www.pwc.de

Risk Management 2025 and beyond – priorities and transformation agenda for the banking industry

pwc

Foreword

Dear readers,

On behalf of the PwC network, I am pleased to present the second edition of our global study on the future of Risk management. This follows the successful 2018 publication of our "Risk Mandate and Organisation" in which we surveyed leading international banks on the topic of the future of the Risk function. Throughout the entire industry, there was a consensus that extensive restructuring of the Risk function was necessary to deal with social shifts, state-of-the-art technologies and intense price pressure. Over the past three years, the financial industry has driven the strategic reorientation of its business and organisational models forward – with considerable variances in both their degree of maturity and progress attained. Framework conditions also changed fundamentally at the same time, while the list of challenges faced by the international finance sector remains endless – the COVID-19 pandemic, political instability, the shift in climate and societal values, regulations, low interest rates and digitalisation are increasingly putting the flexibility and resilience of banks to the test.

As part of our current "Risk Management 2025 and beyond – Priorities and transformation agenda for the banking industry" global study, we conducted more than 80 interviews with senior Risk professionals concerning the main Risk management trends and subsequently drafted an in-depth transformation agenda for banks for the period up to 2025 and beyond. This study was reinforced by feedback from numerous banks regarding the "measurement" of the Risk function. A total of more than 1,500 data points provide gripping insight into the status quo, as well as prospects for Risk management. With unprecedented glimpses into the perspectives of leading banks and decision makers with regard to Risk management opportunities and potential, this study makes a substantial contribution to the discussion of how to overcome challenges. It is clear that the role of the Risk function and the Chief Risk Officer (CRO) is undergoing a period of dramatic transition.

First of all, CROs, Risk managers and their teams deserve much praise. Financial risks will always represent a cause for concern for banking, but banks worldwide are much better positioned today in terms of capital and liquidity. Risks have been greatly reduced, and the balance sheets and assets which do not represent the core business which were amassed in connection with the rapid growth over the last decade have been streamlined. Efficiency was increased further, for example through better capabilities at banks, in establishing counter-cyclical buffers against credit losses anticipated for the future. The ongoing crises and most recently the pandemic have been well managed to a great extent. From our conversations, it has emerged that a holistic view is increasingly being applied to Risk management, under which in particular expectations for the first line of defense – "the business" – have risen.

An additional priority is perceived in Risk officers and their teams developing innovative approaches to react to both thematic and non-financial risks. There is an increasing focus for the Risk function on cyber risks, fraud, money laundering, ESG and the growing dependence on a complex network of third, fourth and fifth parties. They necessitate new mindsets and courses of action, as well as a redirection for staff development and prioritisation and the required capabilities in the areas of Risk.

The lead finding is that Risk functions are becoming more dynamic and flexible and increasingly contribute to leading their banks through a complex and volatile landscape of opportunities and threats. In this context, this cross-departmental function will continue to gain importance within the meaning of integrated Risk management. Looking ahead rather than analysing the past will become the new mantra. This represents a fundamental shift for Risk management, which was traditionally rather quantitative and focused on the past. “Traditional” risk disciplines will be streamlined in years to come by means of digitalisation and reframed to respond to changing customer requirements. At the same time, the Risk profile is shifting to non-financial Risks, requiring new capabilities to be strengthened. We also perceive major advances in the use of technology, in particular with regard to analytics on demand and AI-based solutions to optimise risk management and boost effectiveness.

When these priorities are united, a clear image of the transformation agenda for the Risk management of the future emerges:

- Closer involvement/interlocking of the Risk function for strategy and decision-making processes
- Improvement and dynamism of the (analytical) skill set for stress testing
- Integration and digitalisation of non-financial Risks
- Broad strengthening of operational resilience
- Development of platforms to scale technologies, data and capabilities appropriately

This is reflected by the market: the next five years will continue to result in major changes to the Risk function (and Risk management in the broader sense). As part of our analysis, we have outlined the individual measures required to ensure the success of transforming the Risk function in the near term and which are customised to the size and business model.

I hope you enjoy perusing our study and look forward to your feedback. Please feel free to contact me directly.

Best Regards,

Dr. Sami Khiari
Partner at PwC Deutschland
sami.khiari@pwc.com

Table of Contents

A Background and approach

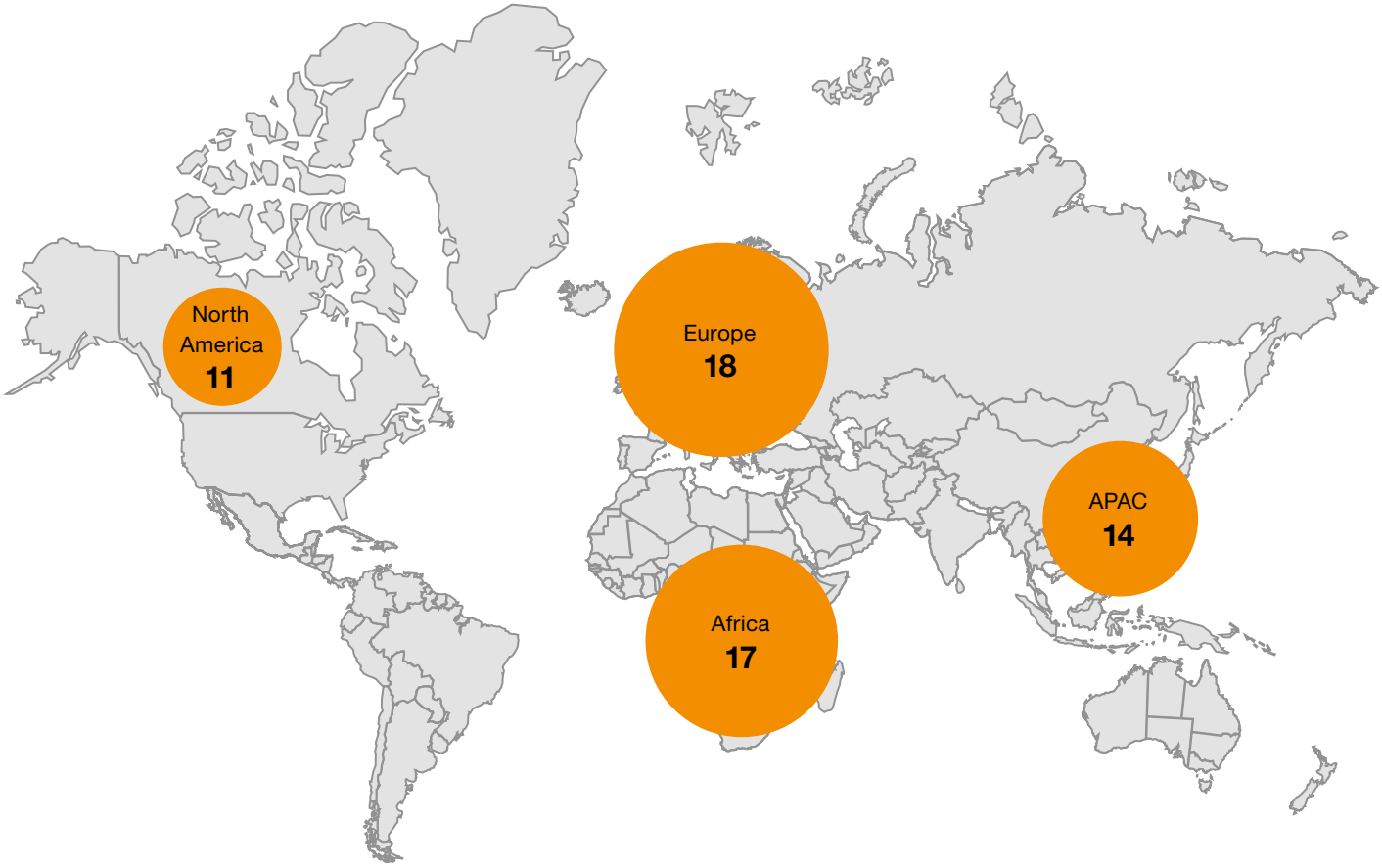
1 Case for an agile and resilient Risk organisation

The PwC 2018 Risk Mandate and Organisation Study highlighted the need for a radical transformation agenda as Risk functions looked to respond to increasing focus on non-financial risks and a growing need to optimise how Risk activities were being performed across the 3 lines of defence.

Over the last three years, the world has become a different place – and this was apparent even before Covid turned it upside down. The topic of climate change has transitioned into the mainstream and this will reshape society. The geopolitical landscape has become less stable with the balance shifting between West and East. In addition, banks are making major changes to their organisation and operating models, driven by pressure to perform and the opportunities provided by new technologies. While this is expected to result in cost reductions of material significance, improved customer experience and enhanced analytics capabilities, in equal measure, it also introduces new risks and amplifies existing risks. In particular, this is increasing the need to think beyond the confines of the institution and raising the prominence of the external risks to which banks are exposed.

We spoke to more than 80 senior Risk professionals across a wide range of global and regional banks to gain their perspectives on key priorities and on the ambitions that exist regarding transformation. Of the 60 banks, 25 participated in an optional standardised questionnaire. The charts in this report are based on the responses provided by participants. Notwithstanding differences in business mix, regulatory environment and operations, we noted a remarkable consensus on many of the key focus areas for the future.

