

Ninth annual EY/IIF global bank risk
management survey

Accelerating digital transformation

Four imperatives for risk management



Contents

Executive summary

3

1. Adapting to a risk environment and risk profile that is changing faster and more intensively than ever

5

2. Leveraging risk management to enable business transformation and sustained growth

11

3. Delivering risk management effectively and efficiently

17

4. Managing through, and recovering from, disruptions

22

Conclusion: Transforming to a digital future to address risk imperatives

25

Research methodology and demographics

26



Executive summary



Last year's eighth annual EY/Institute of International Finance (IIF) global bank risk management survey, Restore, rationalize and reinvent: a fundamental shift in the way banks manage risk,¹ highlighted risk management's significant transformation journey. The initial post-crisis years focused on restoring the industry: rebuilding capital and liquidity buffers, reconstituting the three-lines-of-defense model and restoring trust in financial institutions. The current middle stage, rationalize, focuses on simplifying legal entities and processes, and preparing for the transformation ahead. The third phase, reinvent, underscores the reinvention, disruption and technology that will drive substantive change in business processes, operating models and controls.

The core message last year was that the reinvention phase was likely a few years out. While some banks had accelerated their transformation and were leading the way, the majority were still working to complete their rationalization and to build the necessary foundations for transformation.

However, a year later, the industry's digital transformation and ongoing competitive disruption, coupled with major shifts in geopolitics, macroeconomics and social issues, seem to be accelerating more than many expected. Client-facing transformation is speeding forward. But more substantive, firmwide transformation – from the front to back office – is accelerating as well.

The ninth annual global bank risk management survey, Accelerating digital transformation: four imperatives for risk management, is another collaborative effort by EY and the IIF. Participants included 74 firms from 29 countries. This year's survey highlights that while banks across the industry are still at various places in their restore, rationalize and reinvent journey, fairly soon every bank will have to successfully reinvent itself. Risk management has a critical role to play in the transformation.

¹ *Five challenges for banks as they evolve risk management*, https://www.ey.com/en_gl/banking-capital-markets/five-challenges-for-banks-as-they-evolve-risk-management, 2017.

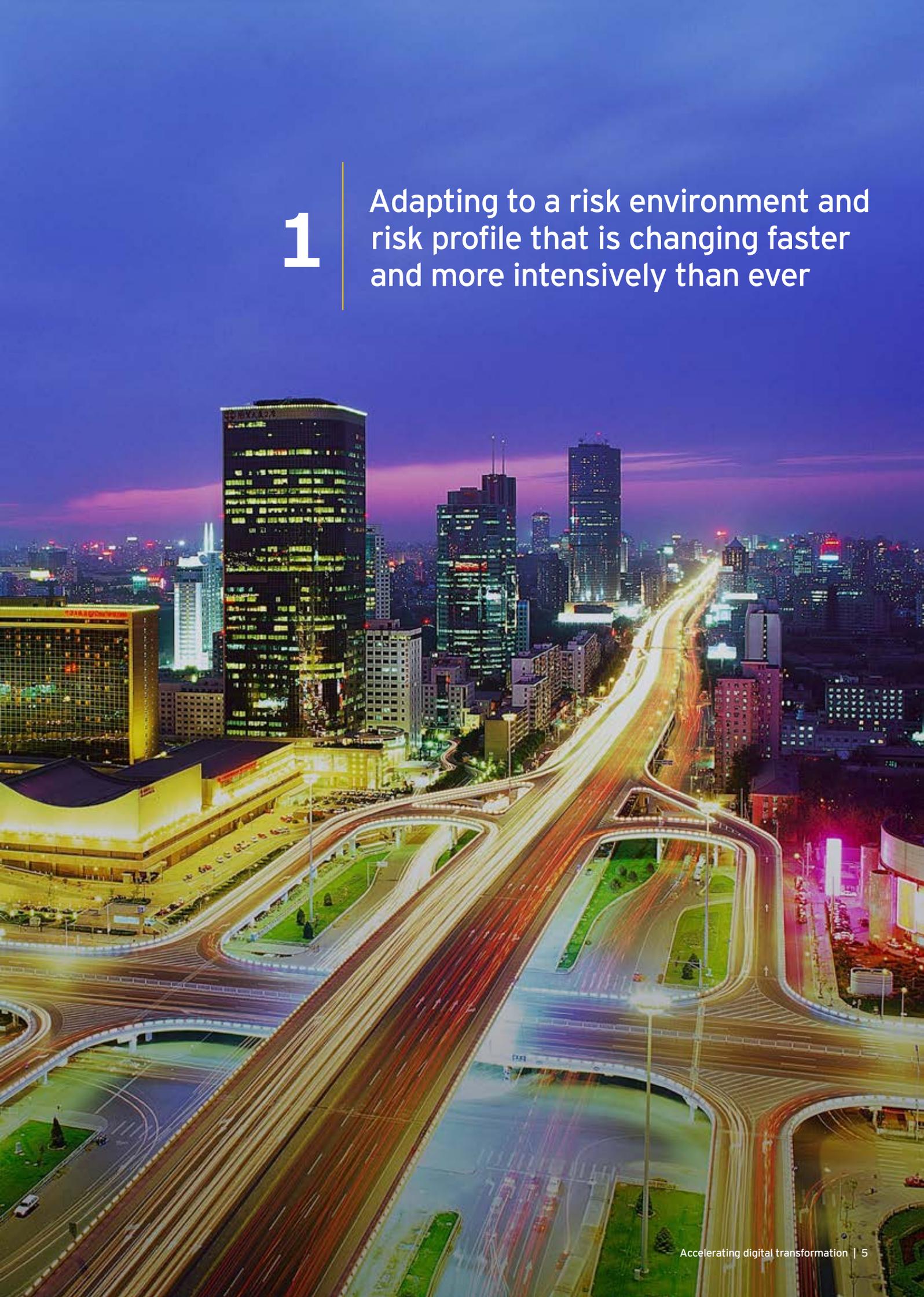
² See *EY Moving from analog to digital: a new paradigm for risk management*

The survey sets out four imperatives that boards, senior management, chief risk officers (CROs) and other key executives will have to address to successfully achieve their digital transformation ambitions:²

1. **Adapting to a risk environment and risk profile that is changing faster and more intensively than ever:** Risk management has to support banks' abilities to react speedily to near-term risks, better navigate emerging three-to-five-year risks, and periodically consider the impact of changes that may occur over the next 10 to 20 years.
2. **Leveraging risk management to enable business transformation and sustained growth:** Risk management professionals need to better balance their roles, both in helping the firm make more risk-informed decisions (i.e., managing downside risk) and supporting profitable, sustainable growth (i.e., capturing upside risk).
3. **Delivering risk management effectively and efficiently:** Risk management, like other parts of the firm, needs to be efficient. It has to devise new operating and talent models, and more fundamentally leverage new technologies in conducting its work. As efficiency becomes paramount, however, effectiveness has to be maintained or enhanced. It's a balancing act.
4. **Managing through, and recovering from, disruptions:** There is a growing sense that disruptions are becoming more frequent and impactful (i.e., cyberattacks, vendor or technology outages, or more extreme weather-related events). Risk management has a key role to play in developing a more integrated, firmwide strategy and approach to operational and financial resilience.

1

Adapting to a risk environment and risk profile that is changing faster and more intensively than ever



Risk management has to stay in the moment, keeping a keen eye for immediate changes in market or firm conditions, and a focus on the future to spot risks and opportunities that are emerging (over the next three to five years) and long-term (10 to 20 or more years out). It has to stay sensitive to financial and non-financial risks that are here today and that might emerge tomorrow.

Risk management is perhaps the only part of the firm that has the remit and capabilities to properly consider these broader changes and their impacts on economies, clients, customers, sectors and, most importantly, their firms.

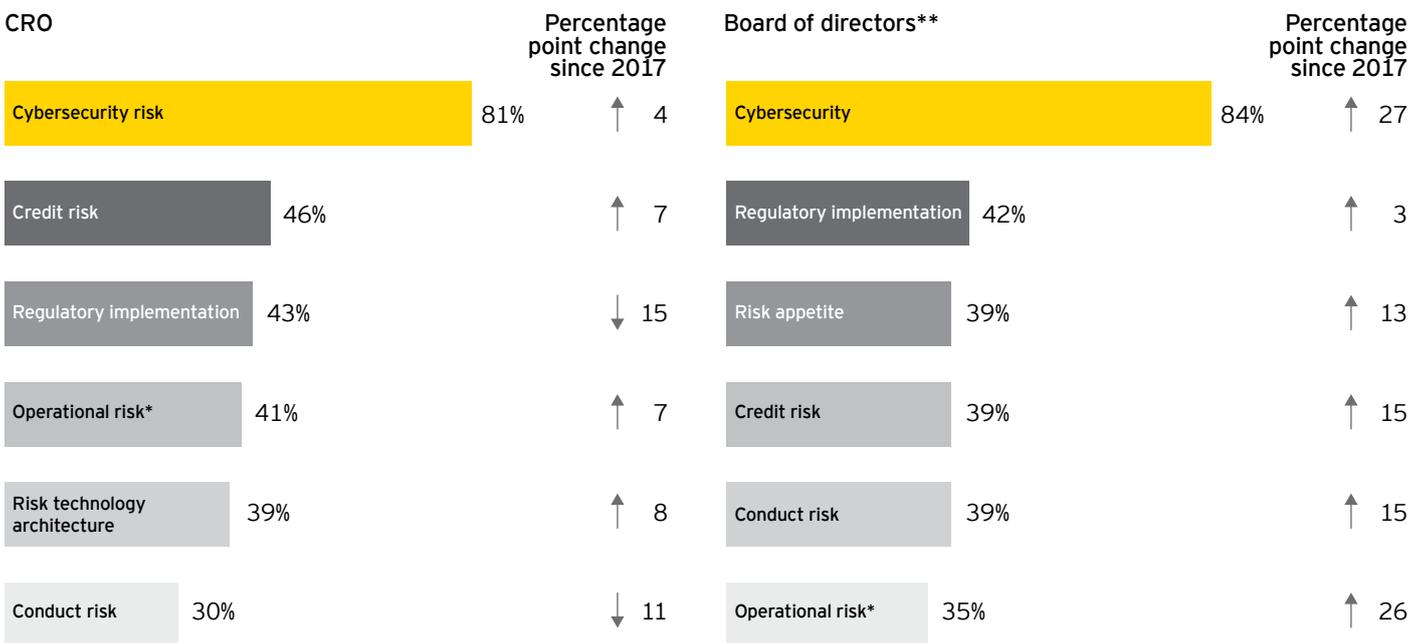
Near-term risks change year to year, as has been apparent over the nine years of the global bank risk management survey. 2018 is no different. However, two key trends have endured in recent years:

