Eighth annual global EY/IIF
bank risk management survey

Restore, rationalize and reinvent

A fundamental shift in the way banks manage risk

IIF
Institute of International Finance

EY
Building a better working world

Contents

Executive summary

The seventh annual global bank risk management survey — *A set of blueprints for success*, produced by EY and the Institute of International Finance (IIF) last year — showed signs that the industry was reaching a key turning point in risk management. After more than seven years of enhancing risk functions, this year's survey shows banks now face a new set of challenges as they move through the 15-year transformation in managing risk that was identified in last year's survey.

Three phases of risk management's transformation

The risk management journey spans three broad phases (see Table 1):

1. **Restore:** the first phase focused on compliance with the global regulatory agenda and restoring trust in banking. Initially, the agenda was prudential in nature, but increasingly conduct regulation expanded. Banks made tactical enhancements to existing frameworks, then began redesigning the overall risk management architecture,

Industry's 15-year risk management journey

	First phase: post-crisis (five to six years)	Middle phase — now	Coming years
	Restore	**Rationalize**	**Reinvent**
Regulatory context	▸ Coordinated global response ▸ Primarily prudential in nature	▸ Implementation ongoing, increasingly conduct-related ▸ Signs of global fragmentation, with taking stock on impact in totality	▸ Revisions to reforms, more local variation ▸ New modes of regulation/ supervision to accommodate innovation and FinTech
Technology focus	▸ Sustaining legacy systems ▸ Addressing identity access management inadequacies	▸ Digitizing customer experience and interface ▸ Implementing three-lines-of-defense cyber risk management	▸ Digitizing middle and back office, and risk function ▸ Building in cybersecurity across the firm (e.g., in M&A, due diligence, new product development)
Risk focus	▸ Building foundational elements ▸ Primarily financial risks ▸ Curtailing risk taking and product development	▸ Embedding risk discipline into businesses ▸ Primarily non-financial risks ▸ Enabling risk taking	▸ Enabling and driving digital innovation ▸ Balancing risk taking and risk discipline
Three lines of defense focus	▸ Building overall framework ▸ Expanding headcount in first and second lines ▸ Controls effectiveness	▸ Implementing operating model ▸ Stabilizing/reversing people growth ▸ Balancing effectiveness and efficiency	▸ Enabling risk management through automation, machine learning and artificial intelligence (AI)

notably implementing a three-lines-of-defense approach to risk. The aim was to improve effectiveness of risk and controls, not necessarily to do so cost-effectively. The go-to solution was to add headcount, which could be done relatively quickly.

Banks strengthened their balance sheets by raising capital and adjusted their funding models to broaden sources of liquidity. Strategic changes — notably reducing or shuttering business lines and withdrawing from certain markets — were more the consequence of higher capital, liquidity and compliance costs than of enhanced competition. Consequently, in a macroeconomic environment driven by austerity and the central banks' low or even negative rate monetary policy, banks' business models were (and still remain) challenged. Return on equity (ROE) targets (in better times, 25% or more) were substantially revised downward, which shareholders had to accept.

2. **Rationalize:** the second and current phase of the risk management journey focuses on migrating toward a digital environment and compliance. Regulation and supervision remain important given that post-crisis rules will take years to fully implement, and may become harder, especially if fragmentation in the global regulatory agenda increases. Other risks have risen on board and chief risk officer (CRO) agendas, most notably cyber risks. The competitive landscape is now changing significantly. Banks are more focused on the cost of risk management, initially through the simplification of organizational or legal-entity structures or processes.

   Increasingly, technology is driving change. Technology has been used initially to enhance the interface with customers, in line with broader industry and societal changes in how people interact with companies and each other. Significant progress has been made, especially in the use of applications, but there is more transformational change to come, in areas such as biometrics and consumer wearables. The use of other technologies — across businesses or within risk management — has been limited thus far, with novel proofs of concept being broadened. Meanwhile, some shareholders have grown impatient and expect banks to deliver on their ROE promises.

3. **Reinvent:** the next phase — which will start in earnest in the coming years — calls for a reinvention of risk management. Technology and open banking will fundamentally change the way banks operate and allow them to deliver seamlessly, and cost-effectively, on their digital promise to customers. Banks will have to consider alternative resourcing models, such as third-party managed service delivery models and industry-wide utilities.

   Risk management functions will have to transform and move from spectators of digital transformation to enablers and drivers. This will test risk management to its core. Banks will have to rethink how they manage risks, what risks need to be managed, and what new types of talent will be required. Real-time risk management and compliance will become commonplace, as will much faster product-development-to-launch life cycles. Banks will need to manage this transformation carefully. Regulators and boards will want strong evidence that risk management and controls remain robust, especially where there has been a focus on cost containment. After all, they will want to know risk management is faster and smarter, not simply cheaper.

Five broad challenges

As banks transition from the middle to third phase, the 2017 EY/IIF risk management survey identifies five broad challenges that banks must navigate:

1. **Manage emerging risks and increased competition (pages 5-15):** the range of risks facing the industry are changing materially in the short and long term. Broader geopolitical, social and environmental concerns are looming larger, as are signs of global regulatory fragmentation. Competition is becoming more intense. The growing FinTech assault is being accentuated by an arguably more fundamental surge of major technology companies into profitable parts of financial services. At the same time, banks' strategic options to deliver on ROE targets of 11%-15% are narrowing — much of the de-risking agenda has been completed, as have the major changes to capital, liquidity and funding. Optimizing capital is a game changer that will call for more sophisticated frameworks and improved data quality. More broadly, banks will have to address the massive challenge of having vast amounts of data: it will either be a liability, due to poor quality and lack of protections, or an asset, if managed and leveraged properly.

2. **Lead a digital transformation of risk management (pages 16-24):** banks continue to simplify their organizational or legal-entity structures or processes. However, increasingly, technology is driving change and customer interface. As the industry's digital transformation accelerates, banks will move from

exploring to implementing firmwide uses of new technologies in the middle and back office. This will challenge risk functions to change how they monitor banks' risk profiles and enable innovation, as well as how they leverage new techniques to be smarter, faster and more cost-effective. This evolution will call for different operating models, new forms of governance and talent needs within risk functions. Major obstacles to the digital transformation include a shortage of talent and cybersecurity concerns.

3. **Operationalize the three-lines-of-defense model (pages 25-29):** after making broad framework changes in recent years, banks are now firmly focused on the difficulties of operationalizing the three-lines model in a way that delivers both effective risk management and cost efficiency. As banks slow the rate of growth in risk and compliance headcount, they also expect talent shortages across all three lines in areas such as advanced data analytics and model risk.

   Standardizing approaches to risk and controls across the enterprise is accelerating, despite a slower than expected rollout of the underlying technologies that enable this, such as enterprise governance, risk and control (eGRC) platforms. Testing in such areas as compliance or operational risk is a core focus, including aligning and automating testing standards and approaches, along with centralizing teams by establishing centers of excellence.

4. **Manage non-financial risks, like conduct, cost-effectively (pages 30-36):** after a decade of reducing intrinsic conduct risk by de-risking (for example, simplifying products), the industry is now developing and implementing approaches to manage conduct risk, so banks can deliver products in the way promised to customers. A majority have implemented conduct risk frameworks as a starting point to determine what conduct risk is, where it occurs, and how to measure and monitor it (i.e., how it can be quantified and aggregated across the firm). However, the industry has a long way to go before framework operating effectiveness is proven and more cost efficient.