We spoke to 60 banks across different regions



The figure below provides an overview of what we see as the key priorities over the next five years and a related blueprint for change. The following sections provide further details on these topics, including a summary of emerging good practice across the industry.

Change priorities

Interlock between Risk and Business Transformation	Moving from analog to digital – unfinished business around non-financial risks	Preparing for climate change	Preparing for the decade of operational resilience	Joining into the advent of true automation	Managing the generational workforce transition

Overview of the expected transformation agenda over the next five years

Embed Risk in strategy and decision making	Enhance stress testing and analytics capabilities	Digitisation of non-financial risk	Building resilience into the organisation	Building platforms to deploy technology at scale
• Strengthen ERM team with focus on thematic risks, Risk digitisation and insights • Establish competence centers in line 1 and 2 for digital risks and resilience • Break existing silos and build holistic thinking across the lines of defense • Partner with business to digitise the bank and develop new value streams such as digital assets • Embed sustainability in strategy, business model and risk mgmt.	• Build faster and more dynamic scenario analysis capabilities • Enhance ability to capture cross-risk type impacts • Develop agent-based and system dynamics-based tools • Develop structures and tools to identify and assess outlier events	• Simplify policy requirements and focus on materiality • Define data models across non-financial risks and collect enriched data set • Redesign GRC platforms to work for the first line • Anchor non-financial risk management in value streams and transition to continuous assurance models • Build digital risk assistants supporting staff and increasing automation	• Create common awareness and understanding • Rethinking risk appetite concepts and strengthen prominence in strategic decisions • Build visibility of value streams and points of failure • Build capabilities to manage risks in the bank's ecosystem • Rethink business continuity management	• Build a shared technology road map across the organisation • Revisit governance, budget and collaboration models • Strengthen demand management and focus on RoI • Treat data as an asset – prioritise frameworks and infrastructure • Build self-service data analysis capabilities • Invest in reskilling of staff

B Key observations and change priorities

1 Interlocking of Risk and business transformation

Bank business models continue to evolve driven by technology changes, new competitors and pressure on shareholder returns. Risk functions need to pivot their skills, capabilities and infrastructure to lock step with these changes to ensure a future proof and agile control environment. This also needs to be supplemented by strengthening interaction models and processes to support ongoing engagement with business lines and other functions which cuts across risk silos.

Industry observations

Most banks see the need for Risk functions to adjust as traditional value streams are disrupted, forcing businesses to reposition themselves or find new sources of value	While efficiency continues to be important, material cost reduction is not on the agenda for the majority of Risk functions	We also note some additional trends and threats did not come up as much as expected in our discussions which potentially highlights gaps/new considerations as part of risk identification

Blueprint for change

1. Align cost and transformation goals across the end to end processes and capabilities rather than functional silos
2. Further refine and evolve the 3 LoD model across different risk types and priority themes especially cyber, outsourcing, resilience and sustainability
3. Strengthen and further build out the mandate and capabilities of the Enterprise Risk Management function
4. Build focus and scale around risk controls, models and analytics

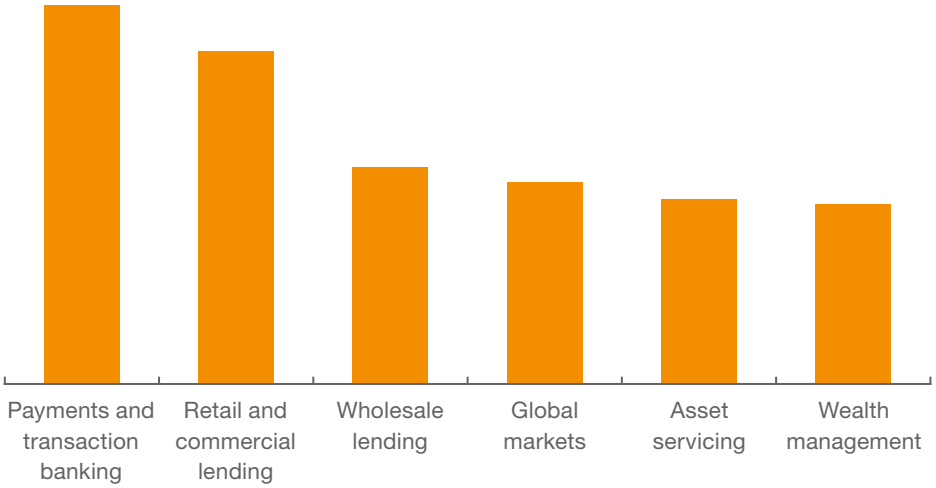
Industry observations

Most banks see the need for Risk functions to adjust as traditional value streams are disrupted and this forces businesses to reposition themselves or find new sources of value

When asked about the business areas expected to undergo the most change over the next decade, most institutions selected payments and transaction banking as their first choice, followed by retail and commercial lending as a close second.

Risk function perspectives on business activities expected to undergo most change over the next decade

Weighted score based on ranking of activities



The key drivers included

- **Disintermediation:** technology and telecommunications companies as well as new competitors are expected to enter the market and decouple payments and transaction services from the banking sector. Furthermore, it is expected that there will be a transition to more open banking architecture and that the prominence of data aggregators will increase. This will have implications for bank-customer relationships and reduce exclusive access to behavioural data, which currently provides a competitive advantage.
- **Introduction of digital assets and crypto currencies:** digital assets are entering the mainstream and it is expected that central banks will launch their own digital currencies. In addition, some of the innovative companies working on distributed ledger technology will likely see their technologies be adopted by different industries. This will reshape business models around payments and settlements, disrupting established market participants but also providing new business opportunities.
- **Advances in infrastructure:** many participants highlighted that payments and settlements are increasingly becoming faster and more convenient. In addition, emerging infrastructure such as decentralised exchanges are seen as emerging alternatives to services provided by a bank.

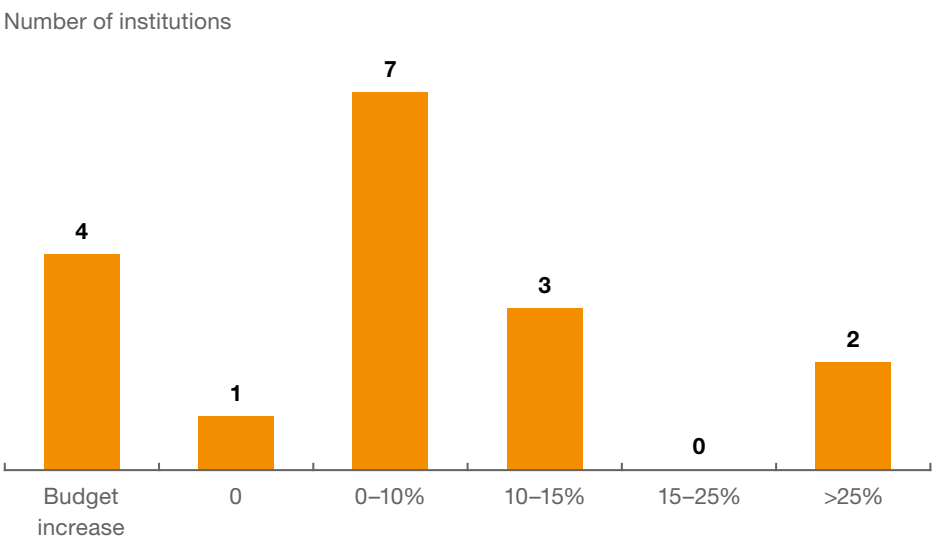
While efficiency continues to be important, significant cost reductions are not on the agenda for the majority of Risk functions

When we conducted the study in 2018, the industry was feeling performance pressure due to the low-interest rate environment and high structural cost bases in many (but not all) institutions. Risk was looked at to contribute to significant cost savings, which were seen as difficult to achieve given the unrelenting nature of the regulatory change agenda and the challenges of legacy data and infrastructure.

Many institutions have since made and continue to make significant progress in automating end-to-end lending journeys, in particular in the retail and small and medium enterprises (SME) businesses. The approach here has been targeted such that it focuses on automating manual activities, such as data sourcing, cleansing and reporting, as well as stepping in earlier to weed out transactions unlikely to go through and identifying and communicating early with at-risk clients. The focus is not just on cost but also on a seamless customer experience, where there is an increasing use of apps with self-service functionality and the ability to position additional products and services of potential interest to the customer. While wholesale lending has not yet undergone the same level of transformation, participants spoke of opportunities to achieve significant efficiencies by leveraging new technologies. This includes, for example, the use of machine learning for the earlier identification of credit applications unlikely to be approved, which can bring about significant savings in the time spent on large and complex deals.

Looking forward, while some individual institutions continued to emphasise significant cost savings targets in excess of 25%, most referred to marginal reductions or even budget increases. However, there is a recognition of the need to be able to do more with less – and efficiency remains a top agenda item across the industry.