- ▶ Cybersecurity continues to accelerate to the top of board and CRO agendas. The second most important risk is materially below cybersecurity.
- ▶ Implementation of new regulations or supervisory expectations remains important but continues to move down the agenda (see Regulation remains important, on page 7).

The focus of boards differs somewhat from that of CROs, reflecting their strategic vs. management mandate (see Figure 1). Conduct, culture and reputation are all more important to boards.

Regional differences exist. European banks are significantly more focused on business model risk and model risk than their peers in other regions, which reflects the importance of these issues on the EU single supervisor’s agenda. North American banks are more focused on non-financial risks, such as operational risks, IT risk architecture and conduct. Beyond cybersecurity, each region has different CRO top priorities, reflecting the maturity of the banks and regional capital markets, as well as regional and local market conditions: credit and liquidity risks in Asia-Pacific (both 58%); risk appetite in Latin America (62%); implementation of new regulations and supervisory expectations in Africa and the Middle East (86%); business-model risk and implementation of new regulations and supervisory expectations in Europe (both 56%); and operational risk (excluding cybersecurity) and risk technology architecture in North America (both 65%).

Figure 1: Risk priorities over next 12 months



* Excluding cybersecurity

** Represents risks' view on the board's priorities; board members were not surveyed.

Regulation remains important

The regulatory and surrounding political environment has changed materially during the past few years. While the implementation of new regulatory requirements and supervisory expectations remain a top risk for boards and CROs, the pace of new requirements has slowed, leading one risk executive to say, "There are no 'new things' on the regulatory agenda." Global systemically important banks (G-SIBs) remain concerned about global fragmentation and their ability to operate efficiently in such an environment, especially given emerging differences in how rules are being implemented and interpreted locally and regionally.

Basel III finalization

The remaining Basel Committee on Banking Supervision agenda related to Basel III is still being finalized, especially with regard to the Fundamental Review of the Trading Book (FRTB), and the agreed-upon aspects still need to be implemented. Progress in conducting impact assessments of final Basel III requirements has not been uniform, although, as expected, G-SIBs have made the most headway. Those banks that have done assessments cite several key areas where they expect significant impact:

- ▶ Revisions to the approach for operational risk – 53%
- ▶ Revisions to standardized risk weights – 50%
- ▶ Output floor for internal ratings-based approach – 40%
- ▶ IRB parameter floors (probability of default (PD), loss-given default (LGD)) – 34%
- ▶ Revisions to the standardized approach for measuring counterparty credit risk (SA-CCR) – 29%

Given the potential impact, banks continue to push for change in the final regulations – more than two in five (43%) banks cite lobbying lawmakers and regulators for relief as their top course of action. If they are unsuccessful, likely planned actions include:

- ▶ Change business or product portfolio – 36%
- ▶ Make operational changes – 36%
- ▶ Alter capital approaches beyond those enforced by the changes (e.g., move some standardized portfolios to IRB) – 13%
- ▶ Change legal entity risk profile – 7%

Interbank Offered Rate (IBOR) transition

After more than 40 years of the financial services industry relying on IBORs as a reference rate for variable-rate financial instruments, the London Interbank Offered Rate (LIBOR) and other IBORs are being replaced by Alternative Reference Rates (ARRs). LIBOR today underpins more than \$300t of financial contracts. The transition is expected to be a significant transformation effort for financial services firms and market participants that have extensive exposure to LIBOR-linked products and contracts.

The stakes could not be higher for the industry, which was damaged significantly by the LIBOR scandal. Getting the transition right will play a role in showing that the industry can manage itself appropriately. Not surprisingly, regulators and industry groups stepped up their activity in the summer of 2018. The message was crystal clear: change is coming, it's coming sooner than you think, and the industry needs to manage it or regulators will step in.

Banks point to several key potential risks associated with the transition away from IBORs that they are most focused on:³

- ▶ Client outreach, including repapering and negotiating contracts – 64%
- ▶ Market adoption and liquidity in ARR derivatives – 58%
- ▶ Operations, data and technology changes – 54%
- ▶ Potential uncertainty about the future of LIBOR – 51%
- ▶ Valuation, model and risk management – 46%

Aligning regulation and innovation

While the technological changes sweeping the financial markets have brought clear benefits to both industry players and consumers, they also have raised fundamental questions around how regulation should adapt. For an industry still finalizing reforms introduced after the global financial crisis, the rise of FinTechs presents another new round of challenges. It's time for financial institutions and regulators alike to ask: How can we build a regulatory environment fit for a digital future?⁴

Banks want certainty as they consider how to transform digitally, and they identify numerous ways that regulators and supervisors can enable the use of new technologies:

- ▶ Create regulatory and supervisory certainty around the deployment of new technologies – 66%
- ▶ Ensure the safety and soundness of the financial system – 56%
- ▶ Clarify risk management expectations around new technologies – 54%
- ▶ Clarify privacy/information security expectations around new technologies – 51%
- ▶ Create a level playing field between existing and new firms and competitors – 50%
- ▶ Clarify third-party risk management expectations around new technologies – 44%
- ▶ Ensure compliance with laws, rules and regulations – 41%
- ▶ Clarify cyber-risk expectations around new technologies – 40%

³ *IBOR transition: a certainty not a choice*, [https://www.ey.com/Publication/vwLUAssets/ey-ibor-transition-a-certainty-not-a-choice/\\$File/ey-ibor-transition-a-certainty-not-a-choice.pdf](https://www.ey.com/Publication/vwLUAssets/ey-ibor-transition-a-certainty-not-a-choice/$File/ey-ibor-transition-a-certainty-not-a-choice.pdf), 2018.

⁴ *How can regulation keep up as technological innovation races ahead?*, https://www.ey.com/en_gl/banking-capital-markets/how-can-regulation-keep-up-as-technological-innovation-races-ahead, August 1, 2018.

Emerging risks: data and disruption

While managing short-term risks and priorities, risk management has to focus on emerging risks. These risks may be new, previously immaterial or known but increasing, and may require more analysis and consideration.

This year, given the fast-changing threat landscape, banks are focused especially on attacks that manipulate or destroy data (79%), as well as data availability (56%). An issue that will likely rise on the agenda in coming years, given banks’ many legacy systems, is IT obsolescence (see Enabling secure and safe use of the cloud, on page 19). Two out of five banks cite this as a top emerging risk. Regulators globally are certainly paying more attention to these issues as part of a broader, more intensive focus on operational resilience (see Managing through, and recovering from, disruptions, on page 22).

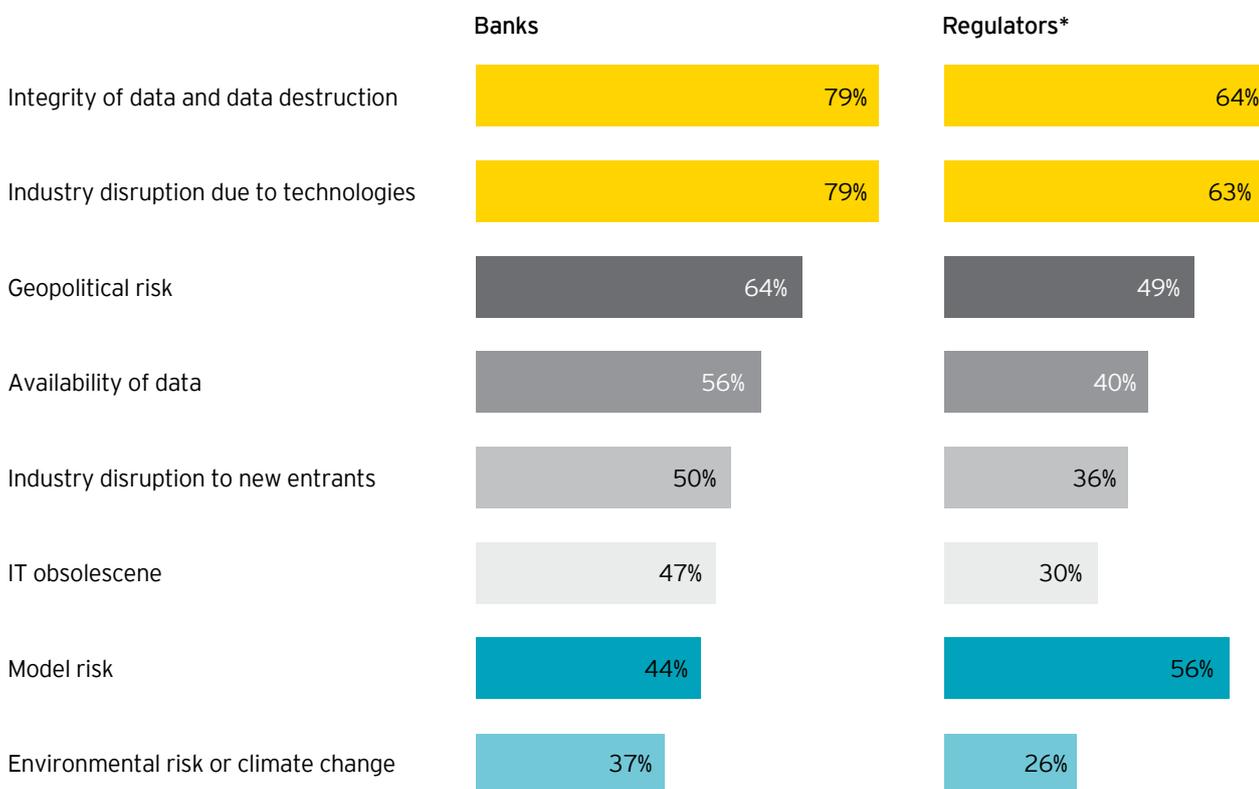
Industry disruption, driven by new technologies or entrants, continues to be a concern for banks and regulators. Banks believe regulators are more focused on electronic trading risks than last year, reflecting broader concerns about market integrity and stability.