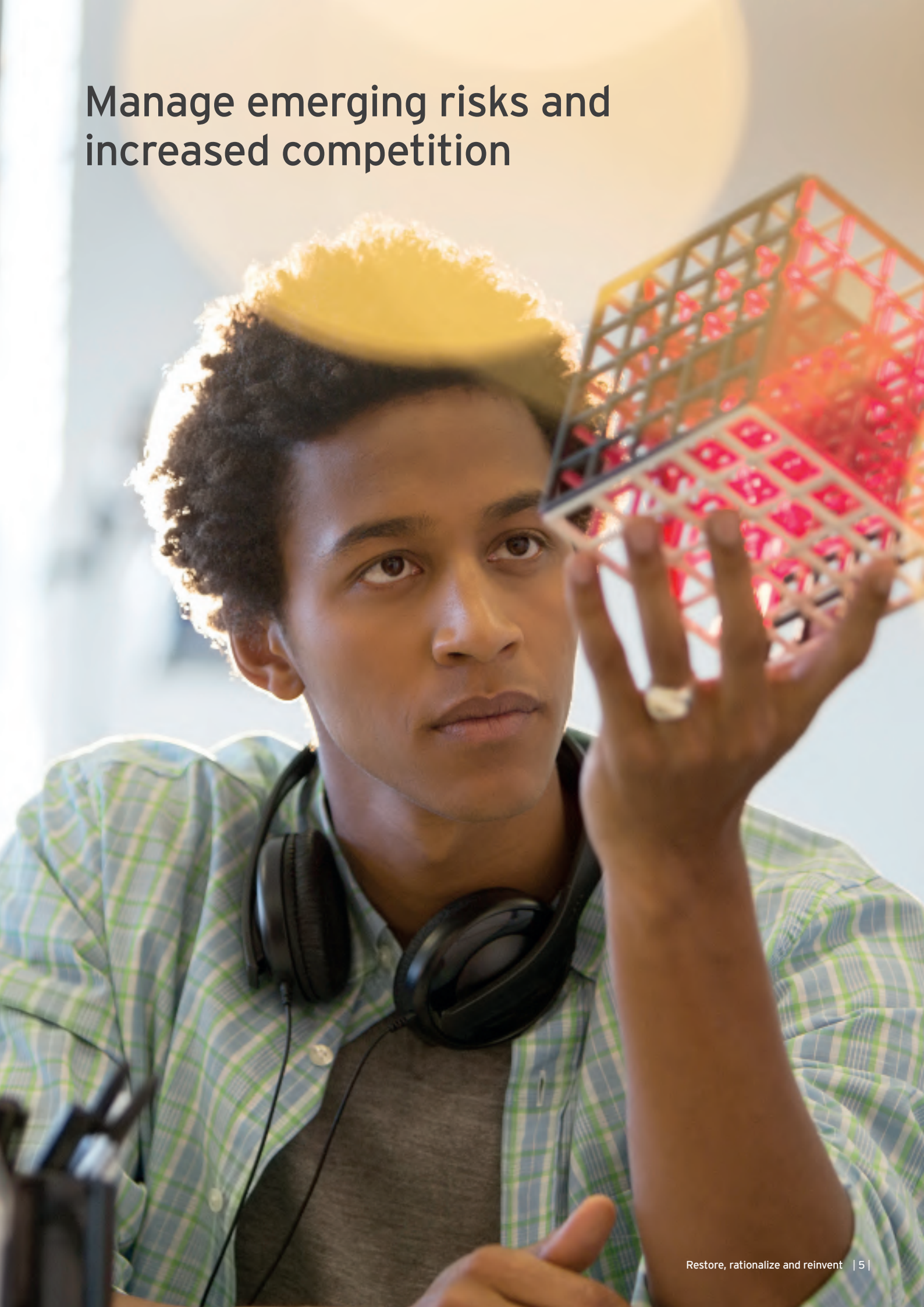
   Banks continue to evolve and implement their risk appetite frameworks and still face common challenges. From a design perspective, this includes expressing appetite for all types of risks, and from an implementation perspective, cascading appetite down into business units. The question of the rationale for, and approach to quantifying, non-financial risks still taxes the industry, especially for risks such as reputational, strategic and cyber risks. There is a natural desire to quantify these risks to aggregate them, but these risks do not easily lend themselves to quantification, and concerns remain around what gets lost when these risks are defined through a narrow set of metrics.

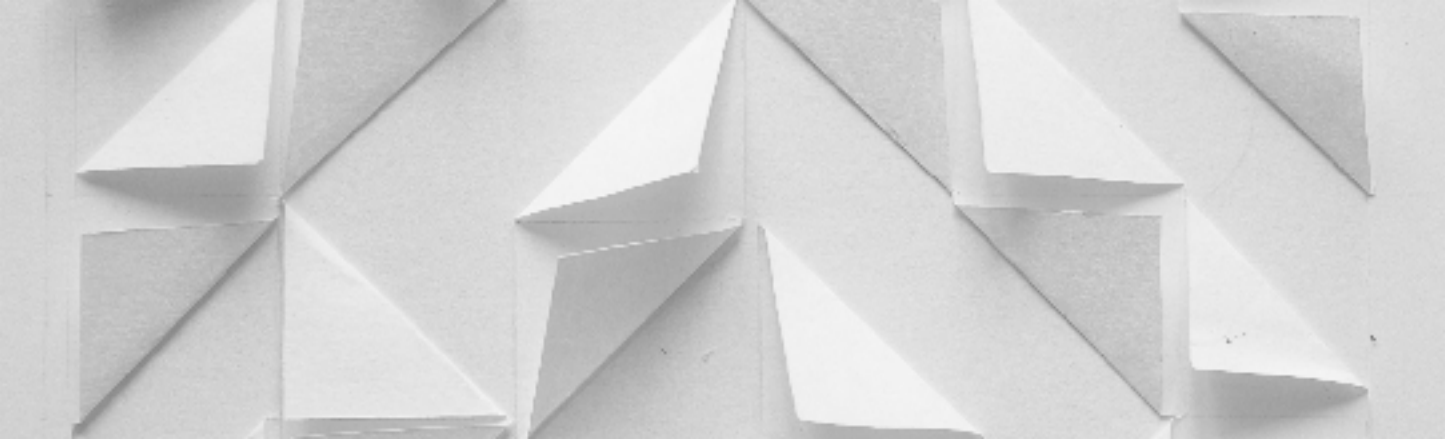
5. **Stay resilient and protect against cyber risks (pages 37-43):** increasingly, the industry is focused on operational and cyber resiliency. Banks are rethinking what constitutes operational resiliency. Core competencies, like business continuity and disaster recovery, remain important. However, to make real progress, some foundational elements, such as data quality and mapping critical process flows, need enhancing. The industry continues to move quickly to manage cyber resiliency across the three lines of defense, with more robust oversight by the board of directors. The quantification and reporting of cyber risks is still challenging for most banks, regulators and supervisors. Managing critical vendors is a key challenge for both operational and cyber resiliency. In some ways, the industry's biggest challenge over the next decade is determining where to focus.

   Banks have to prioritize more than ever. They need to determine which customers to serve, what products and services to offer, how they will be offered and in what countries they will operate. They need to focus on the most critical things and do them exceptionally well. This extends beyond so-called core competencies. Banks had better play to their strengths. But they also need to prioritize the resiliency and protection of critical processes and systems, information security, and managing critical vendors and the most significant enterprise-wide risks. Without such prioritization, investments and management attention will get too dispersed.

Being able to manage multiple challenges and changes simultaneously will distinguish the leaders. As one CRO concluded, "It is as though we are changing the tires — i.e., dealing with our vulnerabilities — while driving, i.e., digitizing our business, implementing automation, dealing with real-time payments and so on." That's no easy feat.

Manage emerging risks and increased competition





The industry has weathered significant challenges over the past decade, from the financial crisis, which was viewed as a once-in-several-generations event to the global overhaul of regulation and the degree to which global banking has for many been pushed back to a more regional model. It has been a tumultuous decade across the industry. Political uncertainty can be seen in Western, as well as developing, markets with unexpected outcomes in terms of political leadership in some countries and Brexit, the UK's decision to exit the European Union (EU). The only certainty in banking appears to be uncertainty.

Top risks in the year ahead

As a result, risk priorities continue to evolve. Implementation of new regulatory and supervisory requirements remains a key industry focus. This is especially the case in regions such as Europe, where supervisors like the European Central Bank (ECB) are rolling out a substantively new supervisory regime.

Still, other priorities have also come to the fore (see Figure 1). Cyber now ranks as the No. 1 risk in the boardroom, a significant change given only 10% of CROs cited this risk as top of mind four years ago. Conduct risk also is moving up CROs' agendas, particularly in North America, reflecting continued challenges in managing employee behavior and new instances of sales practices misconduct.

