



# Internal Audit: Key Risks & Focus Areas 2021



*Your Partner For What's Next*



# Key Risk Areas & Hot Topics for 2021

---

The impact and influence of Internal Audit Functions continues to expand and evolve. With the backdrop of the wider economic and social challenges presented by an unprecedented global pandemic, the expectations of Internal Audit Functions continues to grow. In particular, for Internal Audit Function to adapt to a changing risk landscape, they need to be agile in all aspect of the audit approach. At times, audit plans need to be flexed; and, methodology and audit approaches adapted to a remote working environment.

With regard to the annual Internal Audit planning process, the key question posed to every Head of Internal Audit continues to be:

## **Are you aware of the key current and emerging risks facing the organisation?**

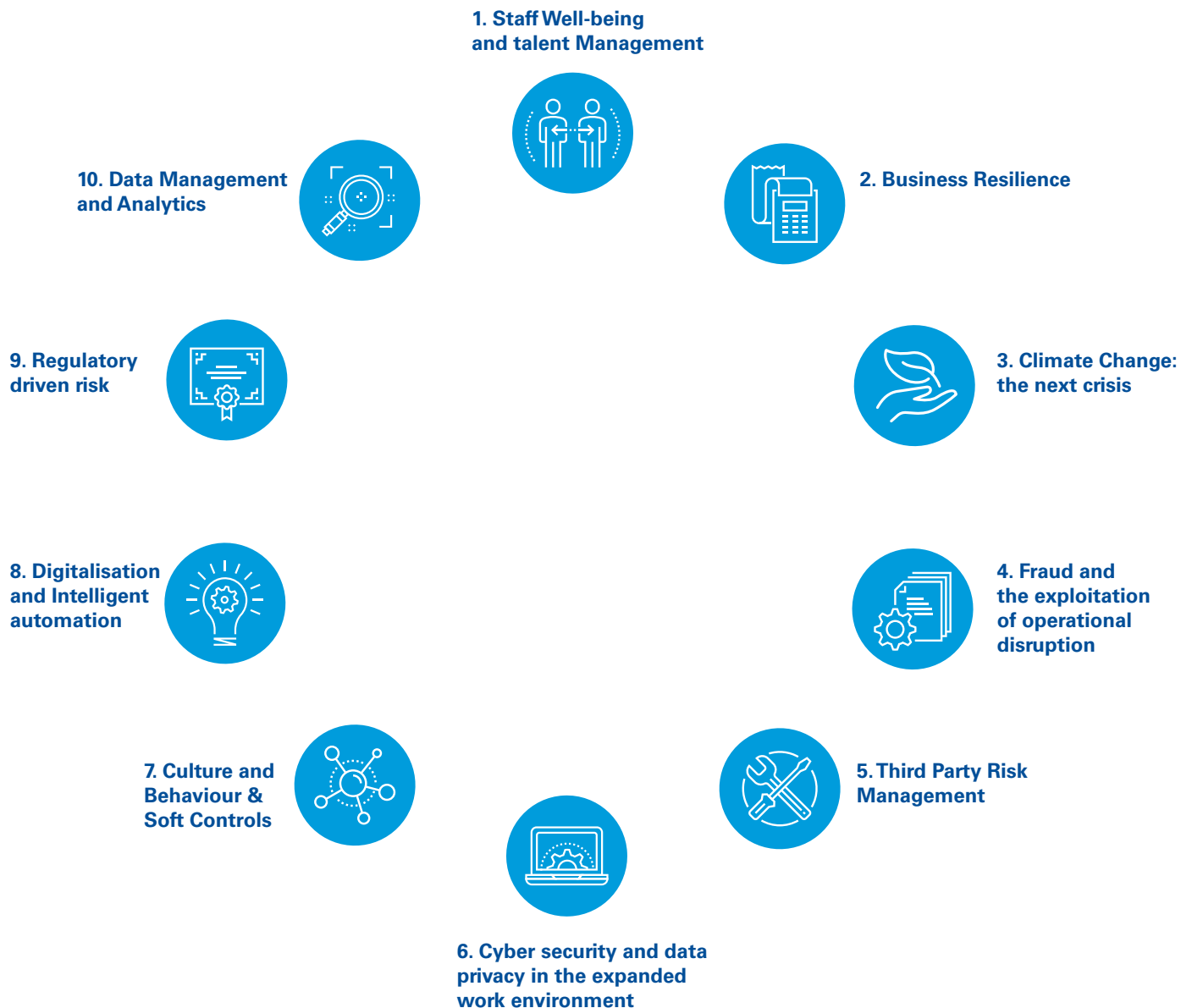
To support Heads of Internal Audit, we have identified and compiled the key thematic areas, 'hot topics' and related risks which Internal Audit functions should consider in developing their Internal Audit plans for 2021.