Cost reduction targets for the Risk function over the next five years



Certain trends and threats did not come up as much as expected in our discussions and this potentially highlights gaps/new considerations for risk identification

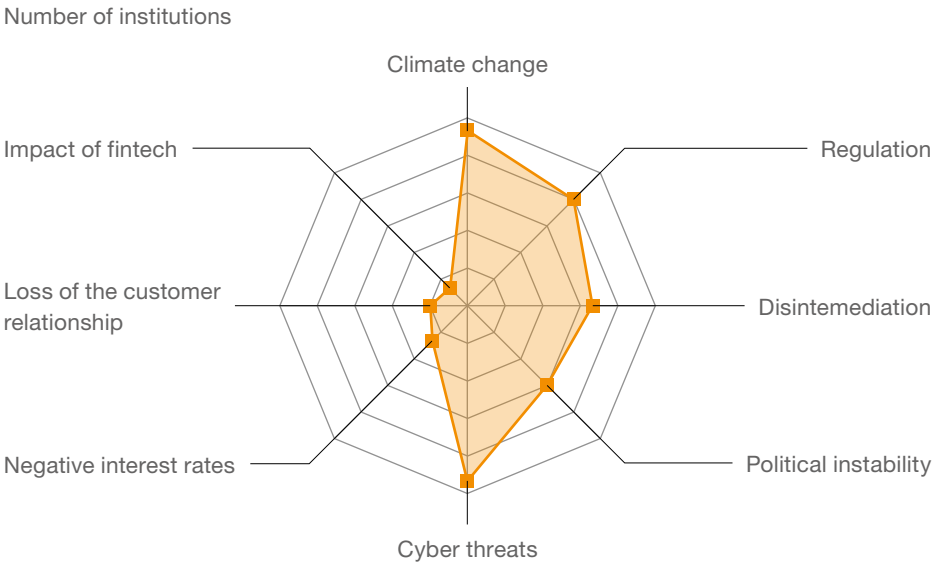
While implicitly covered within digital risks, we see the risks of disinformation as one of the key challenges facing society – yet this was not a topic that was explicitly highlighted in any conversations.

A related priority that we believe will garner greater attention in coming years is how to ensure that data is trustworthy within a much more interconnected economy, especially as increasing volumes of near-time or real-time data become available.

Similarly, the economy emerging around the Internet of things is likely to unlock new business opportunities and in turn compel risk/compliance functions to develop new capabilities.

However, this was not an area which featured prominently in our conversations either and it did not score as highly as other technological innovations in the survey responses.

Risk function perspectives on the largest threats to the banking industry



Blueprint for change

1. **Align cost and transformation goals across end-to-end processes and capabilities**
   Siloed thinking and the difficulties of aligning interests across different parts of the institution continue to pose major challenges to the successful implementation of transformation agendas. The pandemic has shown that it is possible to do things differently and has demonstrated the speed at which it is possible to get things done if some "business as usual" barriers are removed. In particular, we see a need to revisit the way in which the budget and the overall change portfolio is managed and to review accountability structures and incentive mechanisms with a view to enforcing the need for collaboration.

2. **Further refine and evolve the 3 LoD model across different risk types and priority topics, especially cyber, outsourcing, resilience and sustainability**
   While the fundamentals of the 3 LoD model are unquestioned, the question of how to get the best outcomes in managing thematic and non-financial risks came up in conversations in 2018 and remains relevant in our 2021 study. Key focus areas here include thinking about more fluid organisational structures or integrated "units" that straddle first and second line teams. There is also a need to adapt the 3 LoD model to ensure credible and efficient subject matter expertise and the right interaction model, especially in relation to new and emerging risks as well as the oversight of legal entities and smaller locations.

3. **Strengthen and further expand the mandate and capabilities of the enterprise risk management (ERM) function**
   ERM has always had an overarching mandate and is increasingly being positioned as a function "that connects the dots". There are opportunities to further expand capabilities, including developing central risk insight teams within ERM that focus on gaining insights and driving the tooling and data agenda of the Risk function. Further investment areas include better and faster scenario analysis capabilities as well as enhancing the top risks and emerging risks process.

4. **Increase focus and scale of risk controls, models and analytics**
   A consistent objective across banks over the last ten years has been to increase scale by means of cross-functional utilities. While data and reporting have been an established utility that is shared across Risk and Finance functions for a number of years, other areas where such utilities are now beginning to emerge include modelling and analytics (centralising both risk and pricing modelling capabilities) as well as central control teams.

2 Moving from analogue to digital – unfinished business concerning non-financial risks

Most banks struggle to build a close link between performance of controls, specific process vulnerabilities and the loss estimates tagged to non-financial risks. There is equally a recognition of the need for new frameworks, assessment approaches and organisational structures around risk themes like cyber and climate change which can have very diverse impact channels. In addition, holding more capital is not necessarily seen as an effective mitigant against many of the non-financial risks with a need for a stronger focus on resilience and contingency actions.

Industry observations

- There are significant differences in organisation maturity and ambition around non-financial risks
- The interaction model between risk and compliance needs further thought and analysis and remains a complex area for most banks in the context of managing non-financial risks
- First line/line 1.5 control teams have grown exponentially over the past decade, often exceeding second line teams in size
- Firming up risk metrics and making sure that the board has risk-accepted any areas outside of appetite are current priorities shared by many firms

Blueprint for change

1. Restructure non-financial risk policies and procedures to drive effective embedding
2. Define KRIs that are forward-looking and enable an understanding of what drives the aggregate risk profile
3. Replace/augment traditional GRC systems with tools that support flexible changes to controls and a native ability to monitor effectiveness
4. Develop “smart” technology to assist staff and take automation to the next level

Industry observations

There are significant differences in organisation maturity and ambition with regard to non-financial risks

Many institutions have ongoing programmes to transform their approach to non-financial risks and there has been mixed success and progress. The question is often where to start and the challenge is seen as growing exponentially with the size of the institution. The key challenges observed include the following:

- Frameworks and methodologies are not aligned, leading to overlaps and inconsistent practices in the first and second line. This results in different areas within the institution developing their own tools and practices.
- There is a lack of consensus about how and what to measure. While extensive sets of risk indicators and controls exist, these have often been based on what is available rather than what should be looked at.
- Poor data quality and availability often limit abilities to perform even simple analytics. Routine data captured as part of processes such as incident reporting and RCSAs is of mixed quality and granularity and such processes generally do not take advantage of the growing volumes of data being generated by, for example, operational systems and processes.
- There is also a recognition that Risk functions have spent the past decade dealing with incoming regulations while simultaneously facing the burden of large-scale remediation programmes in multiple jurisdictions. There has often been insufficient time to step back and think strategically about how to build scalable solutions within a broader uniform framework so as to provide consistent definitions and ensure that methodologies are embedded in systems. Key examples here include large, poorly maintained control libraries and burdensome anti-money laundering (AML) practices caused by clunky and non-scalable architecture as well as manual processes.

The interaction model between Risk and Compliance functions requires further thought and analysis and remains a complex area for most banks when managing non-financial risks

While there is consensus on the benefit of (and need for) alignment between the Risk and Compliance functions in areas such as definitions, methodologies, lifecycle processes and systems, substantial challenges are faced in bringing this about. In practice, we continue to see varying organisational models.

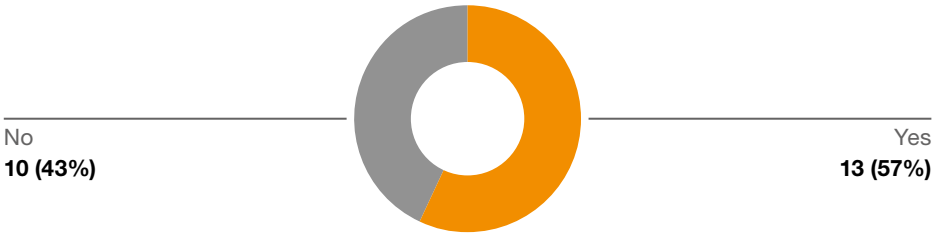
In the case of about half of the participants in our study, the Compliance function reports to the CRO, which is in line with the philosophy that the CRO is ultimately accountable for establishing effective risk management practices and a corresponding culture for all risks. In other institutions, the Risk and Compliance functions are organisationally separate and there are not consistently plans to integrate them in the near future. We also note that while some institutions in territories like Australia have successfully operated integrated Operational Risk and Compliance functions for some time, recent integration attempts by some European institutions have not delivered the expected benefits.

First line/line 1.5 control teams have grown exponentially over the past decade, often exceeding second line teams in size

In 2018, many institutions spoke about redrawing the boundaries of the first and second lines of defence as part of their efficiency initiatives. The execution of these plans has resulted in the transfer of sizable numbers of individuals in some institutions. Although this has brought about a "cleaner" second line, it has shifted rather than structurally reduced the cost base. Apart from this, there were other institutions that expressed unease about any wholesale transfer of activities that could impact the stature of the Risk function in its review and challenge capacity. There was also concern that some areas of the bank lacked maturity and that, considering the potential implications of something going wrong, a practical decision to keep these activities – at least temporarily – within the second line might be a more appropriate option.