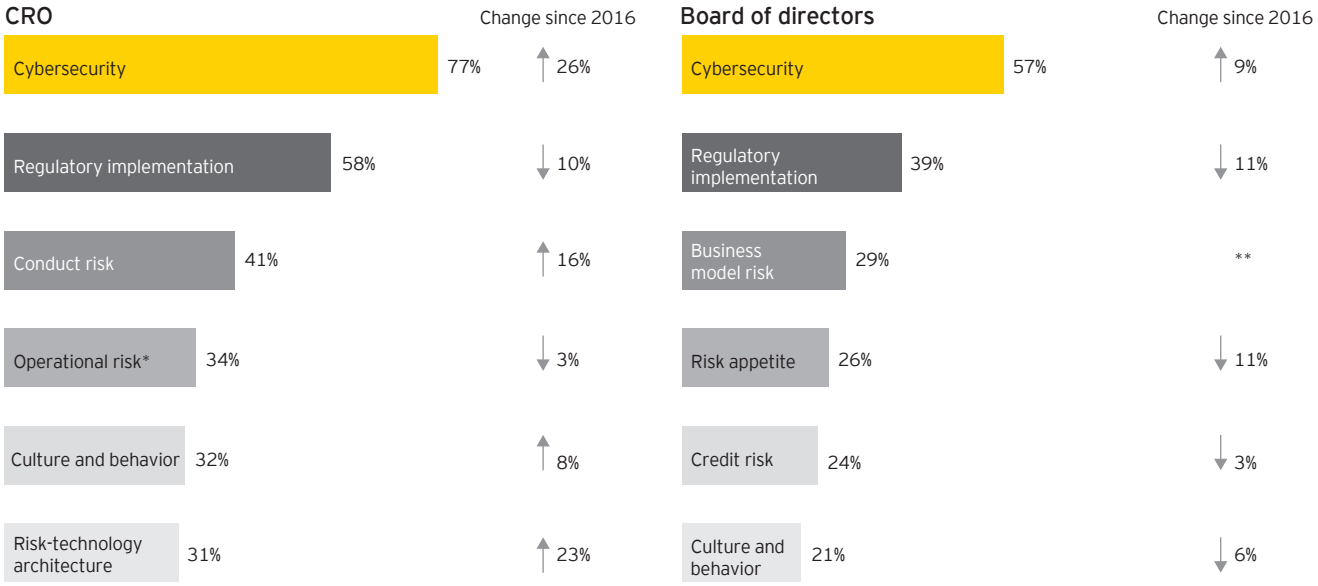
Digitization, new consumer trends and competitive threats, in combination with elevated cost and income ratios, post-crisis, have led to markedly lower ROEs than pre-crisis. This, in turn, has driven the degree to which banks' business models have changed, and continue to do so. As such, boards remain fixed on business model risk, although CROs do not rank this risk so highly. This could reflect differing perspectives on how much ongoing regulatory implementation and intensifying competition — especially from outside the industry — may change future business models, or simply reflect the fact that directors are generally thinking more about strategy than tactical operational issues.

Boards and CRO risk priorities vary by region and by type and size of institution. For example, North American CROs are more likely (57%) to view conduct risks more prominently than banks in Africa and the Middle East (50%), Asia-Pacific (40%), Europe (30%) and Latin America (22%). This reflects the fact that in some countries, such as the UK, regulators have been pushing conduct reform for some time, while US interest has been more recent, given well-publicized sales practices at several banks. By contrast, Asia-Pacific and North American banks (40% and 43%, respectively) are less focused on risks associated with implementing new regulations or supervisory standards than their peers in Africa and the Middle East (100%), Europe (65%), and Latin America (78%). This likely reflects the differing pace and drivers of regulatory change in each region.

"Data is a massive concern. The issue is not just implementing data-related regulations, but also how to use data optimally and protect the franchise."

— Risk executive

Figure 1: Top-of-mind risks for CROs and boards



*Excluding cybersecurity

**Not in 2016 survey

Emerging longer-term risks

The degree of change and uncertainty over the past decade, from a regulatory and economic perspective, has made it difficult for banks to look too far forward. Near-term issues have emerged at a regular frequency and dominated board and management agendas.

As banks try to focus more on the long term, they have identified a number of significant long-term emerging risks, as shown in Figure 2. Several such risks stand out:

- **Data risk:** data is the very fabric of the industry and may prove to be a critical success factor both for long-term players and non-financial-services technology giants moving into the industry. As one executive put it, "Data is a massive concern. The issue is not just implementing data-related regulations, but also how to use data optimally and protect the franchise." Another executive said, "Data presents the greatest opportunity for further integration," with another expanding on that concept when noting that "while different functions use data outputs differently, those differing uses should be made on the basis of the same, centrally produced data — so there is no use in duplicating the data production process." Data also provides a competitive edge. As one executive said, "The use of customer data is just in the beginning [stage]." Given the importance of data, ensuring its confidentiality, availability and integrity is of paramount importance, thus, the view that data risk is so important. This partially explains the increased focus on cybersecurity, as well.

"Regulatory pressure is definitely not slowing down."

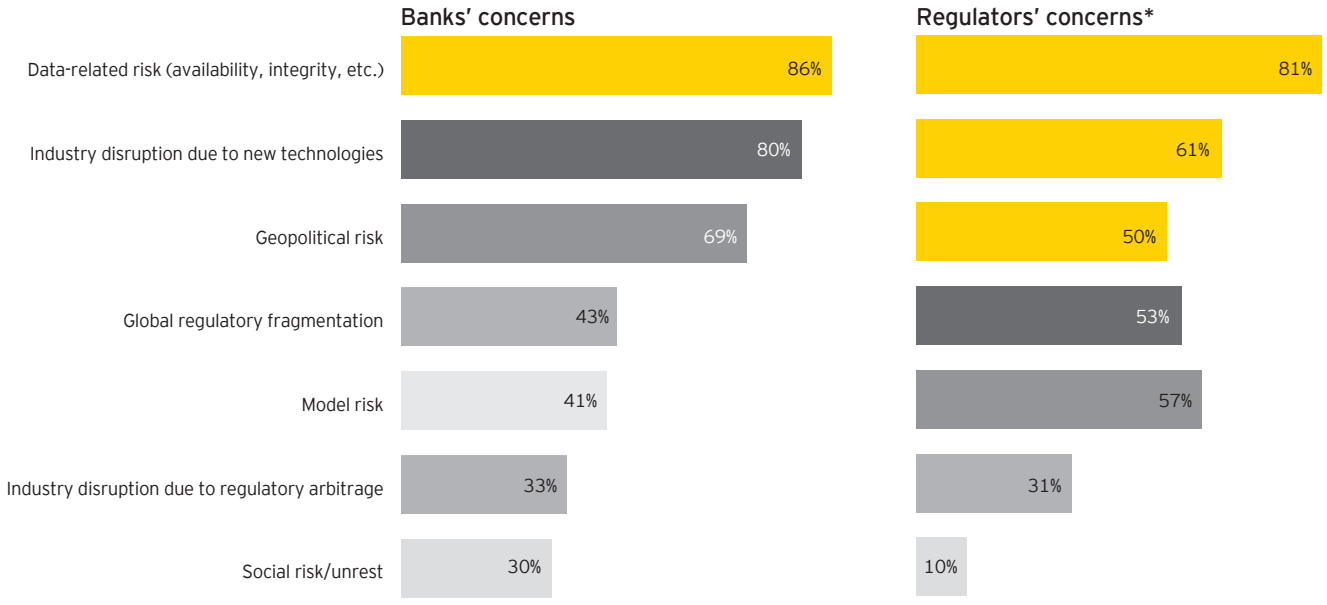
— Chief risk officer

- **Regulatory fragmentation:** some emerging risks, particularly regulatory fragmentation and arbitrage, have been foreshadowed for some time. If anything, the past decade has seen unprecedented global regulatory coordination and agreement on the major areas where reform was required. There hasn't quite been global harmonization, but as close as the industry may come to it. Yet, as political agendas have shifted, regionalism and nationalism have started to creep in. Differing flavors of the same global regulation are now being implemented by national authorities, creating inconsistencies (often material) across borders and, thus, implementation challenges for firms operating in multiple markets. Over the next five years, banks expect regulatory fragmentation to be most likely as it relates to capital buffers (69%), stress testing (61%), models (52%), liquidity buffers (40%) and corporate structures (25%), such as the differing approaches to intermediate holding companies in Europe and the US. Industry leaders have expressed concerns over growing global fragmentation in areas such as privacy and cybersecurity regulation.

- **Global shifts:** some tectonic global shifts are emerging as major risks for the industry over the next decade. Geopolitical risk is viewed as more prominent than any time in the last 25 years. "Geopolitics, including second order effects, create a changing world where we do not know what comes next," said one executive. Social unrest, environmental risk and the aging population are emerging industry risks. Several CROs noted the growing importance of environmental risks, particularly for enhanced climate-change reporting requirements, globally and regionally. Of course, some of these global trends present opportunities for the industry, notably meeting new financial-service needs of the elderly and providing products and services that focus on green investments.