# Key risks for 2021

---

2020 was and continues to be defined by the global coronavirus pandemic which has had disruptive economic and social impacts across all sectors.

This has set the scene for a new business normal for years to come. These new developments are accompanied by emerging risks that Internal Audit should take into consideration in its annual plan, without neglecting key established risks. In particular, key considerations such as the organisation's business and operational resilience arrangements and its ability to operate remotely should inform internal audit planning in the context of the impact this has had on the organisation's risk profile and control environment.





## 1 Staff well-being and talent management

---

The forced introduction of wide scale remote working as a result of the pandemic has driven changes in ways of working, with a growing trend towards flexible working arrangements and greater autonomy for staff. All businesses should have some degree of skills mapping and forecasting capability to understand and anticipate the organisation's human capital requirements.

**Internal Audit** should look for evidence that the business understands and is forecasting what skills and competencies are required to secure its market position and long-term strategic relevance. There is scope here for culture audits or to include culture elements across all audits, to show how the everyday life of the organisation and the behavior of its staff reflect the adopted values.



## 2 Business resilience

---

Crisis management and planning will have to be updated for the potential for more waves of the coronavirus, not to mention other possible pandemics that follow a similarly rapid contagion path.

**Internal Audit** can review whether the business has carried out reviews to determine how well it is coping with the crisis and whether the business continuity or crisis response plans are fit for purpose, are followed and whether they require updating. Internal Audit should also seek evidence of the governance around crisis decision-making and the integrity of data and information reported to Crisis Committees.



## 3 Climate change: the next crisis

---

Internal Audit increasingly recognises the challenge and risks companies face in achieving their sustainability goals and minimising their contribution to climate change.

**Internal Audit** can assist by establishing how well prepared the business is for the climate crisis and what it is doing to ensure it represents an opportunity for the business as opposed to contributing to the issue. Internal Audit can examine this area at an operational level too, given its deep view into the processes that are related to and impacted by sustainability, from materials sourcing to transport and logistics and waste management.



## 4 Fraud and the exploitation of operational disruption

---

The risk profile will change and fraud risk, in particular, will change significantly after the coronavirus pandemic. The control framework and monitoring of potential criminal activity may have become weakened due to reduced headcount and remote working, leaving gaps in fraud detection and creating opportunities for malicious customers and staff. The pandemic has also presented short term liquidity challenges, leading to cost reduction initiatives which may impact the control environment and monitoring activities.

**Internal Audit** can gain insights into the business's fraud risks by identifying the effects of recent operation disruptions. Internal Audit should identify potential fraud risks, during every audit, and evaluate if the established controls that prevent and recognise fraudulent behavior are still in place and operating effectively.



## 5 Third party risk management

---

Third party risk management remains important as organisations choose to outsource their business functions to third party vendors, emphasising an existing need for contract management. As the pandemic is disrupting the supply chain and business service set-up of many companies, relationships with third parties are changing. Vendor insolvencies have the potential to cause massive disruption and few companies accounted for the risk of outsourcing to overseas territories such as India and parts of Southeast Asia and what this means in the event of a global pandemic lockdown.

**Internal Audit** should take a holistic view towards third party risk management, beyond contract management to assess whether the company has a clear vision and a robust framework to support it.