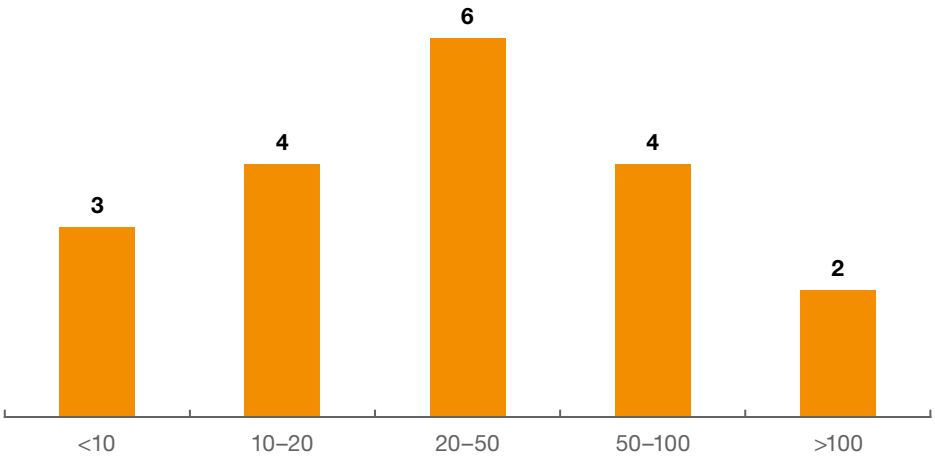
Does the Compliance function report into the CRO?

Number of institutions



Number of indicators included in non-financial risk appetite

Number of institutions per indicator bucket



Current priorities shared by many firms include firming up risk metrics and making sure that the management board has approved risks from any areas outside of risk appetite

While a large number of key risk indicators (KRIs) and controls were in place, there was a strong impression that many of these were designed based on what is readily available rather than what should actually be measured.

Nonetheless, many participants spoke about a significant effort being made to identify and calibrate the correct indicators. The challenge becomes more pronounced in the case of topics like environmental, social and governance matters (ESG), cybersecurity and third-party risk, which require a much better understanding of what the key potential vulnerabilities both within and outside the institution are.

Blueprint for change

1. **Restructure non-financial risk policies and procedures to drive effective embedding across the organisation**
   Risk and Compliance requirements are extensive and complex and are continuously evolving. For the first line, this presents a challenge in fully understanding and embedding the requirements, especially in the case of layered requirements arising from various policies. For example, a few institutions highlighted that deep reviews of the checklists and questionnaires required to be completed as part of the onboarding of third parties resulted in a significant reduction in the number of questions and a much faster onboarding process.

2. **Define KRIs that are forward-looking and facilitate an understanding of what drives the aggregate risk profile**
   While non-financial risk practices are still relatively nascent compared to financial risks, we have noticed an increasing maturity in the design principles for approaching this topic in a structured manner (as compared to the 2018 study). The need for operational resilience is driving much more in-depth assessments of points of failure across organisations and KRIs are being adjusted to focus on what is identified as critical. Greater emphasis is being placed on looking at the same data as decision makers in the first line and – instead of merely monitoring outcomes after the fact – overseeing the decision-making process itself. Data is seen as foundational to the development of more targeted and "predictive" capabilities with significant efforts being made to define the correct data points and to make these accessible in a high-quality format within a single environment. For example, some banks have trained algorithms that are capable of singling out potential incidents and areas of focus and are informed by day-specific market and operational data.

3. **Replace/augment traditional Governance, Risk and Control (GRC) systems with tools that support flexible changes to controls and a native ability to monitor effectiveness**
   GRC systems and the processes built around them have generally been designed with the requirements of second line risk managers in mind. Individual institutions have redesigned the tools to work for the first line and have simplified requirements and user interfaces. To this end, institutions have opted for either reconfigured vendor solutions or in-house platforms. The benefits of this include a significant increase in first line maturity, greater proactivity in identifying risks and issues as well as a substantial reduction in costs.

4. **Develop "smart" technology to assist staff and take automation to the next level**
   AI and machine learning provide the basis for reimagining the possible and the 2021 survey highlighted several examples of this. Many institutions have put more sophisticated tools in place for AML and fraud risks and have also deployed FAQ-style platforms as a self-service tool for staff prior to engaging expensive subject matter experts. At least one bank has gone further and developed digital risk assistants capable of advising employees on specific tasks. This includes formulating questions/checklists for activities such as onboarding third parties, filtering out data and analytics that would be helpful for this task and automating risk and control assessments.

3 Preparing for climate change

Eating an elephant is how one of the banks described climate change. The enormity and uncertainty surrounding evolution of the climate agenda makes it particularly challenging for Risk functions. While the associated events could take decades to unfold, market responses to specific trends and crystallisation of key events could be much quicker. There is a need to establish effective frameworks and operating models to track and act on diverse data sources both for better risk management as well as a potential competitive advantage.

Industry observations

Sustainability was mentioned in passing during our 2018 survey. Three years on, the world has changed as the generational challenge of climate change has transitioned into the mainstream	Climate change and more broadly sustainability as a theme present a range of significant challenges to financial services	While the TCFD report issued in 2017 provided a framework on how to look at transition and physical risks and frame disclosure, regulation is only gradually emerging	While it is clear that firms will need to build capabilities to shape up an informed strategy and build effective and compliant risk management practices, the transition is expected to unfold in an orderly manner	Most institutions have started multi-year programmes in response, looking at this as a joint challenge across strategy, business and risk

Blueprint for change

1. Embed sustainability in the enterprise risk management framework and risk appetite
2. Augment tools and capabilities to identify and assess physical and transition risks as part of risk identification
3. Extend stress testing and scenario analysis capabilities to incorporate climate scenarios and related analysis and reporting requirements

Industry observations

Sustainability was mentioned in passing during our 2018 survey. Three years on, the world has changed as the generational challenge of climate change has transitioned into the mainstream

The Paris accord has led many governments to articulate ambitious targets and develop long-term strategies on how to achieve them. On the regulatory front, Europe has emerged as something of a frontrunner with the Prudential Regulatory Authority (PRA) and subsequently the European Central Bank (ECB) publishing comprehensive expectations for the financial services industry that extend beyond external disclosure. Regulation is beginning to emerge in other parts of the world with the Monetary Authority of Singapore(MAS), for example, recently publishing their expectations.

Climate change and the broader topic of sustainability present a range of significant challenges for financial services

First of all, there is the sheer complexity of how these matters will play out over the coming decades. Transformational change will require the capacity to form a consensus on key policies such as carbon pricing mechanisms. While such arrangements have been emerging on a regional or local-scale, it will take drawn-out negotiations to transition to global solutions.

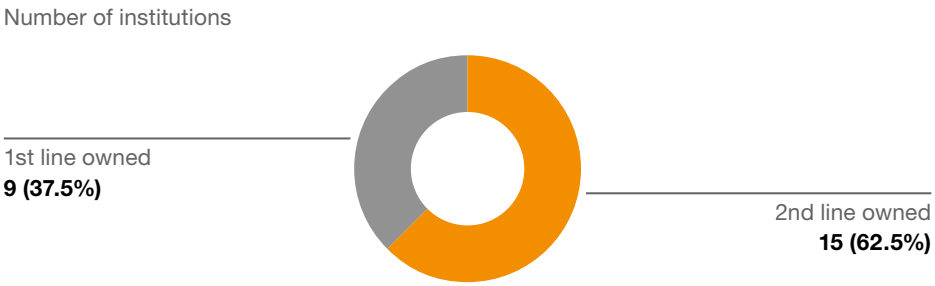
Secondly, it is not the case that one size fits all, as countries have very different characteristics and are hence starting from different positions. This means that while the transition to electric mobility might actually take place in some Western countries within the next decade, there are significant infrastructure bottlenecks in emerging markets that will require major funding to be overcome. Thirdly, there is huge uncertainty as to how actors will behave in such a system, even with regard to who the actors will be to begin with as well as the impact that their actions might have.

While the TCFD report issued in 2017 provided a framework on how to look at transition and physical risks and how to frame disclosure, regulation is emerging only gradually

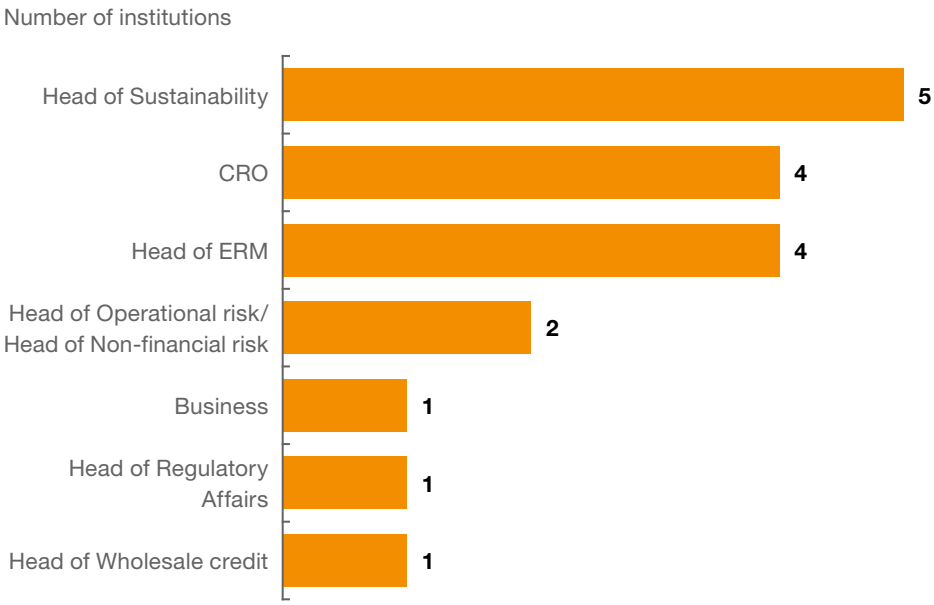
There is a consensus that industry practices will emerge over the coming years with regulators observing what banks are doing and adapting their expectations based on best practices. With regard to how institutions are framing their response to sustainability, we noted several trends:

- Sustainability is seen as a strategic theme rather than as a risk itself – an outlook that is also reflected in regulatory guidelines. However, some institutions have consciously opted to elevate it to the status of a principal risk as this gives it the focus that they feel it deserves.
- Regulators view the Risk function as the first point of contact within an institution; however, many institutions feel that while the Risk function should be prominently involved, it should not be primarily accountable.
- While figuring out the right form of governance and the framing of institutions' responses remain current challenges, there is a broad consensus that this needs to be approached by bringing together strategy, business and risk.
- Most institutions indicate that they have an ESG policy in place. However, responses to the questionnaire indicate that there has been no industry-wide convergence concerning policy ownership to date.