Banks felt that regulators prioritized several emerging risks more highly, notably global regulatory fragmentation, model risk, electronic trading and anti-trust matters. The reasons for differing perspectives on priorities for banks vs. regulators vary by type of risk. For example, while banks may have faith in their internal models, a perceived lack of adequate governance and transparency may explain why model risk is higher on regulators' agendas.

Figure 2: Top emerging risks over next five years



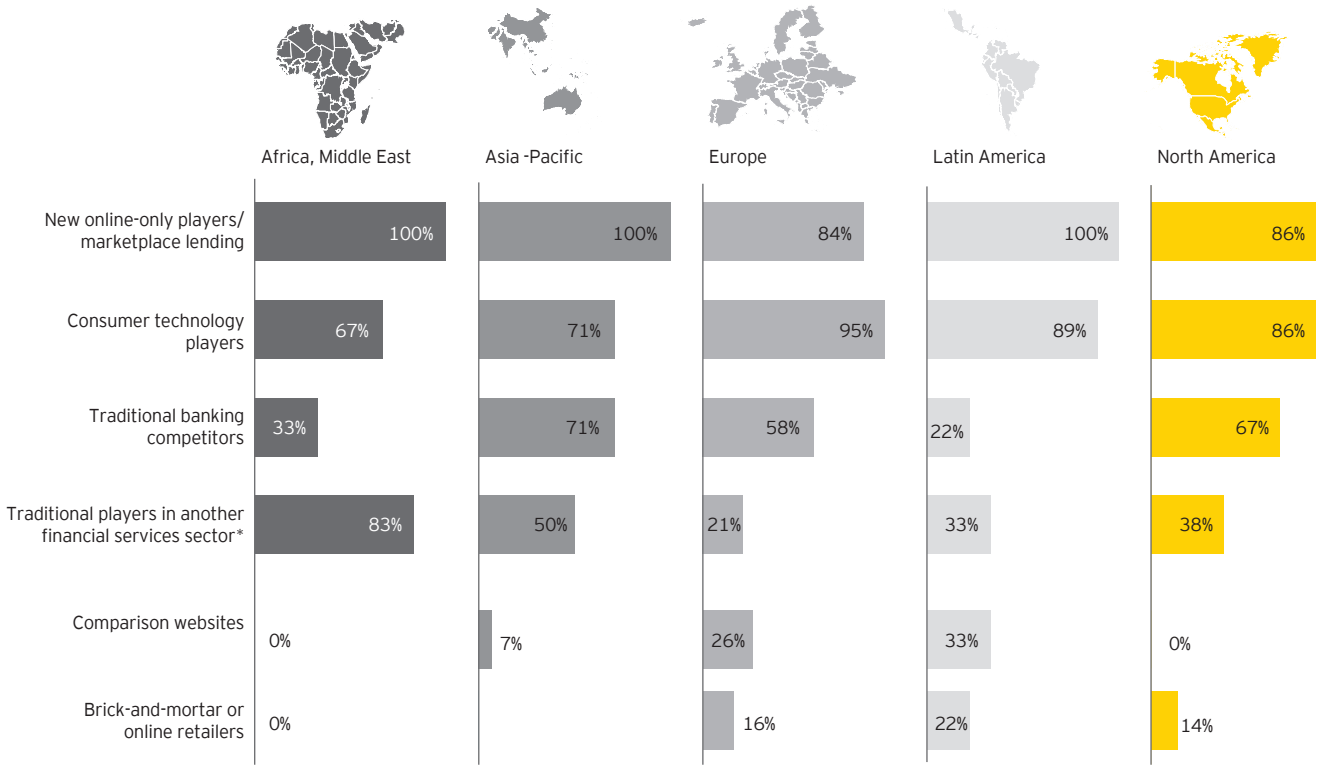
**Represents banks' views on what risks regulators prioritize, not regulators' views*

Enhanced competition

The second-highest emerging risk for banks and regulators is industry disruption due to new technologies. This points to the broader competitive transformation of the industry, with new players — whether small, aggressive challenger banks, FinTech players, or larger, more mature consumer technology companies — starting to make significant inroads into parts of the industry, particularly in areas such as payments and personal and small business lending.[1]

Competition varies by region, as shown in Figure 3, reflecting the makeup of the local financial services industry and the level of dependency on the banking system. However, there is a relatively consistent view on which competitors will be most significant over the next decade. Online-only providers are viewed as the most potent, closely followed by the largest consumer technology companies. As one risk executive put it, "Digital disruption and digital technologies, including FinTechs, are emerging threats strategically — those will affect operational efficiency and carve up the value chain." In some regions, traditional competitors in banking or broader financial services remain significant threats competitively. By contrast, despite ongoing media commentary to the contrary, banks are less concerned about comparison shopping websites and diversified brick-and-mortar or online retailers.

Figure 3: Top competitive threats over the next 10 years



**E.g., insurers moving into banking*

[1] Unleashing the potential of FinTech in banking," EY website.

When considering future competitive dynamics with risk leaders in the industry, CROs cited most concern for large consumer technology companies. Those firms are viewed as having better technology, stronger brands, more interest in leveraging big data to evaluate customer needs and preferences and, above all, a sustained focus on the customer. Many CROs believe those competitors are finding ways to move into the industry without submitting to enterprise-wide regulatory requirements that banks face. For example, technology firms are starting to own customer relationships without having to provide underlying banking products or services. Such firms could "wipe out the industry," speculated one risk executive. Regulators and supervisors are increasingly aware of this potential impact and are focusing not just on the impact of FinTech and technology on banks' business models, but also how best to regulate and supervise these new competitors.

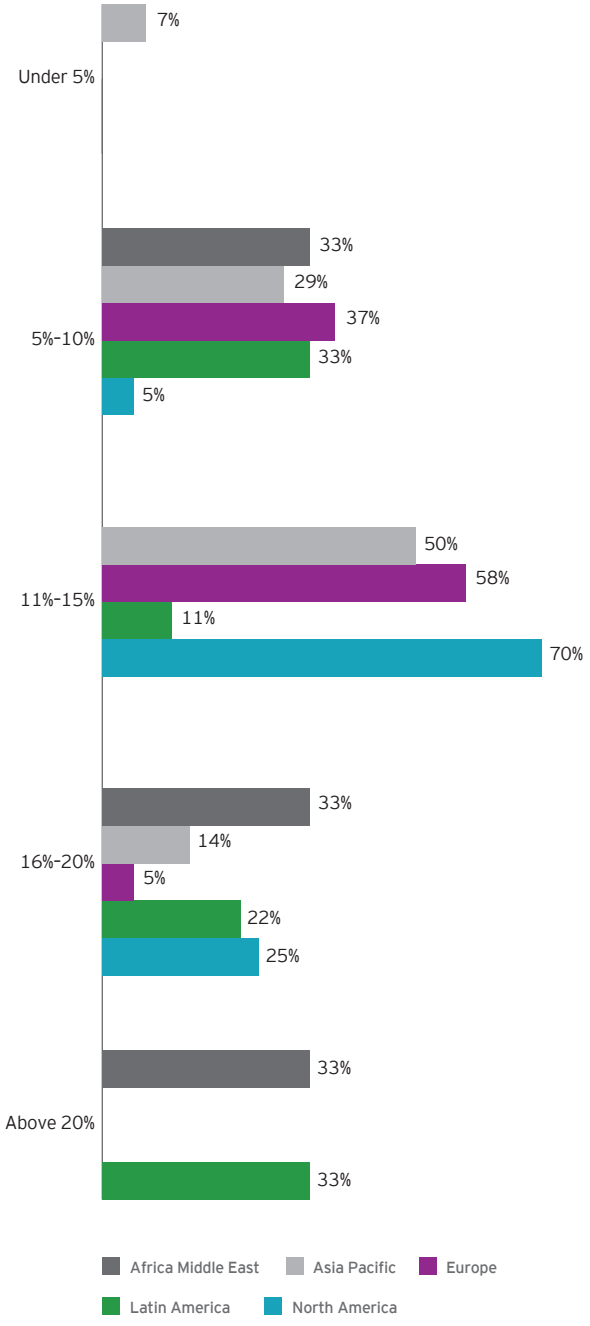
The competitive changes in the industry are likely to be accelerated by moves to open banking to new entrants. Global authorities — and in some countries, regulators — are keen to limit the degree to which barriers to entry inhibit new firms and are pursuing new ways to promote competition. Efforts to accelerate adoption of technologies, such as application programming interface (API), provide the promise of removing key challenges for new firms to compete and for customers to move from institution to institution with ease.[2] Long term, such technologies could radically change the industry. Said one executive, "A 'nightmare scenario' following the introduction of open banking and the rise of the FinTechs would be for core infrastructure to move outside of banking, so that banks only become 'balance sheet providers' — i.e., make loans, but can't earn anything from this activity." Today, such scenarios do not seem as farfetched as they did five years ago.