Risk executives highlighted that the “macroeconomic environment and political uncertainty are major concerns.” More specifically, “an emerging risk that is of concern to the bank is the trade wars happening globally because banks function in emerging

markets, and will likely be affected the most,” says one executive. The impact of these sociopolitical factors on bank economics could potentially be significant, necessitating an active role by risk management. Another executive adds, “The macroeconomic conditions are influenced by the political and external environment, which feeds into the credit landscape of the bank. Risk management procedures and practices need to protect the viability of the bank” (see Brexit: an emerged risk with differentiated impact, on page 9).

Beyond the next three to five years, it is important to consider how risks will evolve over longer time horizons. After all, many financial services firms are investing in assets or providing insurance over 20-to-30-year time frames. Changes that risk may consider include the potential long-term effect on customer demand for financial services products and services from the impact of: climate change; sensor technology and the Internet of Things; urbanization, population growth and mass migration; broad-scale use of artificial intelligence (AI) and virtual reality; and workforce patterns. The long-term impacts could be profound, and short-term solutions that ignore these megatrends will likely create significant problems for those not taking the long view. As one risk executive puts it, “That is the reason why reputational risk and sustainability are so important, and why risk management needs to be a business partner in decisions for longer-term investments.”

Figure 2: Emerging risks over the next five years



Brexit: an emerged risk with differentiated impact⁵

The UK's formal exit from the European Union (EU), scheduled for March 2019, has garnered significant attention in Europe and globally, given the preeminent role of London within the global capital markets. The nature of the final deal – or the fears of a no-deal Brexit – is the subject of daily discussion and debate. Brexit has become the ultimate emerging risk.

Over half of the banks that participated in this year's survey (56%) are directly affected by Brexit. Among those, the specific impacts vary significantly. Almost half (47%) of those that will be affected expect risk management challenges to become more complex, while slightly more than two in five expect headcount to increase. Those predicting the addition of new talent point most to: compliance (73%), regulatory risk management and liaison (67%), and credit risk management (60%).⁶ A quarter (24%) expect Brexit will make it harder to retain top talent with certain skill sets, and almost one in three (29%) expect to have to increase the amount of capital required to support UK and the so-called EU27 countries.

However, some firms are not expecting much impact at all. Almost a third anticipate no direct impact, and only 3% expect to have to exit certain products or business lines. None expect

Brexit will encourage them to exit certain countries. In the end, the UK and mainland Europe are key markets for global banks, Brexit notwithstanding.

The impact on firms' booking models is also mixed. Half of the participants who said they will be impacted by Brexit believe it will not affect their booking model approach, whereas 34% think they will need to significantly redesign global booking models, mainly because of Brexit. North American banks are the least concerned about the impact on their booking model.

Financial resources of some firms will be affected materially, with almost a sixth of survey participants impacted by Brexit (16%) expecting a material increase in capital due to increased counterparty risk and about a tenth (11%) expecting a material reduction in liquidity in global business lines due to additional regulatory requirements between the UK and EU. About a quarter (26%) expect a material increase in legal risk (e.g., due to a lack of clear agreement on the treatment of long-dated derivatives).

⁵ *Brexit and financial services: navigating the negotiations*, <https://www.ey.com/gl/en/industries/financial-services/tso-insights-brexit-and-financial-services-navigating-the-negotiations>, 2017.

⁶ Some banks expect headcount increase in liquidity risk management (27%), market risk management (20%), operational risk management (20%) and third-party risk management (13%).

Determining actionable metrics to better manage non-financial risks

In recent years, there has been a significant focus on the management of non-financial risks – and understandably so. One executive explains: "Financial risks are our primary task, but we are increasingly under pressure, from the board and regulators, to focus on a wide range of non-financial risks. Cyber is the most important, but we also pay attention to reputational risk and model risk, among others." Other stakeholders, such as institutional investors and nongovernmental organizations, are also focused on these underlying risks. Yet, each risk – vendor, IT, cyber, conduct, compliance, etc. – poses unique challenges in how to identify, measure, monitor and mitigate it.

Boards of directors and senior management have been pushing for greater insight into firms' non-financial risk profiles, and their firms' success in managing those risks. Yet banks' board reporting on non-financial risks may still be relatively immature. To quote one executive, "A risk profile goes to the board each month – it is a red, amber and green report. The row for financial risks is mostly green, but the one for non-financial risks is mostly amber and red." Boards need a much more sophisticated approach to truly understand the firm's risk exposure to operational risk.

Innovation in this area will continue, especially as it relates to better risk measurement so that more-informed decisions can be made within the risk appetite context. This will enable boards and management teams to know what level of risk they are willing and able to accept, and shape the extent and success of mitigation efforts. However, measurement and reporting of non-financial risks remains challenging. Says one risk executive, "We are hoping to develop better metrics and the right metrics to manage non-financial risks like cybersecurity, data, privacy, money laundering, etc. As it is difficult to measure the risk and the impact, the metrics become a critical management tool."

Difficult-to-measure risks include reputational (66%), cybersecurity (54%), strategic (39%), technology (26%), conduct (26%) and information security (23%). Risk professionals use existing findings across the organization to determine the magnitude of such risks, and rely on regulatory findings (86%), repeat issues (76%), compliance findings (76%), quality assurance or control issues (67%) and the time that identified control issues take to remediate (66%).⁷

⁷ Percentages relate to summation of the top two of five levels of importance.

Challenges in quantifying non-financial risks vary by region. Asia-Pacific's results for cybersecurity are slightly lower than those for North America, and European banks find it harder to quantify cybersecurity, resilience and compliance than their North American peers. Asia-Pacific banks struggle more than others with money laundering and sanctions risk. European banks struggle more with strategic and conduct risk, vs. Latin American banks that find cybersecurity and reputational risks hard to quantify. Banks in Africa and the Middle East find quantifying reputational, cybersecurity and strategic risks most challenging. G-SIBs struggle more than others with conduct, compliance, money laundering and sanctions risks, while non-

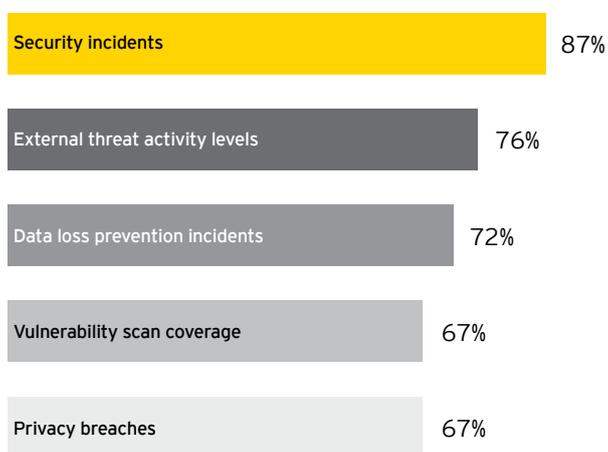
G-SIBs struggle more with cybersecurity, information security and third-party risks.

Firms are seeking out novel and insightful metrics to support board- and senior-level reporting (see Figure 3: Non-financial risk metrics).

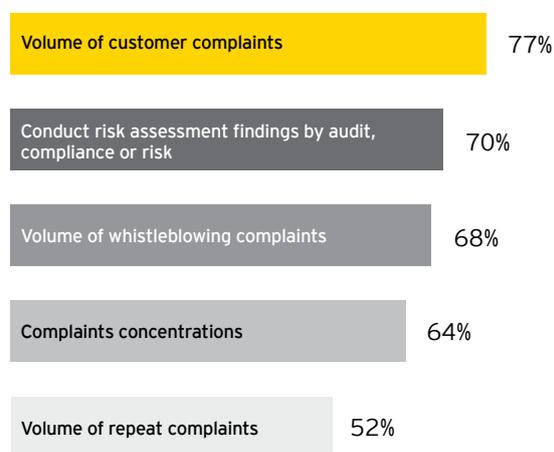
Beyond metrics, banks are building out their risk management capabilities, but this will require significant investment. "Capabilities to sustain growth mean making bigger investments in cyber, data and privacy to manage the non-financial risks, which are expanding," notes one executive.