ESG policy ownership – First vs. second line of defense



ESG policy owner – Corporate title



It is clear that firms will have to develop capabilities for formulating an informed strategy and establish effective and compliant risk management practices; nevertheless, it is not believed that the transition is expected to unfold in a disorderly manner

With the post-pandemic situation taken into consideration, several institutions have expressed the view that governments and central banks will be highly reluctant to take any action that could impact an economic recovery and/or damage the fabric of society, which is already viewed as fragile in many countries. Amongst other factors, it is anticipated that emissions pricing is unlikely to get to a level where it will really bite until the mid to late 2030s or that it may even not be emissions pricing but changes in society that will shape the transition.

Nonetheless, there is also recognition of the need to build robust qualitative and quantitative scenario analysis capabilities in order to assess potential impacts if such expectations prove wrong and earlier action brings about a less gradual transition with more painful impacts in some sectors and countries.

Most institutions have started multi-year programmes in response to climate change and view this as a joint challenge encompassing strategy, business and risk

No uniform approach has emerged here but some institutions have had success in identifying key trends, topics and events and in using these to work out where key vulnerabilities are located within their business and organisation, including those that might only materialise over the longer term. Physical risks can draw upon an extensive body of literature and established methodologies, in particular in the area of insurers and reinsurers where capabilities in this regard underpin their business model. However, there is still much for banks to do in defining and building up the necessary capabilities to support modelling and disclosure requirements. Some institutions are investing in building in-house capabilities, while others are considering drawing on external offerings to identify and understand where physical risks may have an impact on their clients or operations.

A key challenge of transition risks is the difficulty of framing the transition and understanding the complexities of how things will play out across the globe. While institutions such as the International Energy Agency (IEA) and the Network for Greening the Financial System (NGFS) have developed various climate pathways and related scenarios that provide useful anchoring points, these require expansion, in particular for scenarios focused on shorter-term time horizons. Data is often not publicly accessible to the extent that it needs to be. This is an area that is seen as requiring further regulatory guidance and potentially some industry solutions.

Blueprint for change

1. **Embed sustainability within the enterprise risk management framework and risk appetite**
   Sustainability is a thematic trend rather than a risk. Institutions have taken different choices when assigning ownership and positioning it within their risk taxonomies. However, the starting point here is to understand how sustainability impacts the institution and its operating environment across different time frames and to determine the respective strategy. This means defining the principles that will ultimately shape how sustainability influences the enterprise risk management framework and risk appetite.

2. **Augment tools and capabilities to identify and assess physical and transition risks as part of risk identification**
   Climate change is such a complex and multifaceted topic that the question of where to start arises. New tools and capabilities are required to identify and assess its impacts and to figure out how to integrate new requirements into business and risk processes. Embedding a catalogue of well-defined accelerated transition and event-based scenarios is emerging as a powerful tool for this purpose.

3. **Expand stress testing and scenario analysis capabilities to incorporate climate scenarios and related analysis and reporting requirements**
   The particularly long-term time horizons and varying risk drivers here will necessitate the development of novel features; however, these will not replace but rather complement existing stress testing capabilities. Data is seen as a key challenge and the view held here is that regulatory standards will be required in various areas to ensure consistency in the information requested from other parties or provided by data firms.

4 Building on the lessons from Covid-19 – never let a crisis go to waste

Risk functions played a key role in sourcing data and insights to meet heightened management and regulatory demands. Looking forward there are a number of learnings from the crisis which we expect to shape scenario design and frequency, change delivery and data driven decision making. For example, none of the stress scenarios designed and run by banks had prepared them for the level of contagion we saw unfold during CoVID19. Similarly the decisive actions by central banks and governments should help shape future expectations on the role of government and regulation.

Industry observations

The Covid 19 pandemic was the manifestation of a scenario that was severe yet implausible; outside the realm of what is considered realistic enough to be taken seriously as part of scenario design, until it happened	Despite the challenges of, in some cases, tens of thousands of staff across the value chain moving to remote working, all institutions were able to maintain operations without major incidents	The financial impact of the crisis was significantly muted by government interventions globally with clear consequences for future expectations around interaction between governments, financial institutions and the broader society

Blueprint for change

1. Review and where required refine risk framework and appetite to effectively monitor risks arising from large parts of the organisation continuing to work partially from home
2. Recast business continuity and other contingency plans around what would drive a resilience to financial and operational points of failure
3. Fundamentally restructure how scenarios are designed and used. Future scenrios need to include agent-based approaches, drive broader participation and challenge across the organisation (and beyond it) and create awareness of strengths and vulnerabilities
4. Build on learnings from the crisis when designing future risk reports and analytics
5. Invest in faster and more dynamic enterprise-wide stress testing capabilities

Industry observations

The Covid-19 pandemic was the manifestation of a scenario that was viewed as severe yet implausible and beyond the realm of what was sufficiently realistic to be seriously considered as part of scenario design – until it happened

Most institutions included a pandemic in their catalogue of stress scenarios. However, these were generally modelled around a SARS-type event and thus limited in terms of their geographical impact and the time frame of their duration. Not a single institution had considered either the global reach and impacts of social distancing over such a long period of time or the much broader implications of a crisis that was not financial in origin. This continued to be the case even when there were growing signs of a global pandemic in early 2020.

Despite the challenges of, in some cases, tens of thousands of staff across the value chain moving to remote working, all institutions were able to maintain operations without major incidents

This has been the first large-scale test of operational resilience across the financial services industry and many stakeholders would not have expected the ability of even complex global institutions to transition to a remote and digital way of operating within such a short time frame. In some cases, this transition included using partial on-site models, while other institutions were actually able to transition smoothly to remote working arrangements within just one week's notice.

Adapting to the crisis did not take place without challenges and participants across the industry spoke of an intense two or three-month period at the outset where the focus was on health and safety, supporting customers and sorting out technology and equipment to ensure operational continuity.

- Staff and customer health and safety were a clear priority across the industry. While many institutions were able to quickly move to remote working arrangements, this was not possible in all areas – at least not immediately.
- Technology and access to equipment was an early area of focus. Many institutions had significantly invested in their remote working and collaboration platforms in earlier years and this paid off during the pandemic by enabling a smooth transition in most areas. Other institutions spoke of initial challenges relating to bandwidth and secure remote connectivity capabilities but highlighted outstanding performances by their IT functions in quickly bringing such capabilities online.
- Customer contact centres were often not equipped to transition immediately to remote working due to a shortage of equipment such as laptops and, in some cases, outdated telephony systems that posed structural challenges. As such, concepts for on-site arrangements were an immediate priority, including those for maintaining social distancing, staggered working times as well as protocols regarding cleanliness and making personal protective equipment available.
- Offshore locations and third parties were found to not always have robust contingency plans in place and faced impediments such as deficiencies in telecommunications networks or a lack of Internet at home. Furthermore, some institutions spoke of the need to provide equipment such as laptops to third party staff as this was critical to operational continuity. Some had to develop local contingency arrangements for areas such as collections to ensure the ability to service customers on a timely basis.
- There was a need to rapidly improve analytics and build new digital platforms to gather client data as well as scripts to auto-process applications to the greatest extent possible. Supporting customers in distress and administering government programmes/ applying moratoria proved to be a significant operational challenge that required processes and systems to be reoriented or designed and implemented within a short space of time.
- In addition, many firms spent significant resources on building transaction-level analytics for their retail and SME customers as well as on detailed analysis and monitoring of larger corporate customers. This information was used to identify various issues such as deteriorating financial situations or vulnerabilities and to proactively reach out to customers rather than waiting for the collections or restructuring processes to kick in. Some banks recognised that the crisis highlighted their organisations' ability to drive large scale change within very tight time frames and in a dynamic environment.