Narrowing options to meet commitments to shareholders

As was highlighted in the 2016 survey, as banks have slowly moved out of the post-financial doldrums — years characterized in many regions by highly depressed ROEs and serial capital raises — there has been a general industry convergence to 11%-15% ROE targets for the next three years (see Figure 4). That convergence continues this year, although respondents from European banks seem more challenged to commit to such performance compared with their North American counterparts, perhaps due to the sustained low-interest environment that has persisted for longer in the Eurozone than in the US.

[2] Application programming interface (API) is a defined way to allow various applications (of the bank or vendor) to exchange data. It allows developers and companies to create more holistic solutions from a customer perspective by seamlessly incorporating the best of each application or back-office function into a single user experience or interface. APIs hold the promise of delivering better value to customers, creating new revenue opportunities and driving down operating costs, as well as enabling consumers to more easily comparison shop and switch between institutions.

Figure 4: Three-year future ROE targets



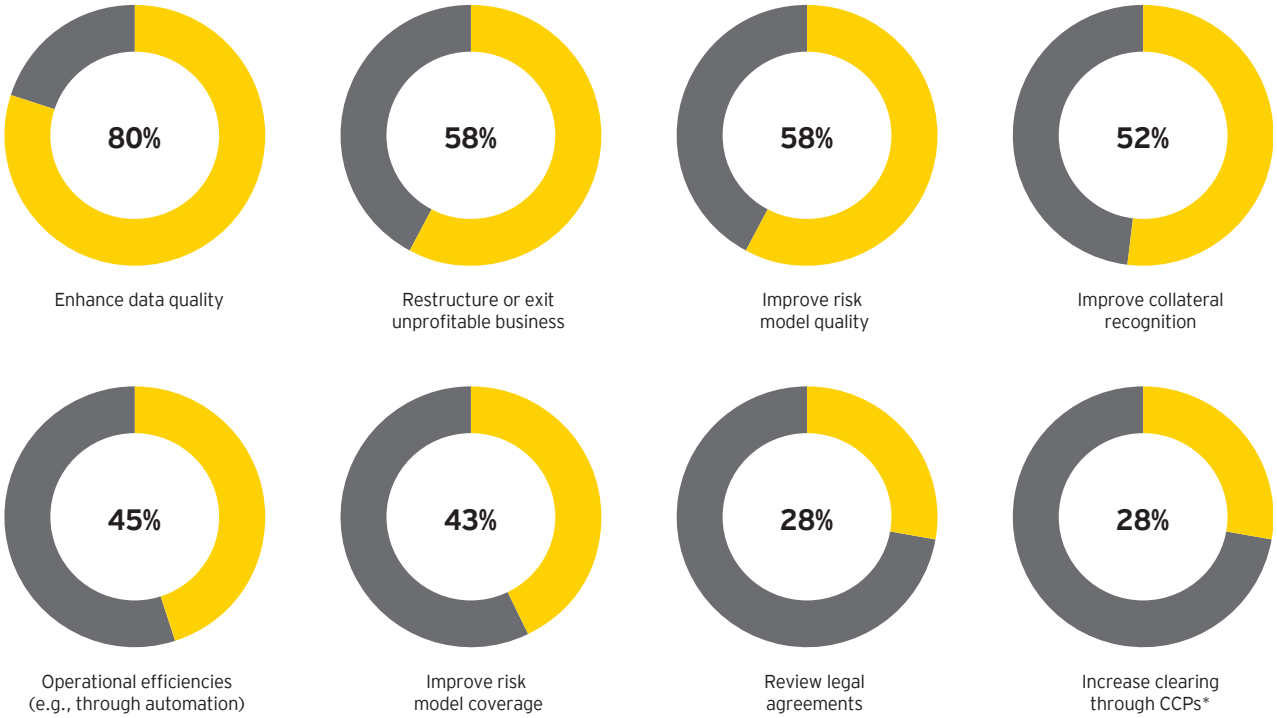
Some emerging market banks, like those in Africa and Latin America, are still seeking higher ROEs than peers in other markets, perhaps reflecting the fact that their regions are still experiencing higher growth and inflation rates and are not yet subject to full global regulatory reform. The interesting question will be whether those banks can sustain such out-performance, over time.

Achieving those commitments to shareholders will be challenging for a number of reasons:

- **The regulatory implementation agenda has a long tail:** the regulatory agenda continues to unfold. Even in countries such as the US, where the pace of new regulation may have slowed, there is a significant tail to implementation. In addition, in some key areas, new requirements are still being rolled out; for example, the long-awaited fundamental review of the trading book (FRTB) (see FRTB: differing stages of progress and material impacts expected, on page 13) and moves to new accounting standards for capital (see IFRS 9/ CECL: accounting change impact on capital and business models, on pages 14-15). Moreover, banks operating in the Eurozone are still feeling the effects of a significantly altered supervisory model, through the creation of the European Banking Union (including the ECB's Single Supervisory Mechanism), and new conduct-related regulations, such as the Markets in Financial Instruments Directive (MiFID II) and Payments Services Directive (PSD2).
- **Strategic options have narrowed:** approximately half (52%) of surveyed banks continue to make business mix adjustments, including asset sales or line-of-business divestitures (45%). Most (75%) are focused on cost management. However, as banks have completed their strategic initiatives in recent years, future options are more limited. For example, after several years of de-risking, fewer firms are exiting lines of business (only 26% compared with 48% last year) or geographies (down to 18% from 27%).
- **Constrained capital flexibility:** the global regulatory agenda has materially decreased the flexibility banks have in managing their capital structure. Regulatory capital buffers (80%), supervisory stress testing (39%) and the ability to raise capital (19%) are viewed by banks as their most significant capital constraints.

Within this context, firms are focused on achieving higher operating efficiency, lower-than-average cost-to-income ratios, and optimizing capital and liquidity. A clear majority of firms continue to be focused on capital optimization and have identified numerous areas where attention is required to achieve their goals. As shown in Figure 5, data quality and integrity is not only the biggest perceived risk, but also provides a real opportunity to drive up ROE.

Figure 5: Opportunities to optimize capital



**Central counterparty clearing house (CCP)*

FRTB: differing stages of progress and material impacts expected

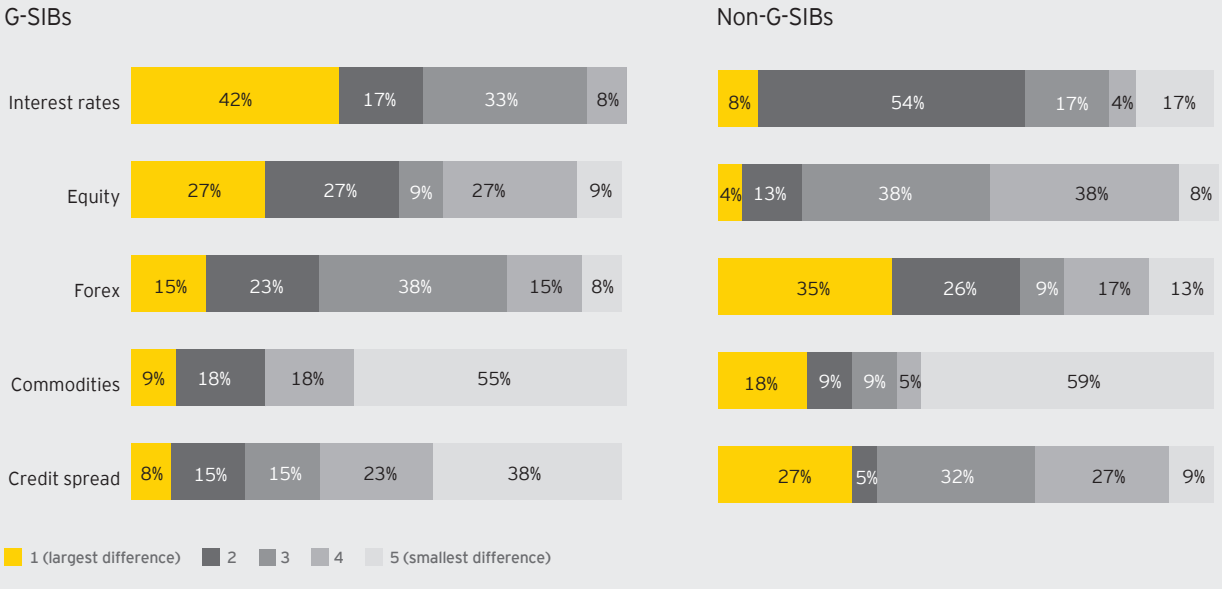
Almost three-quarters (71%) of those surveyed will be subject to FRTB.

