KPMG

Internal Audit Key risk areas 2023

kpmg.com/cn

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 organisations 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 organisations.

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.

01 **Economical and geopolitical uncertainty**

02 **Climate change**

03 **Talent acquisition and retention**

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

05 **Cyber security and data privacy**

06 **Organisational culture and behavior**

07 **Third-Party relationships and supply chain**

08 **Digital disruption and new technologies**

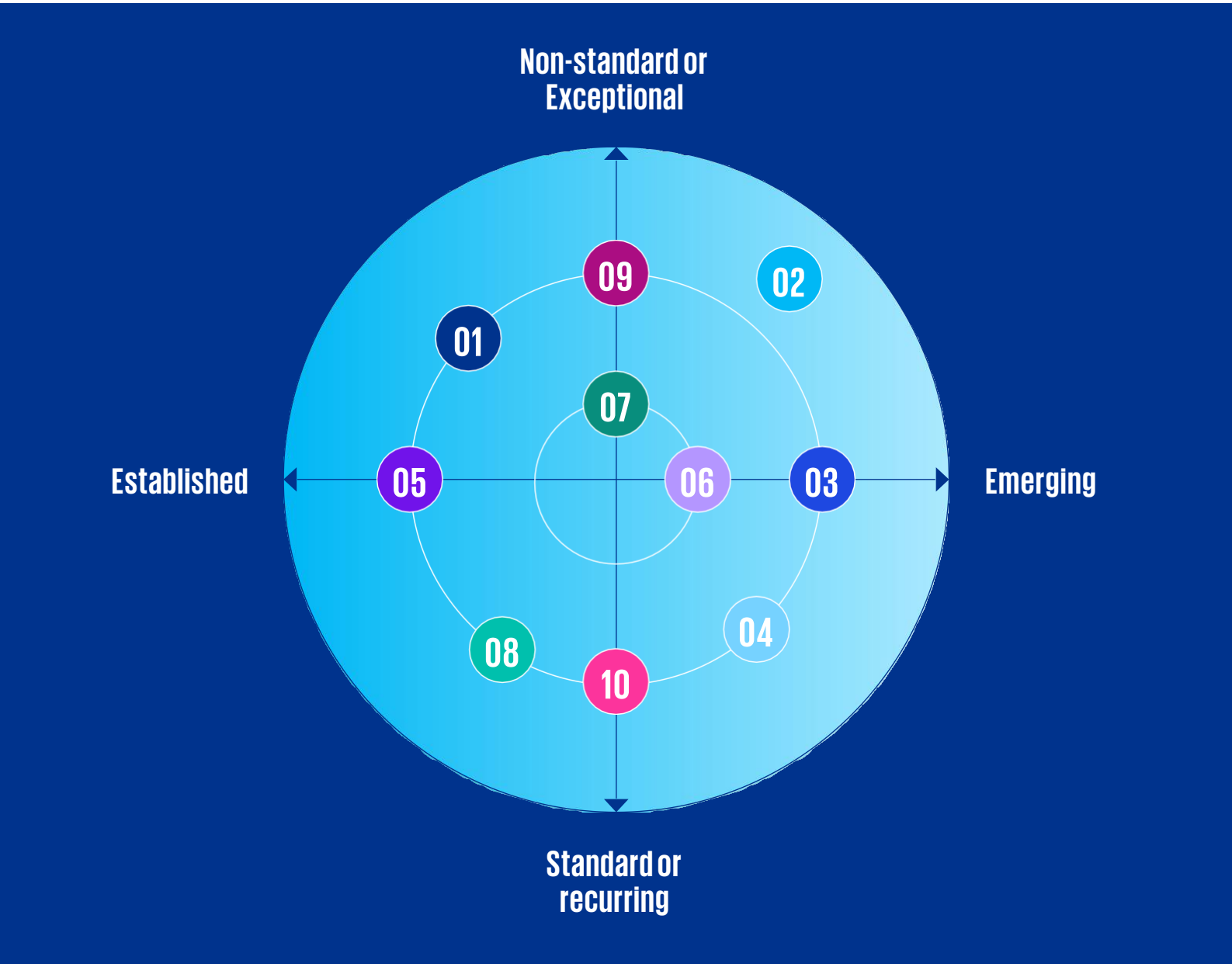
09 **Business continuity and crisis response**

10 **Mergers and acquisitions**

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 Internal Audit Function, 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.

