignment with the organization's values and identify potential fraud risk through the use of data analytics.

## 07

### Third-party relationships and supply chain



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.

The latest global and European developments continue to impose significant pressure on global and domestic supply chains, from production delays and labor shortages to shipping disruptions and increased commodity pricing. This is expected to continue at least through 2023.

#### The role of Internal Audit

Assess the end-to-end procurement process, with particular attention to sourcing and third-party risk, and the distribution of that risk across suppliers. Assist the organization in establishing a contract management framework, scorecards to monitor third-party relationships on an ongoing basis, and comprehensive overview of all the outsourcing arrangements.

Review supply chain logistics and continuity processes, including ESG-related risks and the management of third-party cyber security risks in their operating environments.

## 08

### Digital disruption and new technologies



Digital disruption, transformation and adoption of new technology have accelerated during the last few years, including Artificial intelligence (AI), Predictive Analytics, Cognitive Computing and Robotic Process Automation. These new technologies bring with them new risks, such as those relating to data and cloud storage, usage and privacy, and should not be overlooked.



#### The role of Internal Audit

Assess the digitalization strategy and program along with associated risk management controls, provide assurance over specific digitalization projects, including AI design integrity, algorithm testing, exception management and remediation, change management controls, third-party provider and software vendor management. Provide advice on governance and control frameworks to ensure that AI and bot risks are monitored and mitigated in the long term (after implementation).

Internal audit can also play a role in advising the organization to make their (repetitive) processes more efficient by implementing new technologies and sharing knowledge about the use of new technologies across the organization.

## 09

# Business continuity and crisis response



Many organizations were taken aback by the COVID-19 crisis and have subsequently developed a disaster recovery plan and business continuity procedure. They must 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.

### The role of Internal Audit

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. Internal Audit should review whether the business continuity or crisis response plans are fit for purpose and whether emerging risks and evolving key threats have been considered. Internal Audit should also seek evidence of the governance around crisis decision-making and the integrity of data and information reported to crisis committees.

## 10

# Mergers and acquisitions



After COVID-19, a mergers and acquisitions boom accelerated, with global mergers and acquisitions reaching new record highs. Mergers and acquisitions pose unique 'delivery' and 'delivered' risks during this period of rapid change and the need to realize the benefits of the transaction.

### The role of Internal Audit

Develop an integrated merger risk assurance strategy and plan. This will allow for informed decisions and awareness of the types of assurance the merger will obtain during its life cycle, from real-time assurance through to 'go' / 'no-go' live assurance. A range of focus areas may include: control due diligence of the target entity and remediation plans, governance and integration reviews, IT roadmap planning, supply chain consolidation and business case achievement.



# Contact



**Bart van loon**

Governance, Risk & Compliance Services  
Partner  
VanLoon.Bart@kpmg.nl  
T +31 6 53 24 93 28



**Liane Lambert Mendez- van Eerde**

Governance, Risk & Compliance Services  
Senior manager  
vanEerde.Liane@kpmg.nl  
T +31 6 53 75 26 36



**Huck Chuah**

Governance, Risk & Compliance Services  
Partner  
Chuah.Huck@kpmg.nl  
T +31 6 46 36 60 13



**Maxime Georges**

Governance, Risk & Compliance Services  
Manager  
Georges.Maxime@kpmg.nl  
T +31 6 83 00 01 60

**KPMG.nl**

**home.kpmg/socialmedia**



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2022 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.  
All rights reserved.