Firms are at different states of progress. The EU has published its draft requirements, and European banks are more advanced than others: 82% have mobilized a strategic program compared with 50% of North American banks. Latin American banks are furthest behind, with 50% and 25%, respectively in the pre-mobilization stage or having not started. Some differences may be accounted for by the fact that many local jurisdictions have not yet issued final regulations. For example, in the US there is no draft proposed rule to plan against.

But the work ahead for all banks is significant. When asked to rank progress on a five-point scale, with five representing significant progress, only a small minority reported significant progress on standardized approach implementation (18%), trading book boundary (9%), back testing (7%), profit and loss attribution tests (7%), real price analysis (7%), estimated shortfall measurement (7%), and process and control frameworks (5%). For non-modellable risk factor (NMRF) charge management and default risk charge model, none of the banks reported significant progress.

Notwithstanding the lack of progress, there is broad agreement about the use of the internal models approach (IMA); 86% intend to do so. The estimated differences in capital charges between using the FRTB standardized approach (SA) and IMA are quite different among risk classes between globally systemically important banks (G-SIBs) and non-G-SIBs, which may reflect their differing portfolio compositions and assumptions on model approvals. The charts below show the banks' responses on expected FRTB capital impact on risk classes from most to least impacted. For example, 42% of G-SIB respondents expect the largest difference between FRTB SA and IMA capital charges to be in interest rates.

Respondents ranking of expected differences between FRTB SA and IMA capital charges by risk class



IFRS 9/CECL: accounting change impact on regulatory capital and business models

The banking industry is in the throes of implementing new accounting standards for credit impairment provisioning, which many view as a fundamental shift in accounting globally: International Financial Reporting Standard 9 (IFRS-9) Financial Instruments (generally effective 1 January 2018) and its US counterpart, Current Expected Credit Loss Model (CECL) (generally effective 1 January 2020). While the two standards differ in significant ways, they both require a forward-looking, expected credit loss perspective, which introduces the need for additional methodologies and processes to determine allowances.

While many banks are still working to reliably calculate the impact of adopting these standards, many expect the impact will result in higher provisions and lower capital levels, as well as potential increased volatility in capital ratios at the beginning of a downturn (although, in part, some of this is subject to still-undetermined decisions by the Basel Committee on Banking Supervision and national regulators). The key aspects of the two standards are the incorporation of economic forecasts into loss estimates, determination of asset life and credit deterioration under different scenarios. The standards introduce judgment and complexity into the allowance process, which may lead to volatility in reporting and disclosures, resulting in a need for strong controls and governance across the organization, including at the board level, especially as their full impact on capital — and potentially business models — becomes apparent.

Implementing the standards calls for a significant cross-disciplinary effort, with heavy input from finance, risk and accounting, and likely requires significant enhancements to a bank's data, systems and quantitative models, among other areas.[3] Given that the allowance impacts on financial reporting, there will need to be a focus on controls around the end-to-end process, regardless of the methodological or IT approach taken.

This year's survey shows that there is still significant work ahead for the industry. The results reflect the different implementation dates: all European surveyed banks are, or will, conduct parallel runs in line with the 2018 implementation timeline, whereas 30% of the North America banks have not yet developed plans for parallel runs, given that the implementation date of 2020 is still far out. In practice, CECL banks will have an opportunity to learn from the experiences of IFRS 9 institutions.

The survey results highlight that the banking industry is facing some significant implementation challenges. Over the next several years, banks expect to invest in credit loss model development, enhancement or remediation (91%), model validation (82%), governance and process improvements (65%), technology improvements (62%), data capture (60%), and economic scenario generation development, enhancement or remediation (58%).

However, the critical question is how much will these standards affect banks' business models?

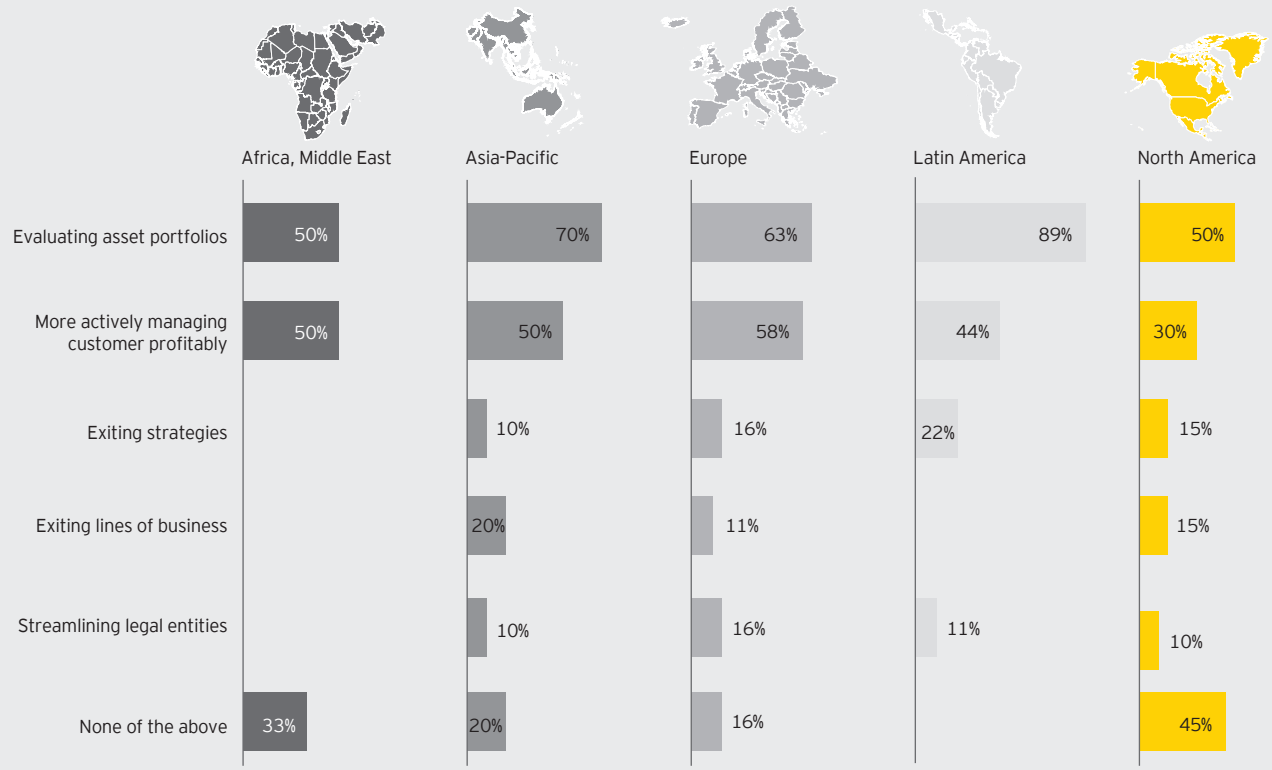
[3] EY IFRS 9 Impairment Banking Survey, EY website.

For those that had estimated the likely increase in credit loss allowance, after implementation, the impact varies materially: less than 10% (31%), 11%-20% (18%), 21%-30% (15%) and 31%-50% (6%). Only a couple reported levels above that. However, over a quarter (27%) still did not have estimates at the time of completing the survey.

Again, the immediacy of the IFRS9 effective date has motivated IFRS banks to conclude that they will have to re-evaluate their asset portfolios and more actively manage customer profitability, in light of the impact of these standards on capital. By contrast, almost half (45%) of the US banks do not yet view this as critical.

Over the next few years, the industry will start to see how these accounting changes influence business models, product design and features, and portfolio distribution. Not surprisingly, the implications for strategy, stress testing processes, capital allocation, and business planning, pricing, and risk appetite are the highest concern for boards.

Expected impact on business model



Lead a digital transformation of risk management

"Almost 80% of our existing processes should be digitized within the next couple of years."

— Chief risk officer

The word *digital* has become ubiquitous. Banks are going digital. Competitors are going digital. FinTech firms are disrupting financial services. Firms are moving to straight-through processing more broadly. New technologies, such as blockchain — or rather distributed ledger — or robotic process automation (RPA) are cited everywhere. Increasingly, customers are talking to chatbots, not sales representatives. Sometimes, it is hard to determine what is real vs. hyperbole.