The financial impact of the crisis was significantly muted by government interventions around the world with clear consequences for future expectations about interactions between governments, financial institutions and broader society

The extreme levels of volatility took risk and provisioning models into uncharted territory and there was a need for significant overlays. Most banks expected a significant shock to financial markets with the initial dislocation plunging markets downwards as Western economies began moving into lockdown. While this did not ultimately translate into losses, some of the early market dislocations will continue to have resonance in future stress scenarios.

Most banks saw government intervention as critical and necessary – a key lesson from the 2008 crisis. Such intervention was not only credited with the short-term stabilisation of the market, but also with preserving the fabric of society during times of turmoil and widespread disinformation. Governments and regulators showed that they had learnt from the experience a decade ago and were still acutely aware of the potentially disastrous economic and social consequences that a crisis of this magnitude could unleash. There is a consensus that the swift action taken in Q1 2020 helped to stabilize the markets by preventing sustained market ruptures like those experienced during the 2008 crisis.

Blueprint for change

1. **Review and – where required – refine risk framework and appetite to effectively monitor risks that arise due to large parts of the organisation continuing to work partially from home**
   After the first year of the pandemic, the "new normal" and what it means for ways of working is at the top of many institutions' minds. The success story of the initial transition to working remotely has caused many organisations to think about accelerating or increasing plans for reducing occupational density. Furthermore, some are still pursuing this goal as a strategic objective. Nevertheless, with the passing of time, firms have become increasingly aware of the negative impacts of remote working arrangements, as these have been taking their toll on staff and amplifying specific risks.

   There are institutions that are now seeking a large-scale return to the office as soon as is feasible but the consensus is that some level of remote working is likely to stay with us and will require the rethinking of leadership and collaboration models. This will mean revisiting risk appetite and control mechanisms, in particular those relating to how confidential information is managed in a potentially non-secure environment.

2. **Recast business continuity and other contingency plans based on what bolsters resilience against financial and operational points of failure**
   Most institutions had designed their business continuity planning around recovery centres that required physical proximity. This did not work in the pandemic and required institutions to think quickly on their feet. While there was therefore some questioning of the actual value of these plans, some institutions felt that their plans came in useful because, although they featured elements that had not been developed with a particular situation in mind, they nevertheless highlighted key elements that needed to function irrespective of the crisis situation. Governance mechanisms, the flow of information and communication strategy were highlighted as key elements that institutions had to get right. A lesson learned across the industry was the need to extend business continuity planning to the institutions' ecosystems because third-party suppliers (and their respective suppliers) exhibited vulnerabilities during the pandemic that had significant implications for the institutions themselves.

3. **Fundamentally restructure how scenarios are designed and used – future scenarios need to include agent-based approaches, drive broader participation and critical thinking across the organisation (and beyond it) and raise awareness of strengths and vulnerabilities**
   The human mind struggles with outlier events such as the pandemic and these are often dismissed as "so implausible that it just will not happen". Current tools are largely focused on analysing "severe, but plausible" events but with very limited time allocated to scenario design or the identification of key vulnerabilities. In most cases, the primary scenarios are largely financial/economic in terms of their origin and the analytical framework is geared towards dealing with historical correlations and the economic drivers of models. The crisis has highlighted the need for scenario design and analysis to play a much broader role in highlighting and promoting organisational scrutiny around a wider range of operational, business and balance sheet vulnerabilities.

4. **Build on lessons learned from the crisis when designing future risk reports and analytics**
   Managing the pandemic and fulfilling information requests from internal and external stakeholders required diverse sets of data to be produced at a much higher frequency. Looking forward, opportunities exist for better accessing, organising and using the data that institutions hold. Questions have also arisen about the standard reporting that was provided because parts of it were not viewed as useful during the crisis and lacked key points of information that were seen as equally valuable for normal times. In particular, many organisations spoke about making much better use of transaction-level data, for example for identifying at-risk customers and for formulating outreach strategies.

5. **Invest in faster and more dynamic enterprise-wide stress testing capabilities**
   The crisis showed limitations in the architecture of stress testing and in abilities to assess various different scenarios in crisis situations (when quick turnaround cycles are essential). The need to create a better link between capital and liquidity and to enhance abilities to ascertain the impact of a given scenario across multiple risk types were also recurring themes here.

5 Preparing for the decade of operational resilience

As growing numbers of risks prove too hard to anticipate, resilience is likely to become a core tool for senior management to deliver on their risk management obligations. Bank frameworks are still at an early stage of integrating resilience into scenario analysis as well as overall outcomes which Risk functions track. There is also a need to continue to build and embed risk insights in business decisions, including leveraging new data sources.

Industry observations

Operational resilience is emerging as the other key trend (next to sustainability) that will require continued focus over the next ten years	Banks see the need to build a deeper and forward looking understanding of operational vulnerabilities more or less at par with financial resilience	Similar to sustainability, operational resilience is not seen as primarily Risk-owned, although Risk will be playing a key role	There are material linkages with third party risk especially in the context of the impact of outsourced operations on resilience

Blueprint for change

1. Getting the basics right – establishing a common understanding and thinking materiality-based
2. Look beyond the boundaries of the institution when assessing resilience
3. Develop rigour around the calibration and use of appetite and tolerances
4. Review “move to cloud” initiatives through the lens of operational resilience

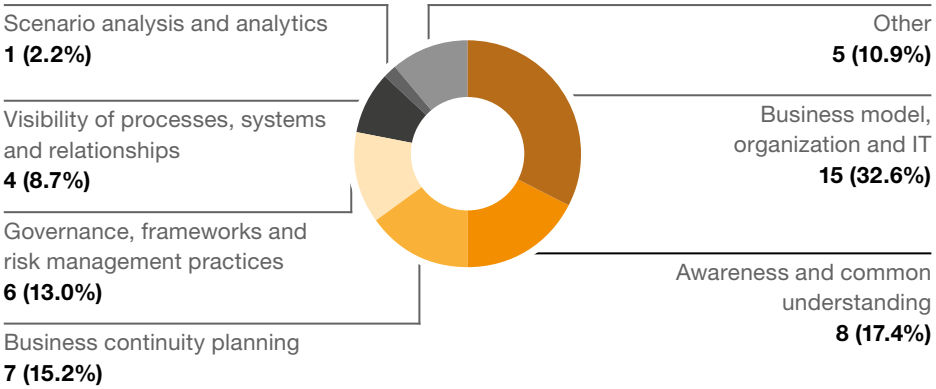
Industry observations

Operational resilience is emerging as the second key trend (next to sustainability) that will require continued focus over the next ten years

Similarly to sustainability, this topic was more marginal in 2018 and has now transitioned to the top of the agenda. UK regulators were frontrunners here in terms of setting expectations and communicating with institutions over the past 3–4 years. Other regulators are now increasingly following suit with key regulators focusing on where “concentrations” are broadly located in terms of points of failure. In Europe, related standards already existed regarding cyber and information security as well as outsourcing and the focus is now shifting toward operational resilience due to experiences from the pandemic in combination with the publication of standards by the BCBS.

Main challenges in building a resilient organisation

Number of mentions



While practices relating to this topic are more established than in the case of sustainability, weaving the different strands together nonetheless remains a work-in-progress. The key challenges described include:

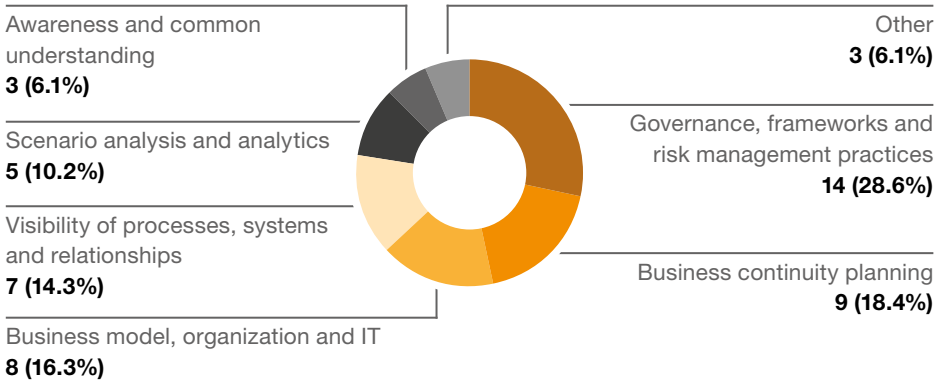
- Building awareness and a common understanding of the concept of operational resilience across institutions and how it relates to existing practices
- Thinking end-to-end along value streams/customer journeys and, where relevant, looking outside the organisation at third parties including service providers and industry utilities
- Developing sustainable capabilities for identifying and understanding where key vulnerabilities are located as well as what to measure and how to set tolerances around the key metrics identified
- Investing in the right expertise in both the first and the second line of defence so that the individuals entrusted with tasks and oversight have a deep understanding of what the real issues are, how to measure them and how to make the right cost/benefit choices in shaping the target state control environment

An interesting point of view expressed in numerous conversations around sustainability and operational resilience is the need for industry standards and potentially for industry-wide utilities. An example highlighted by several participants was joint audit/control models for cloud providers.