Figure 3: Non-financial risk metrics

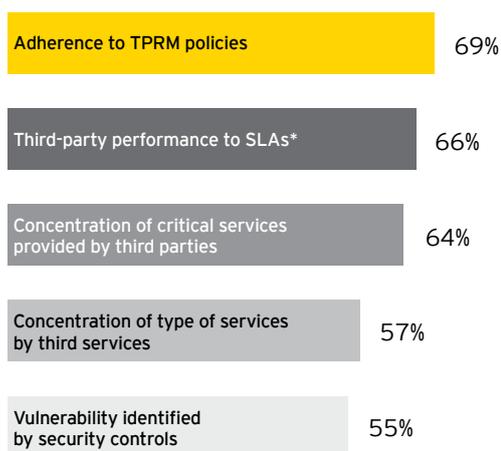
Cybersecurity



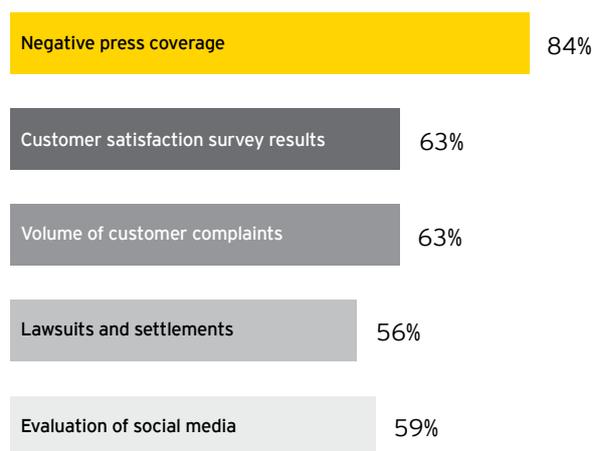
Conduct risk



Third-party risk management (TPRM)



Reputational risk



* Service-level agreements

2

Leveraging risk management to enable business transformation and sustained growth



Risk management is not simply about risk avoidance. It is about enabling the firm to strategically make risk-informed decisions to grow and prosper. According to one CRO, “The business is now saying don’t tell us why we can’t; tell us how to do it.” Risk management professionals have to work with the business in managing through a digital transformation to properly address new risks and identify and grasp growth opportunities presented by industry change.

The trick is to balance the need to remain independent from the first line, challenge their decision, and validate that they are operating within board-approved risk appetite and risk policy constraints, with the need to contribute to sustained firm growth, profitability, and safety and soundness. One risk executive describes the balance well: “We need to help steer businesses to take the right form of risk – some risks we want to take, others we definitely want to avoid.” Some banks are making progress and engendering the necessary discipline. As another executive says, “The message to people in my organization is to decline transactions that are below our return metrics.”

Banks identified a number of critical ways in which risk management can support the firm’s performance (see Figure 4). Put simply, “Risk management assists in sustaining growth by monitoring the bank’s return on equity and how it is maintained” (see Drivers to achieving target ROEs, on page 13).

Risk management has to inform the firm’s approach to enabling growth (see Figure 5). Products and services – and the manner in which customers are engaged and served – are changing materially. Without risk management’s deep involvement in such change, firms run the risk of mispricing or understating risk, or inadvertently creating future misconduct-risk challenges. Very soon that risk could be dwarfed by the potential failure of risk management to inform and guide material changes to business and operating models.

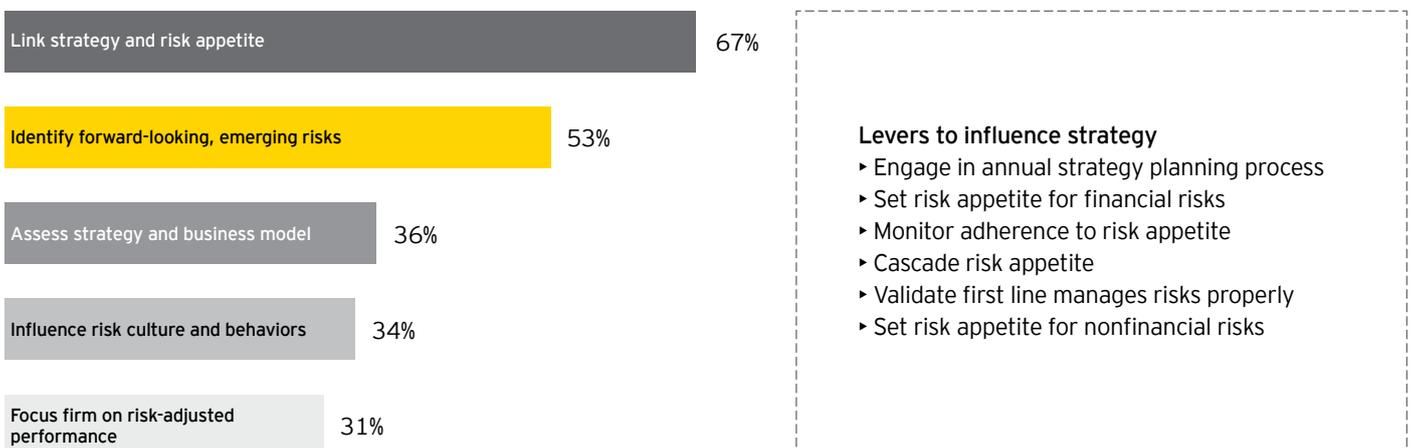
There are regional differences in how banks view the role of risk management in growth. For example, Asia-Pacific banks put more emphasis on validating the first-line risk activities and

supporting the business in setting quantitative metrics, whereas they place less focus on participating in strategy discussions or validating that emerging risks have been properly incorporated in business plans. North American banks place more importance on protecting the firm’s reputation than banks from other regions. Variations exist between G-SIBs and non-G-SIBs. G-SIBs are more likely to view risk management’s role in validating the first-line risk approach as important, reflecting their long-standing efforts to instill first-line accountability.

Banks point to the central importance of the risk appetite framework and board-approved risk tolerances in helping drive performance, as well as manage risk. For example, two-thirds of banks say risk management can influence capital allocation to optimize returns within the context of risk appetite, and risk appetite is a key tool for risk to influence firm strategy. According to one CRO, “We have a risk appetite statement and should operate within it, but we also should not routinely come up too short because that’s when we leave value on the table or forego revenue.” To use it in this way, changes would be required. One executive says, “We are planning to transform the risk appetite in a more dynamic environment. Typically, it’s a static chart, but it could be conditional, where triggers could evolve if the realized scenario differs from the one that has been approved in the risk appetite.”

Risk management has to consider broad internal and external changes to determine whether new risks are being created as business models adapt and whether the firm is managing the quantum of risk associated with major change brought about by digital transformation (see Figure 6). “It is important to carefully assess what is and isn’t changing. Technology is increasing the speed with which new risks emerge, as well as their depth and the interplay between risks,” comments one risk executive. Keeping pace with the speed of change is challenging, notes another executive: “Just keeping track of those innovations is very difficult, so we will be spending a lot of attention and energy in the future on staying connected.”

Figure 4: Risk management’s role in influencing long-term, sustainable performance



Drivers to achieving target ROEs

In recent years, the industry has trended toward three-year target ROEs of 11% to 15% and, at the same time, bank economics have generally been improving. Those patterns continue in 2018, with somewhat more banks targeting those levels or above than in prior years. Non-G-SIB banks continue to target higher ROEs than their G-SIB competitors.

Achieving those targets remains challenging. Important factors in doing so will be banks' ability to grow revenue (68%) and reduce operational costs (62%) – even more so for G-SIBs. Beyond that, their ability to implement new technologies effectively will be important (51%). Of course, macroeconomic conditions will play a role (46%).

Perhaps surprisingly, most other potential factors play much less of a role, in the view of banks:

- ▶ Ability to manage risks – 25%
- ▶ Impact of competition – 16%
- ▶ Ability to price risks – 12%
- ▶ Ability to attract and retain talent – 9%
- ▶ Ability to reduce compliance cost – 6%
- ▶ Impact of regulatory fragmentation – 3%

To some extent, this may simply highlight that these other issues will have a more material impact on banks' profitability over a longer timeframe than three years. In that shorter period, revenue and costs remain critical.

Figure 5: Risk management's role in enabling growth



Figure 6: Risk management's role in assessing business model risks



* In the context of business-model viability



North American banks, and to a lesser extent European banks, emphasize risk management's role in challenging corporate and business line strategies more than other regions. Perhaps this reflects the fact that those firms have more systematically linked strategy and risk. G-SIBs are much more likely than non-G-SIBs to have risk management validate that changes to business models are captured in the risk appetite framework, and to monitor business model viability and sustainability.

Risk management's role in informing technological transformation

The financial services industry is undergoing a massive transformation, and risk management runs the risk of falling behind and focusing only on downside risk. Risk management has to have a seat at the table and, to be credible, it needs to be very much a part of the overall digital transformation discussion, from strategy to implementation. Being an interested spectator is not an option.

The scale of change is significant. One risk executive notes, "We are thinking about how to become fit for the future – how to digitize our processes and products, removing retail branches, etc. The change has significant implications in terms of culture

and ways of working, and we need to rethink how banking works." In taking this broader perspective, says another executive, "We need to look at it from the point of view of the whole journey of digitalization."