When it comes to the ongoing situation in Ukraine, it is important to consider 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 organisations.

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 organisation. Internal Audit should also review third-party suppliers exposed to economic shifts, and more broadly consider the organisation'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 sparring partner 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 organisations. This summer, extreme temperatures have caused new issues in the global 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 organisations face in achieving their sustainability goals and minimising their contribution to climate change will not decrease over the coming years. Coupled with this, investors, regulators, customers and employees are increasingly expecting organisations 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 organisation is prepared to face a climate crisis and in supporting the organisation 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 labour market. High employee turnover rates are causing disruptions for many organisations, 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 organisation in terms of business disruption, recruiting and onboarding. Organisations 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 organisation'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 organisation 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, there is a rapid movement that ESG reporting requirements will be broader and all-encompassing. The HKEx's ESG reporting requirements have incorporated certain key recommendations of the Task Force on Climate-Related Financial Disclosures (TCFD). Meanwhile, Hong Kong's Green and Sustainable Finance Cross-Agency Steering Group has announced plans for mandatory TCFD-aligned climate-related disclosures by 2025.

Therefore, all organisations 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.

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

The role of Internal Audit

For organisations 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 organisations further progressed on their ESG journey, internal audit should provide assurance on relevant governance frameworks, organisational 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 organisations 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 digitisation, regulators continue to increase their vigilance, and data privacy and protection continue to pose significant challenges to organisations. The relevant laws and regulations such as Personal Data (Privacy) Ordinance (PDPO) in Hong Kong, the Personal Information Protection Law (PIPL) and the Data Security Law (DSL) in China, and the General Data Protection Regulation (GDPR) in European Union should not be overlooked by organisations. Continued focus on compliance with the relevant laws and regulations 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 organisational data to which third-party providers have access. Perform a gap analysis against proposed legislative reforms, or a maturity assessment against the relevant laws and regulations.

06 Organisational culture and behavior

Organisations 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 organisations. For example in the banking industry, weak culture has been linked to many historic incidents of loss or fraud. That has led local banking supervisors to increase their focus on risk culture. Hong Kong Monetary Authority (HKMA) has launched self-assessment on bank culture and culture dialogues with individual banks.

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 organisation 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. Audits 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 organisation and its impact on the effectiveness of the controls in place.

Assess the current level of employee alignment with the organisation’s values and identify potential fraud risk through the use of data analytics.

07 Third-party relationships and supply chain

Organisations are increasingly reliant on third-party suppliers to deliver business-critical products and services to their clients and customers. Organisations 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, organisations should develop clear strategies for the selection, approval and management of third parties.

The latest global developments and pandemic continue to impose significant pressure on global and domestic supply chains, from production delays and labour shortages to continued shutdowns on major ports and associated shipping disruptions and increased commodity pricing. This is expected to continue at least through 2023.

The role of Internal Audit

Assess scenario and contingency plans, including in supplier contracts and service continuity within these.

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 organisation 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 digitalisation strategy and program along with associated risk management controls, provide assurance over specific digitalisation 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 organisation to make their (repetitive) processes more efficient by implementing new technologies and sharing knowledge about the use of new technologies across the organisation.

09 Business continuity and crisis response

Many organisations 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 realise 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

Frank Mei
Partner, Head of Governance,
Risk and Compliance, China
+86 (10) 8508 7188
frank.mei@kpmg.com

Alva Lee
Partner, Head of Governance,
Risk and Compliance, Hong Kong
+852 2143 8764
alva.lee@kpmg.com

Johnson Li
Partner, Governance, Risk and Compliance
KPMG China
+86 (10) 8508 5975
johnson.li@kpmg.com

Kelvin Leung
Partner, Governance, Risk and Compliance
KPMG China
+86 (755) 2547 3338
kelvin.oc.leung@kpmg.com

kpmg.com/cn/socialmedia

For a list of KPMG China offices, please scan the QR code or visit our website:
https://home.kpmg/cn/en/home/about/offices.html