Banks view the need to build a deeper and forward-looking understanding of operational vulnerabilities as more or less equal to the need for financial resilience

Business continuity planning has been a requirement and good practice for a long time and expectations regarding cyber and information security as well as third party management have been increasing over the last five years. However, the concept of operational resilience is now taking these issues to the next level and weaving together various risk topics. Building a resilient organisation is seen as requiring a much better understanding of the points of failure that it is exposed to and these may be located both within and outside the organisation. Many institutions are at the beginning of their journey, investing in the creation of much greater transparency around processes, systems and third-party relationships and identifying which are the most critical among them.

Key current focus areas in building a resilient organisation



Similarly to sustainability, operational resilience is not seen as primarily owned by Risk functions, although Risk functions have a key role to play

For most respondents, the overall framework is owned and maintained by the Risk function. However, the first line is entrusted with coordinating and implementing the requirements. Second line teams are starting to emerge within Risk functions but these are still relatively small. Key focus areas here include education, process mapping and the use of scenarios to identify key vulnerabilities as well as investing in better and more resilient infrastructure. The Cloud has emerged as an area of focus across the industry due to the potential new points of failure as well as the need to develop effective control and assurance mechanisms.

There are links of material significance with third party risk, especially with regard to the impact of outsourced operations on resilience

The pandemic was seen as highlighting the importance of offshore operations and third parties for operational resilience due to instances of operational disruptions and material breaches of standards at some institutions. It is important not only to consider each third party in and of itself, but also each third party's ecosystem and exposure to disruptions that could compromise its ability to operate. This is seen as an area of increasing focus for regulators and concern has been raised by some banks that expectations may be raised to a standard where the economics of offshoring and outsourcing arrangements may no longer be viable.

Blueprint for change

1. **Getting the basics right – establishing a common understanding and thinking on the basis of materiality**
   A potential key challenge in this area is a lack of awareness about operational resilience and its connection to established practices relating to business continuity planning, cyber and information security and third-party management.

   Strong governance, clear accountability and consistent definitions are essential in order to push ahead with efficient programmes for building a resilient organisation. For example, a common understanding of what "critical" actually means for services, systems and data items is important for focusing on what really matters when identifying potential points of failure and developing response capabilities.

2. **Look beyond the boundaries of the institution when assessing resilience**
   Operational resilience requires institutions to think beyond their own boundaries. Institutions spoke of a need to operate outside of risk appetite in their dealings with third parties during the pandemic (e.g. departing from the status quo position of "no appetite for remote working") as well as incidents such as data breaches and a lack of access to adequate equipment that posed challenges to business continuity. In addition, there is a growing awareness of other points of failure that are beyond the control of the institution, such as a central counterparty (CCP) falling over or a prolonged Internet or power grid outage. A key area of focus here is mapping out value streams and identifying critical areas that could impact operational continuity, including those which may lie outside the institution itself. Doing so will require developing a toolkit that includes stress testing, structured scenarios and process simulations.

3. **Develop rigour around the calibration and use of appetite and tolerances**
   It is hard to define risk appetite in relation to operational resilience because this topic encompasses several risks that are thematic in and of themselves. The development of metrics is a work-in-progress. Points of interest here include the need to consider incidents such as systems outages on a dynamic basis due, for example, to the different impacts of a critical system outage during normal business hours compared to night-time.

4. **Review "Move to Cloud" initiatives through the lens of operational resilience**
   While looked at as a strategic priority in terms of building resilience, agility and reducing cost, the Cloud also poses new challenges. Given the asymmetry of negotiating power between the big Cloud providers and financial services institutions, industry standards will have to be defined and this may require regulatory or governmental action.

6 Seizing upon the advent of true automation

There has been considerable investment in building self-service analytics platforms and making these available to staff across the institution with an aim to provide more effective capabilities and potentially reduce cost at the same time. Compared to our survey in 2018, we also note significant progress in the advanced analytics space, with new tools and models having gone into production across the risk management lifecycle. However, realising the potential of emerging technologies at scale still faces a number of challenges, in particular legacy infrastructure and data quality as well as governance and demand management.

Industry observations

Many firms see big data and AI/ machine learning at a must-win battle to remain competitive. In particular, there is a limit on how far the cost of risk and compliance can be reduced without much more use of advanced analytics

Much adoption is being driven organically within institutions where large analytics and data science teams are beginning to emerge within Risk functions and are driving the data and tooling agenda

Banks are exploring at scale application of AI/ML in a wide range of risk topics going beyond the initial focus largely around Compliance and financial crime

Blueprint for change

1. Set up a technology vision and integrated roadmap aligned with other parts of the organisation and underpinned by strong governance and demand management
2. Augment staff by providing better toolkit and analytics capabilities
3. Articulate and follow through on data related foundational enhancements; set up a clear and actionable ethics policy

Industry observations

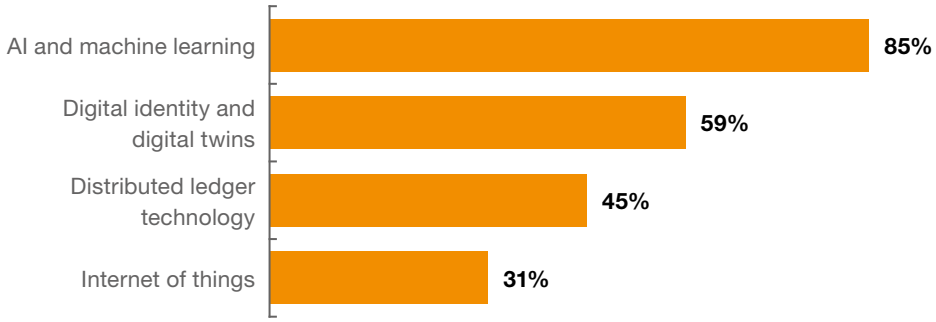
Many firms see big data and AI/ machine learning as a must-win struggle to remain competitive, especially in light of the limits on how much the cost of risk and compliance can be reduced without using advanced analytics

The adoption of advanced analytics had already started in 2018 with many institutions highlighting that computing power and data availability/accessibility had arrived at a stage where it was possible to enjoy real benefits from deploying these technologies. However, a feeling existed that Risk functions were lagging behind the other parts of the firm and had not been sufficiently integrated into the broader initiatives in this area.

Three years on, there are signs of an accelerating adoption in the Risk and Compliance space. While not every institution has made the same progress, everyone is at least thinking about and experimenting with applications. And some institutions have made remarkable progress, which was evident from the examples provided and the level of depth at which our interview partners spoke about their initiatives. While there were some contrarian views expressed on the transformational potential, and some institutions explained deliberately not aiming to be leaders in this space, the overall ambition is to deploy AI and ML at an increasing scale.

Risk function perspectives on the relative importance of emerging technologies

Weighted score based on ranking of technologies



Much adoption is being driven organically within institutions where large analytics and data science teams are beginning to emerge within Risk functions and are driving the data and tooling agenda

Some institutions have made significant progress in the area of data governance and are putting central data stores and automated data feeds in place. Many institutions spoke of using third-party solutions in this space and some have gone so far as to acquire equity stakes in promising start-ups. Others have further entered into partnerships with leading technology firms for uses relating to horizon scanning and developing early warning systems.

A number of obstacles still remain, including a need for improvements in the management of returns on investment, legacy systems and access to/availability of high-quality data. Clarifying accountabilities and aligning interests across different functions and areas of the institution remains a challenge. Participants highlighted several areas under consideration with a view to enhancing governance and demand management mechanisms:

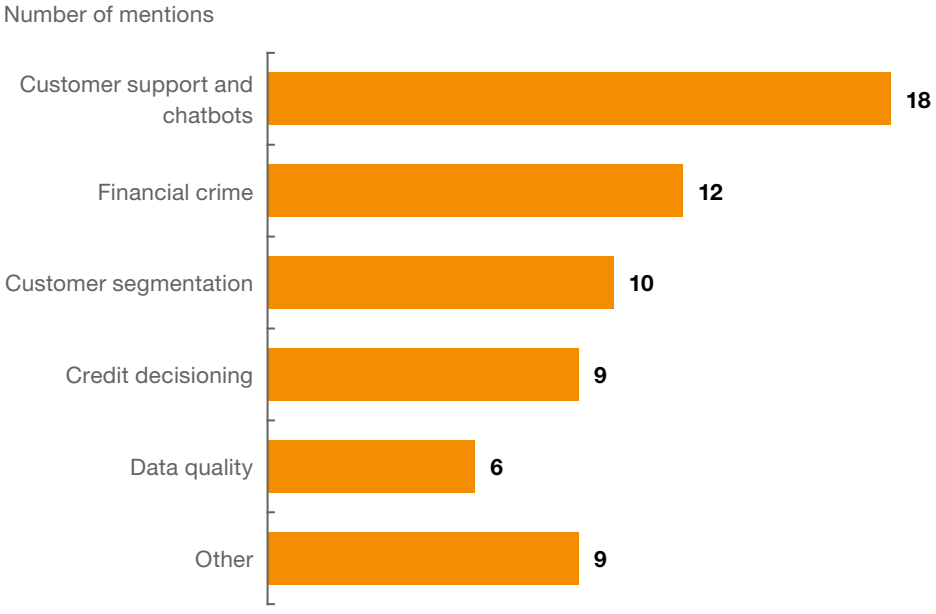
- Positioning the right individuals within executive management to give appropriate prominence to data and advanced analytics
- Revisiting how budgets are allocated and managed across different areas as well as increasing the rigour in relation to business cases and tracking the delivery of expected benefits

Banks are exploring at-scale applications of AI/ML for a wide range of risk topics and going beyond the initial focus area of Compliance and financial crime

Compliance and financial crime were the areas in which most institutions were using some form of AI/ML-based tools (including both in-house developments and third-party solutions). This is seen as transformational in this area as it enhances effectiveness and efficiency while simultaneously being well received by regulators. Most banks highlighted that their areas of focus were expanding throughout the institution and that priorities included credit risk, operational risks and regulatory/internal reporting.