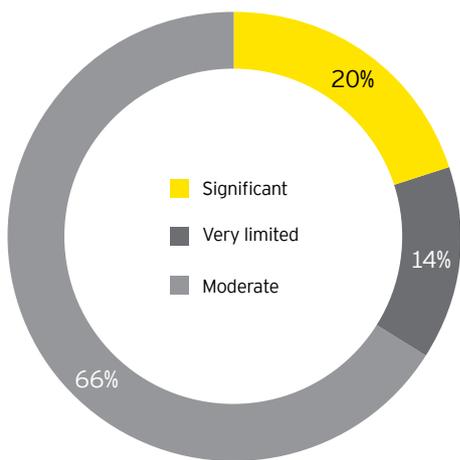
To date, banks' risk management groups often have taken a somewhat passive role in technology transformation. Generally speaking, there is only moderate input from risk into the firm's IT and digital strategy, and moderate alignment of that strategy with risk management's operating plan (see Figure 7).

Leading banks have instilled greater engagement; their risk management groups provide significant input to the IT and digital strategy (20% of banks), and have aligned their plans with the risks associated with the IT and digital strategy (17%). According to one executive whose bank has taken the more embedded approach, "Risk is deeply involved with our risk engine in the digital transformation processes. Many processes are multi-channel with more automated decisions. We are at the heart of this because the decision engine is now incorporated in risk management." Such engagement requires a cultural change, notes another executive, "The front office thinks they can do whatever they want, or use whatever platform they want. If it fails, it will be the risk guys and finance guys who sort it out."

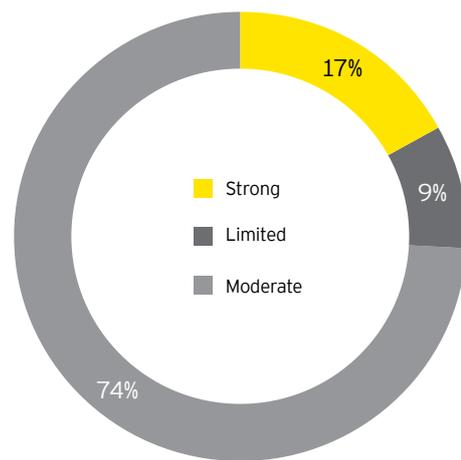


Figure 7: Alignment with IT and digital strategy

Risk management's input to prioritization of firm's IT and digital strategy



Alignment of risk management plan with risks in IT and digital strategy



Risk can help put digital transformation in context; after all, regulation and other matters have not gone away. One CRO summarizes it this way: “The interconnection with digitalization and the regulatory landscape is important. The role of risk management must evolve to be proactive and work closely with finance in steering the businesses and making them aware of those connections.”

Managing agile development and product development

To quicken the pace at which firms can meet changing customer needs and enable faster deployment of technology, banks are moving toward agile development.⁸ Such approaches will test how risk management and compliance embed themselves and their tools to ensure that new products, services and functionality are deployed in a safe and secure manner. After all, while agile development brings real benefits, “agile methodology is identified as a risk, industry-wide,” concludes one risk executive.

The industry is in a state of transition to agile development. Almost a third (31%) of banks surveyed have only limited use of these techniques, while a handful (6%) have not even started. Those banks using agile development are at various levels of maturity:

- ▶ A small minority (13%) have redesigned their first-line agile development process to be fully integrated into the firmwide process risk and controls framework.
- ▶ Some banks have formalized the way in which they monitor the level of risk associated with products or features designed in the agile development process (27%) or introduced a formal role in the first-line agile development team (25%).
- ▶ Just more than one in 10 (12%) of the banks have had their third line – internal audit – audit the agile development process.

However, more than two in five (42%) acknowledge that risk management’s involvement is inconsistent.

The extent to which agile development approaches are used, and the degree to which risk management is involved, varies across banks. The role of risk management is more inconsistent in European and North American banks than in other regions, while Latin American banks signal they have tried various ways to embed risk management in the agile process. To date, banks in Asia-Pacific, the Middle East and Africa – and G-SIBs as a group globally – are less likely to be using agile development.

The discussion on agile development highlights a broader point about the evolving role of risk management in product development. Often, risk management does not get involved early enough, and when it does – typically through committee review and oversight – it is viewed as slow and bureaucratic.

However, risk management’s role could be energizing if structured well, explains one executive: “Risk performs stress tests on the potential returns of new products. They aim to understand how the new products will affect existing ones, their impact on the fair treatment of customers, and what risks these new products bring environmentally and socially.”

To be effective, risk management has to be “more involved in the front end of product design and roll-out, as systems will require the necessary risk management capabilities inherent in the digital products when they launch,” notes a risk executive. Risk management also has to focus more on the customer. One risk executive says, “The evolution of the product-approval process is important because we no longer analyze only the purely technical aspects, but also the strategic ones: planning, budget, customer needs. The most important question is whether it is a good product for the customer. Inside the risk management function, the approval process starts with the customer perspective. The best way to destroy a reputation is to sell a bad product.” However, as one executive emphasizes, “What makes the process harder is not so much new products themselves, but rather adjusting to variations in those new products.”

⁸ “Agile development” is a set of principles on which to base software development, which depends on a highly disciplined, collaborative, cross-functional approach. Thus far, the main focus of financial institutions has been using this approach well beyond the domain of software development to better meet consumer demands, but increasingly it is being seen as a means to reduce risk and respond to rapidly changing external forces.

A nighttime photograph of the Sydney Opera House, illuminated with warm lights. The building's iconic white, shell-like roof is the central focus. In the foreground, there are horizontal light trails in green and yellow, suggesting a long-exposure shot of traffic or lights. The background shows other city buildings with lights.

3

Delivering risk management effectively and efficiently

In the last 10 years, banks have focused on effectiveness to strengthen risk management in the first and second lines. Do firms have the appropriate resources to identify, manage, monitor and mitigate risks? Often, near-term risks – notably, regulatory and reputational – have preoccupied firms. Boards and regulators have had a laser focus on implementing and maintaining a robust set of controls that keep residual risk within the bounds of the agreed-upon risk appetite.

However, risk management is not, and should not be, immune from working efficiently. It has to seek out and continually find ways to conduct its work efficiently.

Deploying technology to manage risk more effectively

Risk management has to deploy new technologies across its own activities, which inevitably will necessitate new operating and talent models. The pace of change in digital risk management is quite remarkable and ongoing. There is significantly more use of automation and data analytics – and the establishment of new industry consortia and utilities – in areas such as know-your-customer and other aspects of financial crime, as well as third-party risk management. Very quickly, the same will be true in other areas, such as cybersecurity and fraud, credit analysis, and regulatory reporting and compliance.⁹

⁹ *Machine Learning in Credit Risk*, Institute of International Finance, <https://www.iif.com/publication/regulatory-report/machine-learning-credit-risk>, May 2018.

Banks identified a range of areas where new technologies will have a material impact:

- ▶ Fraud surveillance – 72%
- ▶ Financial crime – 68%
- ▶ Modeling – 57%
- ▶ Credit analysis – 57%
- ▶ Cybersecurity – 57%
- ▶ Know-your-customer activities – 57%

Other areas that could be impacted include the controls framework (28%), risk reporting (26%), market surveillance (25%) and underwriting (22%).

As last year's EY/IIF global bank risk management survey highlighted, we are on the cusp of a move into transformational reinvention. As such, risk management has to quicken the pace at which it embraces new technologies or it will fall behind.

While some banks believe they have completed their transformation in terms of risk management leveraging new technologies, others are moving more quickly into reinvention than was expected last year. Just over half (54%) view their transformation as partially complete, while about a third (34%) admit they have only just started. G-SIBs are behind their non-G-SIB competitors in executing technology-enabled transformation, perhaps highlighting that smaller banks are more nimble in driving the necessary change.



Enabling secure and safe use of the cloud

Banks are exploring new ways to leverage the use of cloud technology to provide a safer, more secure, cheaper and easier approach to managing their systems and data environment. For the most part, banks are still in the early stages of using the cloud, with usage expected to accelerate. Most (51%) banks are using a hybrid public/private approach to the cloud, and a third (34%) are still only using a private cloud. A tenth of banks are not using cloud technology at all, to their knowledge. Only a handful of banks (4%) are using only a public cloud. Of those using the cloud, most (71%) have deployed it for less than 20% of their environment; less than a tenth have deployed it for more; none have used it for more than a half of their environment.

The benefits of a public cloud will likely lure more banks in that direction.¹⁰ As such, risk management has a critical role to play in validating that a firmwide cloud strategy framework is in place (in some cases, second-line risk will develop and own that framework) so that the deployment of the cloud – especially a public cloud – is done in a well-thought-out and controlled manner. One executive articulates the challenge well: “The desire for activity in areas such as cloud computing is getting ahead of people’s understanding of those technologies. It is very important

¹⁰ IIF Cloud Computing paper (Part 1), Institute of International Finance, <https://www.iif.com/publication/regulatory-comment-letter/iif-cloud-computing-paper-part-1>, August 2018.

to get things onto the cloud responsibly. Regulators and the industry need to develop a good understanding of why we should move to the cloud.”

Banks identify a host of risks that need to be addressed in the cloud framework and ongoing deployment:

- ▶ Data security risk – 94%
- ▶ Third-party risk – 78%
- ▶ Resilience risk – 71%
- ▶ Regulatory risk – 69%
- ▶ Reputational risk – 68%
- ▶ Service level performance – 68%
- ▶ Compliance risk – 66%
- ▶ Legal risk – 54%
- ▶ Geographic location of cloud services – 54%

European banks placed more emphasis on certain risks than on others, notably regulatory risk, legal risk and the geographic location of cloud services. This may reflect a much more significant focus due to the 2018 implementation of the EU’s General Data Protection Regulation.