**Internal Audit** can assess whether the business has paid sufficient attention to the need to remodel supply chains and outsourcing strategies to improve its operational resiliency.



## 6 Cyber security and data privacy in the expanded work environment

---

The wide-scale shift to homeworking arrangements rapidly increased the vulnerability of organisations to cyber attacks as work laptops are now forced to share home WiFi networks. There is also greater potential for controls and safety measures to soften or be circumvented when employees are unsupervised, as they are often overlooked and ignored to save time. Advances in technology also increase the sophistication and frequency of cyber security attacks and frauds.

**Internal Audit** can offer its view on the extent to which any relaxing or adaptation of controls has increased the risk of data leakage or security breaches. Internal Audit should also check whether cyber security awareness is being sufficiently fostered and whether staff training has been updated in light of changes to the working environment and IT infrastructure.

**Internal Audit** should improve the organisation's understanding of cyber security risks and identify possible mitigation strategies to these risks to determine if cyber risks are being adequately managed.



## 7 Culture and behavior and soft controls

---

Recent studies have shown that companies with a clear purpose and an explicit set of values are more successful. They instill trust in products from customers and promote comradery among employees.

**Internal Audit** should continue to conduct soft control audits to provide assurance over the current culture in the organisation and its impact on the effectiveness of the controls set in place.



## 8 Digitalisation and intelligent automation

---

Artificial intelligence, Algorithms, Cognitive computing and Robotic Process Automation (RPA) are among the top technologies that will continue to have a significant impact on the way we conduct business in the future. As digitalisation continues to disrupt operations, business processes and business models, it ultimately brings new risks and challenges in this digital age.

**Internal Audit** can add value by assessing the change management process and recommending enhancements to ensure that governance, risk and control matters are appropriately considered across the change life cycle. In addition, Internal Audit can play a significant role, whilst maintaining independence, of advising on governance and control matters relating to the digital transformation strategy.

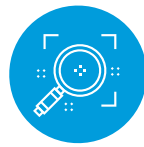


## 9 Regulatory driven risk

---

Organisations, regardless of industry, are being inundated with new regulatory requirements. These new regulations place growing pressure on executive management and add complexity to the organisational governance and control structure.

**Internal Audit** needs to have a strong understanding of the existing regulatory landscape in which the organisation operates in order to assess compliance with relevant regulatory laws and regulation.



## 10 Data management and analytics

---

Increased digitisation of data and technological advances, provide businesses with the opportunity to leverage the value in data to support decisions making. The adoption of data analytics tools is becoming more common place. It is therefore essential that organisations not only identify the opportunities but also the risks associated with the adoption of these tools and capabilities into their operations and decision making processes.

**Internal Audit** are uniquely positioned to advise the business on the risks associated with an over dependency on data analytics tools, in particular any complex business models. Internal Audit play an important role in recommending the development data quality controls and can provide assurance that the data used to support business decisions is appropriate.



# Contact us



**Patrick Farrell**

Partner  
Risk Consulting

**t:** +353 1 7004029

**e:** [patrick.farrell@kpmg.ie](mailto:patrick.farrell@kpmg.ie)



**Claire Heeley**

Managing Director  
Risk Consulting

**t:** +353 87 050 4080

**e:** [claire.heeley@kpmg.ie](mailto:claire.heeley@kpmg.ie)



**Neil Taaffe**

Director  
Risk Consulting

**t:** +353 87 7441648

**e:** [neil.taaffe@kpmg.ie](mailto:neil.taaffe@kpmg.ie)

## **kpmg.ie**

© 2020 KPMG, an Irish partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

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 endeavour 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. The KPMG name and logo are registered trademarks of KPMG International Limited ("KPMG International"), a private English company limited by guarantee.

If you've received this communication directly from KPMG, it is because we hold your name and company details for the purpose of keeping you informed on a range of business issues and the services we provide. If you would like us to delete this information from our records and would prefer not to receive any further updates from us please contact [unsubscribe@kpmg.ie](mailto:unsubscribe@kpmg.ie). Produced by: KPMG's Creative Services. Publication Date: December 2020. (6780)