The increasing availability of data as well as capabilities to segment individuals much more effectively and combine novel data sets that are used for targeting and understanding risk profiles are bringing the need to establish strong ethical foundations into the limelight. We note that this is at the top of institutions' minds, even among those operating across a number of jurisdictions with different standards around privacy/data protection. It is expected that this topic will gain further prominence as privacy and data ownership continue to be a growing concern in society.

Focus areas where AI and ML-based models have been successfully deployed into production



Blueprint for change

1. **Establish a technological vision and integrated roadmap that is aligned with other parts of the organisation and underpinned by strong governance and demand management**
   Data and analytics have been successfully deployed for many risk types and across many areas of activity. However, not everything can or should be done at once. There is a need to emphasise return on investment both in the selection of any solutions being developed and after they go live. In addition, governance and the way in which budgets are structured were seen as an area that requires additional attention.

2. **Augment staff by providing a better toolkit and analytics capabilities**
   Building “smart” tools such as "interactive FAQ-systems/ chatbots" and the prototyping of digital risk assistants (see section on non-financial risks) are priority areas of investment for larger firms and those with international operations seeking to develop effective, efficient and future-proof capabilities.

3. **Articulate and follow through on data-related foundational improvements and set up a clear and actionable ethics policy**
   Significant investment has gone into addressing the challenges of legacy architectures and data quality. There is an increasing awareness that these factors will be critical for remaining competitive. Because more data about individuals is being used, ethics and privacy are increasingly coming to the fore and some view strong privacy regulation as an advantage rather than a drawback.

7 Managing the generational workforce transition

As institutions become increasingly digital and automated, this changes the risk profile and the ways of working. While "traditional" financial risks will still remain relevant, the way in which they are managed will evolve with the expectation of increased use of technology and materially smaller teams. On the other hand, there is agreement that staff with a very different background will be required to deal with some of the emerging new risks, with particular focus on affinity for data and technology as well as diverse specialisms.

Industry observations

Institutions are reappraising the skill sets of risk management professionals as they reposition their Risk functions and explore new organisational structures and ways of working	The transition will not happen overnight and is expected to take place more gradually over time	The incoming generation has grown up with technology and is looked at as inherently tech-affine, bringing skills and attitude to tech enabled problem solving that institutions are looking to build

Blueprint for change

1. Setup plan and mechanisms to manage the generational transition
2. Build a balanced team with the right behavioural and specialist skills
3. Develop a data-driven strategic workforce management framework

Industry observations

Institutions are reappraising the skill sets of risk management professionals as they reposition their Risk functions and explore new organisational structures and ways of working

The participants highlighted the following core principles for the design of their target state:

- Risks should be managed where they are taken with operational activities being moved to the first line wherever possible
- Risk needs to focus on material vulnerabilities, especially where there is a conflict of interest between risk taking and risk oversight
- Risk functions should be involved in decision-making at an early stage rather than just overseeing them and challenging outcomes once incidents have already taken place
- Risk should be allowed sufficient time to consider what could happen and should apply a philosophy of hedging/preparation in order to prevent unwelcome surprises

While these principles may not necessarily sound new, conversations with a wide range of institutions across the industry have shown that it is still hard to apply them in practice and the thinking here is still evolving. There is a consensus that this will require the development of more holistic thinking, risk awareness and accountability across the organisation as well as support from the right incentives. Establishing a strong risk culture is seen as pivotal to delivering these goals and there is a general recognition of the challenge this poses in times when everyone is chasing returns, costs are being cut and extensive changes are taking place. Many participants linked this closely to their ideas regarding the Risk professional of the future, explaining that in the course of instilling more holistic and thematic thinking within institutions, they are consciously trying to promote this type of culture and skills mix within Risk functions. While the growing need for specialist skill sets was similarly highlighted as important, having Risk professionals who are able to work constructively with heads of business departments on initiatives, such as setting up a new legal entity in a particular jurisdiction or assisting with the launch of a new customer-facing app, was seen as a critical thing to get right.

The transition will not happen overnight and is expected to take place more gradually over time

Existing staff will need to be supported during upcoming times of significant change as ways of working evolve and become more technology enabled. This outlook applies not only to the second line but to the entire organisation because achieving the target state of a specialised, agile and more senior second line function will require the development of maturity and holistic thinking that extends into the first line as well. This has led many institutions to invest significantly in upskilling and the development of self-service platforms with risk and compliance modules available to their first lines of defence.

The incoming generation has grown up with technology and is looked at as inherently tech-affine, bringing skills and attitude to tech enabled problem solving that institutions are looking to build

It is also believed that leadership models and career pathways will have to evolve to cater to the differing expectations of millennials. While this view was more prominently expressed among European institutions, there was a general sense of the growing importance of work-life balance and a lower readiness to undergo geographical (including in-country) relocation in return for promising opportunities. Furthermore, career journeys may need to be structured such that they include positions in multiple parts of the firm in order to foster the holistic mentality that firms have singled out as a critical capability that they are seeking to develop.

Blueprint for change

1. **Set up a plan and arrangements to manage the generational transition**
   The digital transformation of institutions is seen as requiring tools and new arrangements to support existing staff. At the same time, institutions must remain attractive to future talent, which means rethinking career journeys and ways of working.

2. **Build a balanced team with the right behavioural and specialist skills**
   There is broad consensus on the need for balanced teams. While there were no uniform views regarding the skills of the envisaged risk professional of the future, there was a strong emphasis on individual skills such as holistic thinking, storytelling and digital affinity as well as on the importance of emphasising a balanced mix of personalities throughout the team.

3. **Develop a data-driven framework for strategic workforce management**
   We found that some institutions have developed workforce management frameworks that bring together planning, change initiatives and data relating to the Risk function headcount and skills. However, responses to the questionnaire indicate that data on skill sets is not tracked or immediately available in many institutions and that clear targets have not been set. We believe there is a need for improvement in this area and that this will be critical for facilitating the successful transformation of Risk functions over the next decade.

Study Development and Coordination

Johannes Göldner
Senior Manager, PwC Germany
johannes.goldner@pwc.com

Ajay Raina
Director, PwC UK
ajay.raina@pwc.com

About us
At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 155 countries with over 284,000 people whoare committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

Contacts

Europe

Dr. Sami Khiari
Germany
Tel: +49 30 26361453
sami.khiari@pwc.com

Dr. Michael Rönnberg
Germany
Tel: +49 69 95851524
michael.roennberg@pwc.com

Gregory Joos
Belgium
Tel: +32 2 7109605
gregory.joos@pwc.com

Rami Feghali
France
Tel: +33 1 56577127
rami.feghali@pwc.com

Anthony Kruizinga
Netherlands
Tel: +31 61 3087637
anthony.kruizinga@pwc.com

Casper Ruizendaal
Netherlands
Tel: +31 88 7927538
casper.ruizendaal@pwc.com

Symon Dawson
United Kingdom
Tel: +44 7483 422850
symon.k.dawson@pwc.com

Ajay Raina
United Kingdom
Tel: +44 7714 153427
ajay.raina@pwc.com

Jukka Paunonen
Finland
Tel: +358 20 7877715
jukka.paunonen@pwc.com

North America

Dietmar Serbee
United States
Tel: +1 917 902638
dietmar.d.serbee@pwc.com

Pranjal Shukla
United States
Tel: +1 203 8092522
pranjal.m.shukla@pwc.com

Jonathan Riva
Canada
Tel: +1 416 8155069
jonathan.riva@pwc.com

Michael Auret
Canada
Tel: +1 416 6878676
michael.auret@pwc.com

APAC

Edwina Star
Australia
Tel: +61 2 82664940 x64940
edwina.star@pwc.com

Justin Waller
Australia
Tel: +61 2 82660181 x6018
justin.waller@pwc.com

Sam Shuttleworth
New Zealand
Tel: +64 21 976949
sam.shuttleworth@pwc.com

Tamara McDonagh
New Zealand
Tel: +64 22 0199636
tamara.x.mcdonagh@pwc.com

Yoshiteru Ito
Japan
Tel: +81 80 13472227
yoshiteru.ito@pwc.com

Jun Muranaga
Japan
Tel: +81 80 13472227
jun.muranaga@pwc.com

Africa

Jacques Muller
Africa
Tel: +27 11 2870609
jacques.muller@pwc.com

Kumar Tulsi
Africa
Tel: +27 11 2870361
kumar.tulsi@pwc.com

© 2021 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity.

Please see www.pwc.com/structure for further details.This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisers.

www.pwc.de