The potential to leverage technology is significant. As one executive puts it: “Machine learning and AI will become more prevalent in the operations of the bank and the risk function.” However, for many banks, the broad-scale use of new technologies would require far-reaching change in their operating model. “We are currently using new technologies (AI, analytics), mostly for low- or medium-level decisions,” says another risk executive. “We could use them more extensively, but we would need to reorganize quite substantially to do so.”

A similar pattern exists as to the degree that risk management has partnered with FinTech firms (including so-called RegTech and RiskTech firms, which address regulatory compliance and risk management issues, respectively). Only about one in 10 (9%) banks report they are extensively working with such firms. Typically, the engagement is more targeted, with about half (49%) working with a select set of firms and targeting which others to work with, whereas about a third (32%) are still in the exploratory phase. An executive from a bank taking the targeted approach says, “We are using the best of what FinTech can offer, but only for specific needs.” European banks are more active than others in partnering with FinTech firms.

Data analytics: the lifeblood of more effective risk management

Data has been called the new oil. As well as being deeply concerned about the integrity and availability of data, as noted above, banks are equally committed to leveraging it more. “Once you get your basic data right, it can be used to facilitate business in terms of both how we approach clients and how we look at risk,” says one CRO. “We are using analytics, AI and machine learning on unstructured data to identify any emerging risks and how the risk fraternity can manage these risks or use them to the advantage of the bank,” adds another.

In a digital environment, core risk management needs to allow for end-to-end management of the firm’s risk portfolio using data and analytics to provide accelerated identification, measurement and monitoring of customer and portfolio risk signals in support of customer and product strategy and alignment with the board-approved risk appetite. Risk, compliance and control intelligence requirements need to be built in at the design stage so that necessary data is captured from the outset to aid risk monitoring and analysis. Such an approach allows for more real-



time risk detection, more informed and granular risk and reward optimization, and better and more aggregated reporting across the entire organization.

In terms of their risk data management priorities over the next three years, banks are focused on improving data quality (93%), automating processes (74%), and updating data lineage (i.e., data across the life cycle from origin to processing) and controls (57%).

Poor data quality is a major challenge. “Data and data quality are structural issues that most banks have – if you don’t have good data, then by definition a lot of your initiatives will stall,” warns one executive. Banks cited other priorities such as the need to increase data granularity (23%) and use the cloud (23%), and reduce the cost of managing data (19%). (See Enabling secure and safe use of the cloud, on page 19).

There are several factors driving firms to invest in new technologies to better manage risk data, including data quality (80%), data availability for development of new products and better customer experience (67%), data lineage (62%), risk reporting (59%) and regulatory reporting (52%). G-SIBs were more likely to cite wider system rationalization as a driver, reflecting the fact that many G-SIBs are conducting firmwide initiatives to rationalize their processes, and risk management and compliance activities. The automation of data processes is

also a key focus, notably in reporting (74%), extraction (60%), data entry (47%), modeling (46%) and preparation (41%).

A major hurdle to deploying more data analytics is finding and retaining the necessary talent. But there are other constraints as well. For example, poor-quality data (61%) constrains data analytics. Moreover, despite having more scale, G-SIBs identify budgets as a limiting factor more than non-G-SIBs, whereas half of the participants think that non-G-SIBs struggle more with having a strong business case for investment. Over half (54%) cited time spent satisfying immediate regulatory demands as a major constraint on building an effective and efficient data governance model.

Talent remains critical

Technology may elevate the performance and efficiency of risk management, but talent within risk management still plays a critical role in risk strategy and decision-making. Banks expect to add new specialist talent in second-line risk management over the next year (see Figure 8).

Talent needs vary by region. Compared with others, Asia-Pacific banks expect to be filling second-line risk roles in cybersecurity, technology, conduct, liquidity, credit, and

market and counterparty risks. European banks expect to hire more model risk management and stress-testing talent. Latin American banks will be most focused on cybersecurity talent. North American banks expect to focus on hiring in the technology and conduct areas, and are much less likely to hire into financial risk disciplines.

However, long term, a people model based mainly on subject-matter professionals will not suffice – additional new skills will be required, notably linked to data analytics, technology, product design and agile development. “We typically use resources from operational risk, and we need to include more people with deep understanding of the technological components,” asserts one executive.

Soft skills such as communication and negotiation skills; diversity and inclusiveness; and active teaming across lines of business, functions and geographies will become paramount.¹¹ Those who can combine business and technical acumen – and knowledge of customers and products – will move forward faster, gain competitive advantage and excel in a changing world. One risk executive says, “Having the right set of skills is a big issue. We will need more people skilled in data management and analytics, but will still need people with more traditional skills (e.g., credit risk, market risk, etc.). We are currently going through an exercise to inventory existing skills and assess what will be needed in the future. We are investing heavily in training staff.”

¹¹ To learn more about skills required by a new generation of risk professionals, refer to the EY article: “Do you have the right talent to take the right risks?”, https://www.ey.com/en_gl/digital/do-you-have-the-right-talent-to-take-the-right-risks.

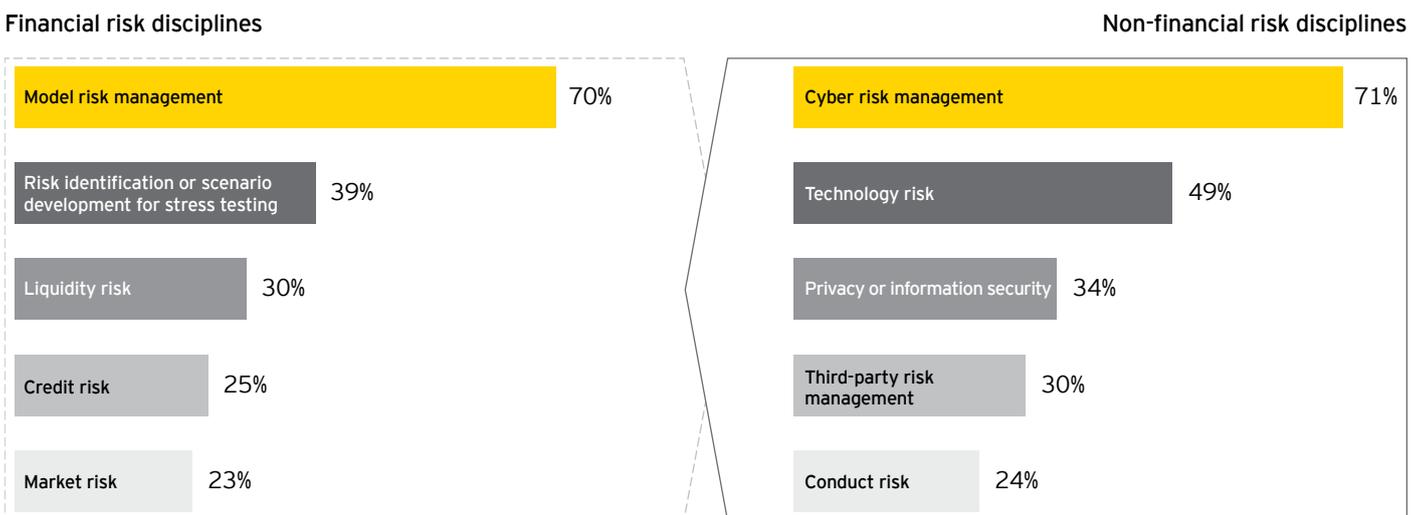
Finding necessary talent will be challenging and will call for a range of approaches. For example, in the risk data management area, banks listed a number of talent strategies:

- ▶ Hire new staff with necessary skills – 80%
- ▶ Enhance training – 70%
- ▶ Build in-house – 58%
- ▶ Use third parties on projects – 51%

Some banks cited staff augmentation (23%), outsourcing to third parties (22%) and the use of third-party industry utilities or consortia (20%). European and North American banks were more likely to cite utilities, reflecting the fact that new utilities are being created in those regions. Utilities will likely become an ever more important way to address talent challenges as they get established in new domain areas.

Without a new approach to talent, banks will struggle to transform their firms and risk management. Data analytics highlights this visibly. Attracting and retaining top talent is viewed as the most significant constraint on developing data analytics, alongside poor data quality (both cited by 61% of participants). Similarly, one of the most significant hurdles to implementing an effective and efficient data governance model is insufficient talent.