In practice, there are four dimensions of digital transformation:

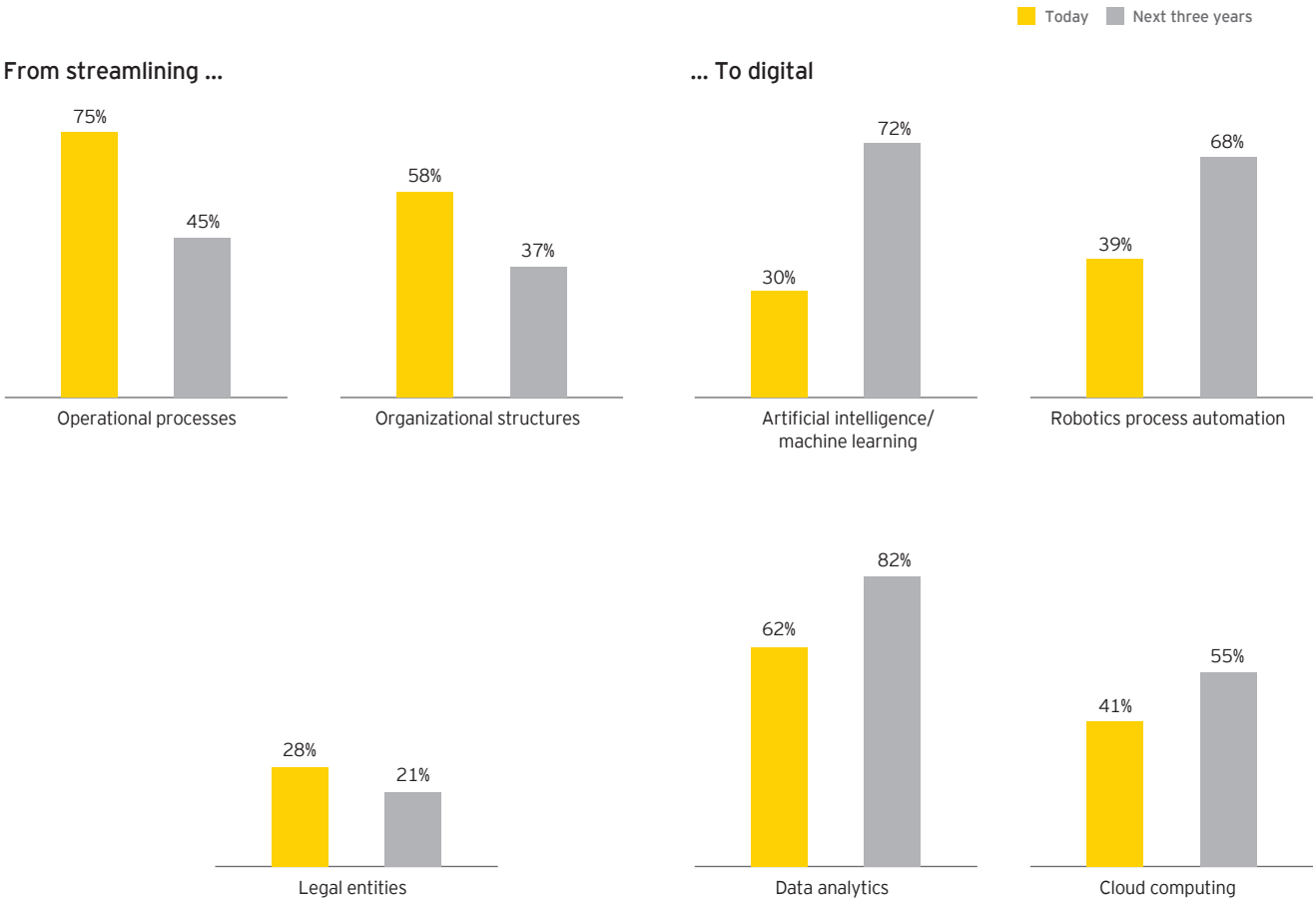
- **Emphasize simplification and automation:** in some ways, the precursor to firmwide digital transformation is the ongoing simplification of organizational and legal entity structures and processes. While some changes have been driven by regulation and cost concerns, they provide a solid foundation on which to build more transformational digital changes, for example, automation.
- **Apply innovative technologies and techniques across firms: digital transformation continues to be focused on the customer interface**. Increasingly, firms are building — or planning to build — technology solutions that fundamentally change the way banks operate in the middle and back office so they can deliver the digital promise to customers speedily and cost-effectively.
- **Consider how digital will drive risk management:** Beyond banks' interactions with customers, risk functions will increasingly have to consider how to change their approach to managing the shift in the firm's risk profile resulting from digital transformation, and being agile enough to enable innovation. Over time, risk functions will have to leverage technology to improve risk management, and become technology innovators, rather than spectators.
- **Overcome implementation challenges:** Notwithstanding the promise of technology to banks and risk functions, important implementation challenges remain for banks to overcome, notably a shortage in talent and cybersecurity concerns.

Emphasize simplification and automation

In the first round of change (as shown in Figure 6), banks are heavily focused on streamlining their operational processes (75%), organizational structures (58%) and legal entities (28%).

A natural extension of this simplification process is automation. Almost two in five banks (39%) are already using RPA and one-third machine learning, in areas such as anti-money laundering (AML) and know-your-customer (KYC), and more than two-thirds expect to do so within three years. New applications of these technologies include credit, market and counterparty risk management. Not only will automation allow banks to reduce costs and make smarter and faster risk decisions, but over time it will reduce error rates and operational risk.

Figure 6: Actions being taken to cut costs



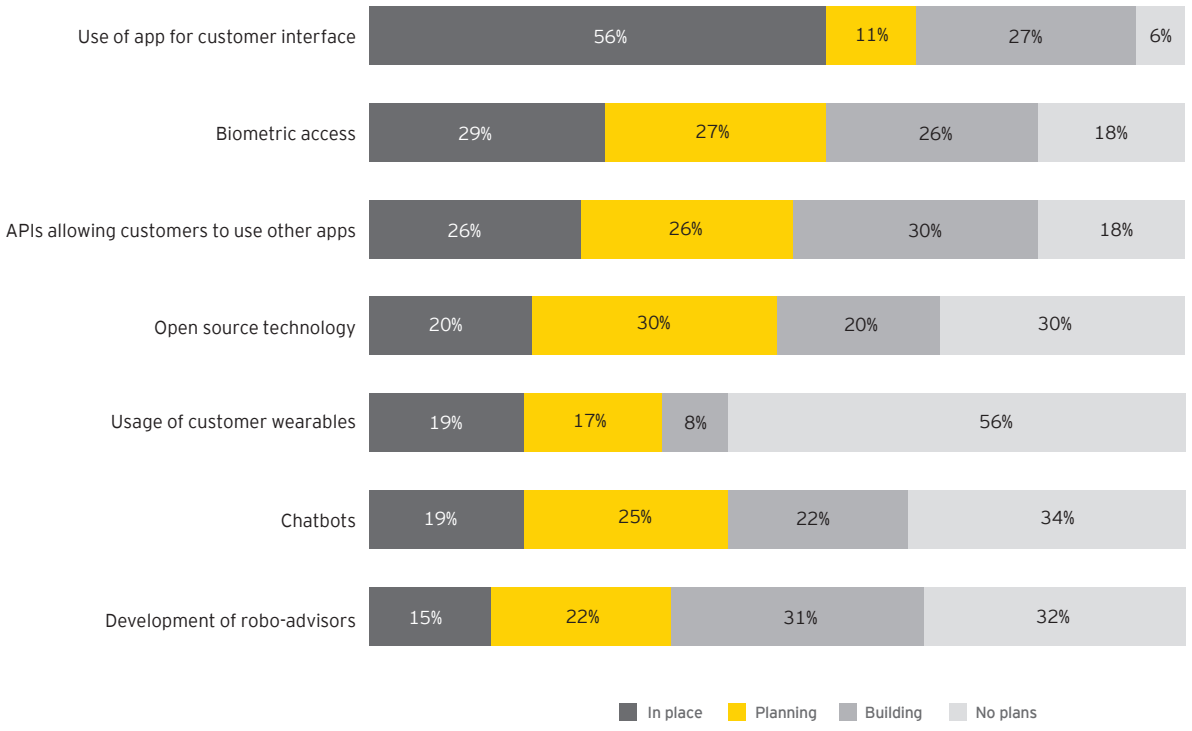
Apply innovative technologies and techniques across the firm[4]

Increasingly, management agendas are switching from simplification to innovation. To date, some of the most visible innovation in the industry is related to how banks use technology to interface with their customers, especially applications, as shown in Figure 7. In addition, banks are building — or planning to build — capabilities to use other technologies, such as biometric access, the use of APIs via apps, and open source technologies. This build-out will take years; fewer than a third of banks have built these types of capabilities, and most do not yet have plans to do so for technologies, such as consumer wearables.