Figure 8: Additions to second-line risk management



4

Managing through, and recovering from, disruptions



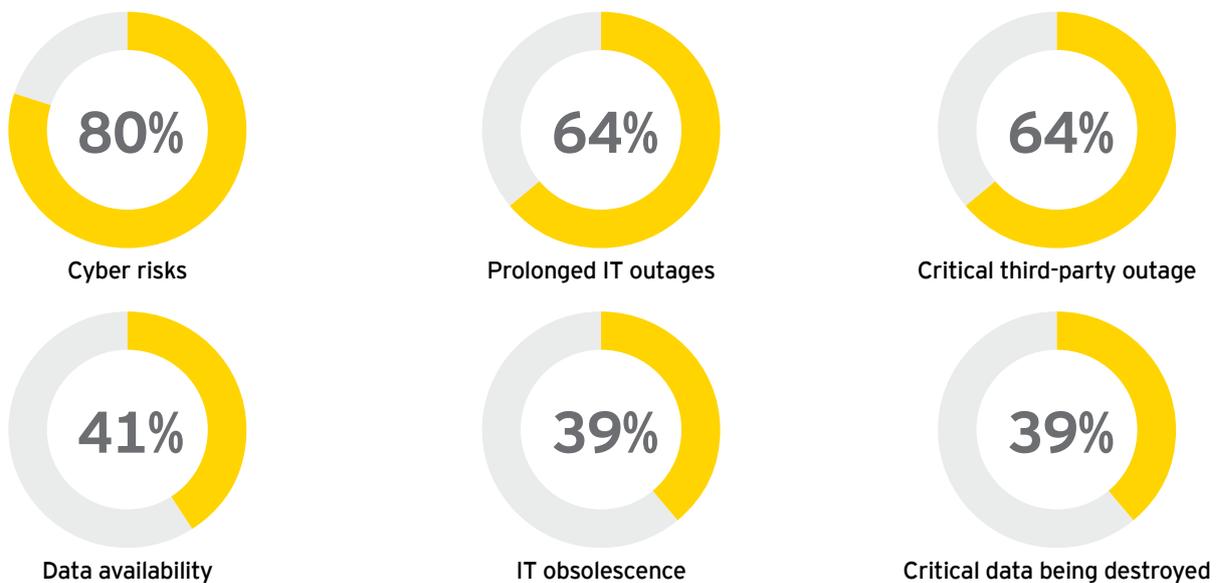
Risk management has a central role to play in not only helping navigate the evolving risk profile but also in preparing for, managing through and recovering from disruptions.¹²

Such disruptions are becoming more commonplace, making senior executives increasingly concerned about their firms' true resiliency capabilities. Cyber attacks are driving some of these concerns (80%, as shown in Figure 9), as is an elevated focus on fragile information technology and more frequent and pronounced weather-related disasters. Dependency on third- and fourth-party providers, industry consortia and new partners (e.g., FinTechs) is accentuating the focus on resiliency because dependencies and concentration risks in the ecosystem are being created or amplified.

Several risk executives interviewed for this survey identified resilience – a combination of operational, technological and financial resilience – as the critical go-forward risk to be managed. "Resilience is the new stress test or resolution plan," says one. Another adds, "A key priority for risk is operational resiliency and continuity, inclusive of legacy technology – especially being a global bank and given the current regulatory focus on this topic."

Concerns vary by region. African and Middle Eastern banks are more concerned than others about third-party outages and ransomware, whereas those in Asia-Pacific worry most about IT outages inside their organizations. European banks are more concerned about business-model viability as a specific risk than banks in other regions but less concerned than North American banks about cyber risks, third-party outages and data destruction. Latin American banks most fear cyber risks and IT obsolescence. A quarter of all banks cited ransomware, as well as concerns about a systemic player getting disrupted for a prolonged period.

Figure 9: Top resiliency concerns



The link to cyber threats is palpable for many risk executives. "One of the main aspects of the cyber risk management program is to get cyber-resilient; and the old business continuity program may not be good enough for this," admits one executive. However, addressing this ever-growing risk is challenging, especially as it quickly jumps to broader technology resilience. Another CRO remarks, "From a technological point of view, how resilient do you want your system to be? You can't be too resilient or else everything slows down. Contingency planning is key."

The degree of change taking place in banks is a factor that risk management should consider in the context of resilience. Two areas of change are:

- **Major projects and initiatives:** Risk can assess the impact on the firm's risk profile (70%), monitor operational risk (77%), how well controls are implemented (51%) and the progress in implementation (44%).
- **Risk culture:** Risk can monitor culture at the enterprise level (70%) and business-unit level (49%), and define key risk indicators to assess change management (51%).

Increasingly, however, firms recognize that their continuity activities are disparate and unconnected. They often have countless activities across business continuity, disaster recovery, cyber incident response and crisis management (and for large banks, the integration with recovery and resolution planning). Often, myriad crisis and contingency plans exist across lines of business, technology, human resources and other areas. Few plans are connected or consistently applied, few have common or consistent triggers for escalation and decision-making, and few have properly prepared their senior executives and/or boards for actual crises. The result is often ineffective or slow decision-making in times of stress (see Learning from others' crises, on page 24).

¹² To learn more about emerging continuity factors refer to the EY article *Managing through crises: preparation is key*, [https://www.ey.com/Publication/vwLUAssets/ey-managing-through-crises/\\$File/ey-managing-through-crises.pdf](https://www.ey.com/Publication/vwLUAssets/ey-managing-through-crises/$File/ey-managing-through-crises.pdf).

Learning from others' crises

Headline risk seems to have risen in financial services, due to increased event risk such as weather-related events, vendor or system outages, cyber attacks, or geopolitical and macroeconomic instability. With a heightened probability of disruption to the continuous delivery of services, firms keep asking: what can we learn from others who have experienced a major crisis?

Banks cite a range of reasons why they think other firms struggled to manage through past crises:

- ▶ Lack of preparedness – 69%
- ▶ Slow decision-making – 61%
- ▶ Ineffective crisis management governance or protocols – 61%
- ▶ Mishandling of media or corporate communications – 60%
- ▶ Weak escalation processes – 47%
- ▶ Ineffective communications with customers – 41%
- ▶ Lack of understanding about cause of crisis – 26%

Not surprisingly, banks are building new approaches to implement a more integrated firm resilience strategy and organization. Indeed, some banks are consolidating disparate activities into a new or enhanced unit or function, typically as an enterprise-level group within the first line, and pulling together a range of activities, which can include:¹³

- ▶ Business continuity plans – 71%
- ▶ Crisis management – 71%
- ▶ Cyber incident response – 68%
- ▶ Disaster recovery – 64%
- ▶ Technology incident response – 59%
- ▶ Crisis communications – 58%
- ▶ Recovery and resolution planning – 51%
- ▶ Simulation or tabletop exercises – 48%
- ▶ Industry-level initiatives – 19%

Within this, the role of risk management in firmwide resiliency is changing. According to one executive, “A significant part of risk management’s responsibilities is ensuring bank resilience. The true test is how they practically embed the plans they come up with in the day-to-day running of the bank.”

Key roles for second-line risk management now include:

- ▶ Active participant in crisis management plan – 82%
- ▶ Provides effective challenge of the first line’s implementation of the firmwide resiliency framework – 71%
- ▶ Sets and monitors enterprise-level risk appetite for resilience risk – 56%
- ▶ Sets and monitors enterprise-level resilience risk metrics – 50%
- ▶ Validates that resilience risk is incorporated into the firm’s risk management structure and taxonomy – 50%
- ▶ Establishes firmwide resilience risk framework – 49%
- ▶ Manages crisis management plan/process – 47%
- ▶ Evaluates technology resilience – 47%
- ▶ Sets requirements for technology resilience, e.g., recovery time objectives – 37%

Second-line risk management also can play an important role in third-party risk related to resilience; almost half (49%) independently conduct periodic assessments of critical third parties, and over a third (36%) independently assess criticality of third parties. Some banks’ risk management groups evaluate single points of failure within their firm (32%) and within the broader financial ecosystem (24%).

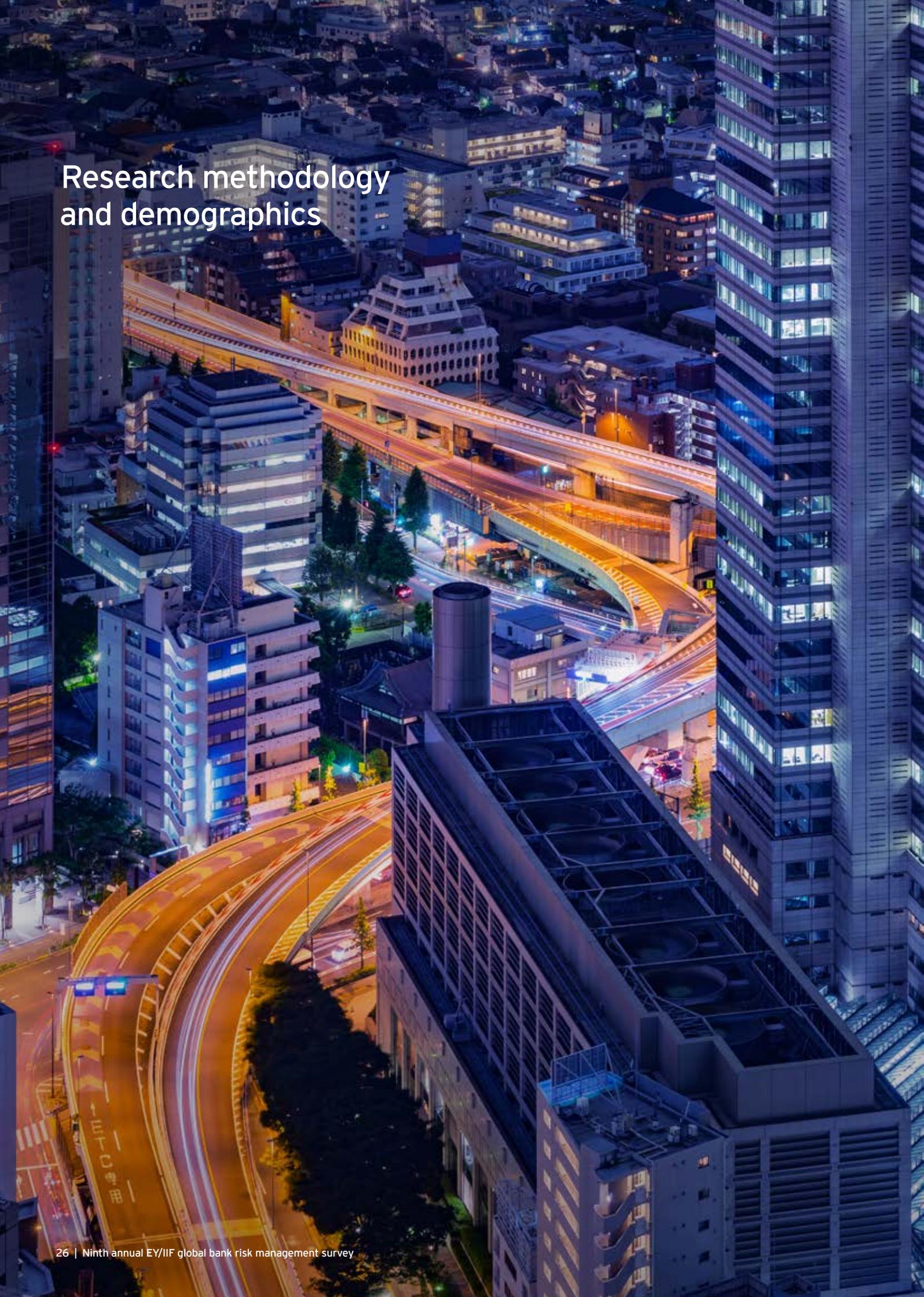
¹³ [https://www.ey.com/Publication/vwLUAssets/ey-getting-serious-about-resilience-a-multiyear-journey-ahead/\\$File/ey-getting-serious-about-resilience-a-multiyear-journey-ahead.pdf](https://www.ey.com/Publication/vwLUAssets/ey-getting-serious-about-resilience-a-multiyear-journey-ahead/$File/ey-getting-serious-about-resilience-a-multiyear-journey-ahead.pdf)



Conclusion: Transforming to a digital future to address risk imperatives

The financial services industry is undergoing a massive transformation, and risk management runs the risk of falling behind and staying focused only on downside risk.

Over the past decade, risk management has helped restore and protect franchises and the industry at large. That role remains critical. However, risk management will now have to undertake a transformation that feels even more substantial. It has to build on solid foundations and its strong stature across the firm to be a leader in enabling business transformation – adapting to a fast-changing risk environment – and in helping the firm manage through, and recover from, disruptions. It must do so in an extremely effective and efficient manner.

An aerial night photograph of a city, likely Tokyo, showing a complex highway interchange with light trails from traffic. The surrounding area is filled with various buildings, some of which are brightly lit, creating a vibrant urban scene. The text 'Research methodology and demographics' is overlaid in the upper left corner.

Research methodology and demographics

EY member firms, in conjunction with the IIF, surveyed IIF member firms and other top banks in each region (including a small number of material subsidiaries that are top-five banks in their countries) from June 2018 through September 2018. Participating banks' CROs or other senior risk executives were interviewed, completed an online survey, or both. In total, 74 firms across 29 countries participated. The charts in this report display data for banks that completed the quantitative online survey, while the text includes information gleaned from both the quantitative survey and qualitative interviews.

Participating banks are listed below by geographic region. An asterisk after the bank name indicates it is one of the 18 G-SIBs that participated. Of the others, 39 are

domestic systemically important financial institutions (SIFIs). Participating firms represented a range of asset size (as of 31 December 2017) from 15% having US\$1t or more to 28% having US\$100b or less; the largest percentage (37%) was in the US\$100b to US\$499b range. Most (73%) of the institutions operated in four or more countries, with 17% operating in more than 50 countries. Many (45%) viewed their institution as a universal bank; 39% considered their institution as primarily a retail and corporate bank, and 6% as primarily an investment bank.

Note that 14 additional financial institutions participated informally by responding to the survey, but their data and participation is not included in this survey report.

Africa/Middle East	Asia-Pacific	Europe	Latin America	North America
ABSA Bank	Agricultural Bank of China*	ABN Amro	Banco de Bogota	American Express
Al Rajhi Bank	Bank of the Philippine Islands	Barclays*	Banco de Crédito del Perú	Bank of Montreal
Arab Bank	CIMB Bhd	BBVA	Banco de la Nación Argentina	Bank of Nova Scotia (Scotiabank)
Discovery	ICBC*	Commerzbank	Banco do Brasil	BB&T
FirstRand Bank	ICICI	Credit Suisse*	Banco Frances BBVA	CIBC
Investec	Macquarie	Danske Bank	Banco General	Comerica
National Bank of Kuwait	Maybank	Deutsche Bank*	Banco Inbursa	Desjardins
Standard Bank Group	Mitsubishi UFJ Financial Group*	HSBC*	Banco Macro	FifthThird Bank
	Mizuho Financial Group*	Intesa Sanpaolo	Banco Patagonia	Goldman Sachs*
	Sumitomo Mitsui Financial Group*	KBC Group NV	Bancolombia	Huntington Bank
	Suncorp	Kommunalbanken	BBVA Bancomer	Keycorp
	The Norinchukin Bank	Lloyds Bank	Citibank Argentina	M&T Bank
	United Overseas Bank	Nationwide Building Society	Grupo Financiero Banorte	Morgan Stanley*
		Nordea Bank AB*		Northern Trust
		Nykredit		Regions Bank
		Santander*		Royal Bank of Canada (RBC)*
		Skandinaviska Enskilda Banken AB (SEB)		State Street Corporation*
		Standard Chartered*		SunTrust Bank
		UBS*		Toronto-Dominion Bank
		UniCredit*		U.S. Bancorp

* Designated as a G-SIB by the Financial Stability Board in November 2017

EY contacts

Global

Bill Schlich
Global Banking & Capital Markets Leader
Toronto
bill.schlich@ca.ey.com
+1 416 943 4554

Jan Bellens
Global Banking & Capital Markets
Deputy Leader
Singapore
jan.bellens@sg.ey.com
+65 6309 6888

Dai Bedford
Global Banking & Capital Markets
Advisory Leader
London
dbedford@uk.ey.com
+44 20 7951 6189

Keith Pogson
Global Banking & Capital Markets
Assurance Leader
Hong Kong
keith.pogson@hk.ey.com
+852 28499227

Americas

Tom Campanile
Partner, Financial Services
New York
thomas.campanile@ey.com
+1 212 773 8461

Adam Girling
Principal, Financial Services
New York
adam.girling@ey.com
+1 212 773 9514

Americas (continued)

Gary Kozlowski
Latam Financial Services Leader
New York
gary.kozlowski@ey.com
+1 212 773 1011

Bismark Rodriguez
Partner, Financial Services Risk Management
Panamá
bismark.rodriguez@pa.ey.com
+507 208 0160

Mario Schlener
Partner, Financial Services Advisory
Toronto
mario.schlener@ca.ey.com
+1 416 932 5959

Mark Watson
Executive Director, Financial Services
Boston
mark.watson@ey.com
+1 617 305 2217

Asia-Pacific

Gary Mellody
Partner, Financial Services
Singapore
gary.mellody@sg.ey.com
+65 6309 6519

Doug Nixon
Partner, Financial Services
Sydney
douglas.nixon@au.ey.com
+61 2 9276 9484

Sameer Rege
Partner, Financial Services
Hong Kong
sameer.rege@hk.ey.com
+852 28499458

Asia-Pacific (continued)

David Scott
Partner, Financial Services
Hong Kong
david.scott@hk.ey.com
+852 26293070

Yoshio Wagoya
Partner, Financial Services Advisory
Tokyo
yoshio.wagoya@jp.ey.com
+81 3 3503 1110

EMEIA

(Europe, Middle East, India, Africa)

Frank de Jonghe
Partner, Financial Services
Brussels
frank.de.jonghe@be.ey.com
+32 2 774 9956

John Liver
Partner, Financial Services
London
jliver1@uk.ey.com
+44 20 7951 0843

Ivica Stankovic
Partner, MENA Financial Services
Kuwait
ivica.S@kw.ey.com
+965 22955000

Abigail Viljoen
Partner, Financial Services Africa
Sandton
abigail.viljoen@za.ey.com
+27 72 566 3555

Max Weber
Partner, Financial Services Risk
Stuttgart
max.weber@de.ey.com
+49 711 9881 15494

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

About EY's Global Banking & Capital Markets Sector

In today's globally competitive and highly regulated environment, managing risk effectively while satisfying an array of divergent stakeholders is a Sector key goal of banks and securities firms. EY's Global Banking & Capital Markets network brings together a worldwide team of professionals to help you succeed – a team with deep technical experience in providing assurance, tax, transaction and advisory services. The Sector team works to anticipate market trends, identify their implications and develop points of view on relevant sector issues. Ultimately, it enables us to help you meet your goals and compete more effectively.

© 2018 EYGM Limited.
All Rights Reserved.

EYG no: 011872-18Gb1
1809-2901375
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com/bankingrisk

The views of third parties set out in this publication are not necessarily the views of the global EY organization or its member firms. Moreover, they should be seen in the context of the time they were made.

About the Institute of International Finance

The Institute of International Finance (IIF) is the global association of the financial industry, with close to 500 members in more than 70 countries. Its mission is to support the financial industry in the prudent management of risks; to develop sound industry practices; and to advocate for regulatory, financial and economic policies that are in the broad interests of its members and foster global financial stability and sustainable economic growth. IIF members include commercial and investment banks, asset managers, insurance companies, sovereign wealth funds, hedge funds, central banks and development banks.

The Institute of International Finance (IIF)
1333 H St NW, Suite 800E
Washington, DC 20005-4770
USA

Tel: +1 202 857 3600
Fax: +1 202 775 1430

www.iif.com
info@iif.com