Beyond the use of technologies to enhance the customer interface, in the mid-term, it will be the use of technologies in the middle and back offices, and in second-line risk functions, that will become more significant. A major initial driver may be the opportunity to gain efficiencies and contain costs, as shown in Figure 6, but clearly there is huge potential to improve the quality of risk management, as well.

Banks see the most potential from artificial intelligence (AI) and machine learning to gain efficiencies over the coming years. In some ways, that reflects the maturity of those technologies. CROs highlighted applications such as behavioral pattern recognition in AML, or new ways to measure and predict credit quality.

Figure 7: Use of technologies to interface with customers



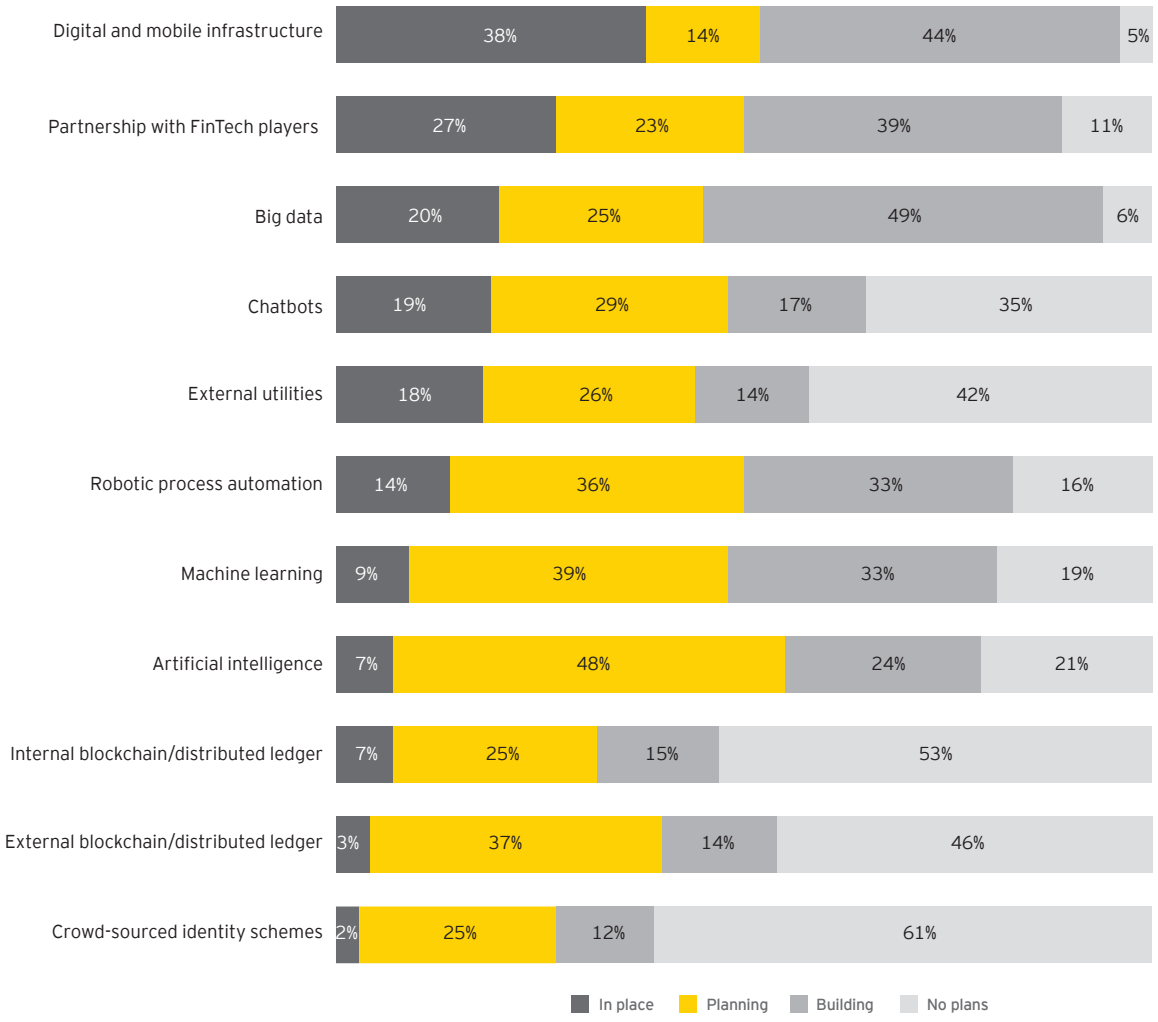
[4] "Financial Services Innovation," EY website.

Cloud computing will also become more important as firms conclude that it provides a safer, cost-effective, and more resilient way to undertake some activities compared with doing them in-house, often on less stable, more expensive, legacy systems. However, banks will need to be transparent with their regulators as they depend more heavily on technologies such as AI and cloud computing, so that regulators can gain comfort that banks are well positioned to use these technologies in a well-controlled manner.

Data analytics remain important. Firms fully appreciate that the ability to gather timely, accurate data and to mine it for insights – whether for customer needs or risk management – will be central to how they compete and survive.

Plans to leverage new technologies to manage costs are in various states of progression, as shown in Figure 8. Digital and mobile infrastructure initiatives are most advanced, followed by partnerships with FinTech players. By contrast, the industry is in the early throes of moving to automation and

Figure 8: Status of initiatives to cut costs



> "We are focused on how best to support the bank's digital transformation."
>
> — European risk executive

machine learning. Many options that require collaboration, notably industry efforts on distributed ledger and crowd-sourced identify schemes, have not been prioritized as high as technologies that are in the banks' own control. However, some of those collaboration technologies have advanced materially in areas such as trade finance and securities clearing.

Consider how digital will drive risk management

Taken together, the accelerating adoption of new techniques and technologies will transform the industry over the next decade. Inevitably, risk management functions will need to evolve as well.

Four major changes will be required:

1. **Manage the shift in risk profiles:** as banks transform their operations and use of new technologies, their risk profiles will change. In some ways, this creates opportunities to reduce risks. For example, replacing legacy systems can improve resiliency, using automation can reduce error rates, and leveraging more data can allow for more proactive, predictive risk management. At the same time, some risks may increase, if only in the short term. Some new technologies are relatively nascent, with few truly tested at an industrial scale in banking. Moreover, more dependence on new technologies brings other risks — for example, with more access points through digital banking, a higher potential adverse impact if automated (vs. human) processes get corrupted, hacked or poorly designed, or dangers associated with machine learning replicating human misbehaviors.

   Risk management executives recognize this challenge. "Digitization and the move to streamline processes should reduce risks, but it also bring risks — it's a balancing act," commented one executive. "The bank's risk profile is changing as a result of more open data, shared data, and open IT platforms," said another. As such, banks will need to seek new ways to evaluate their changing risk profiles as these changes flow through.

2. **Be agile enough to enable innovation:** in terms of digital adoption, risk and compliance functions have critical roles to play.

   Key ways in which risk and compliance can contribute to digital innovation include:

   - Help to identify risks and align strategic efforts with risk tolerance (71%)
   - Offer guidance on laws and regulations that could be interpreted as relevant to new technologies, products or services (49%)
   - Provide review and approval prior to product launch (47%)
   - Deliver critical input into evolving risks for information security and privacy protection (40%)
   - Have a formal role throughout the product development processes, from product initiation to design to development to testing to product launch (37%)
   - Provide initial requirements and final review and approval at product launch (36%)

To operationalize this new role, the operating model for risk management will need to evolve, likely materially, so that risk and control thinking can be incorporated appropriately. This needs to be within the much faster cycle of agile development when compared with a more traditional model for product development. Long term, it is hard to envisage a situation where only one-third of banks' risk management functions have a formal role in the full innovation product development process. Surely, all banks' risk functions will have to be involved, eventually.

3. **Leverage technology to improve risk management:** risk leaders highlighted that new technologies will have an increasingly significant impact on the risk function over the next few years (see Figure 9). They identified a number of risk and compliance processes that could be digitized:

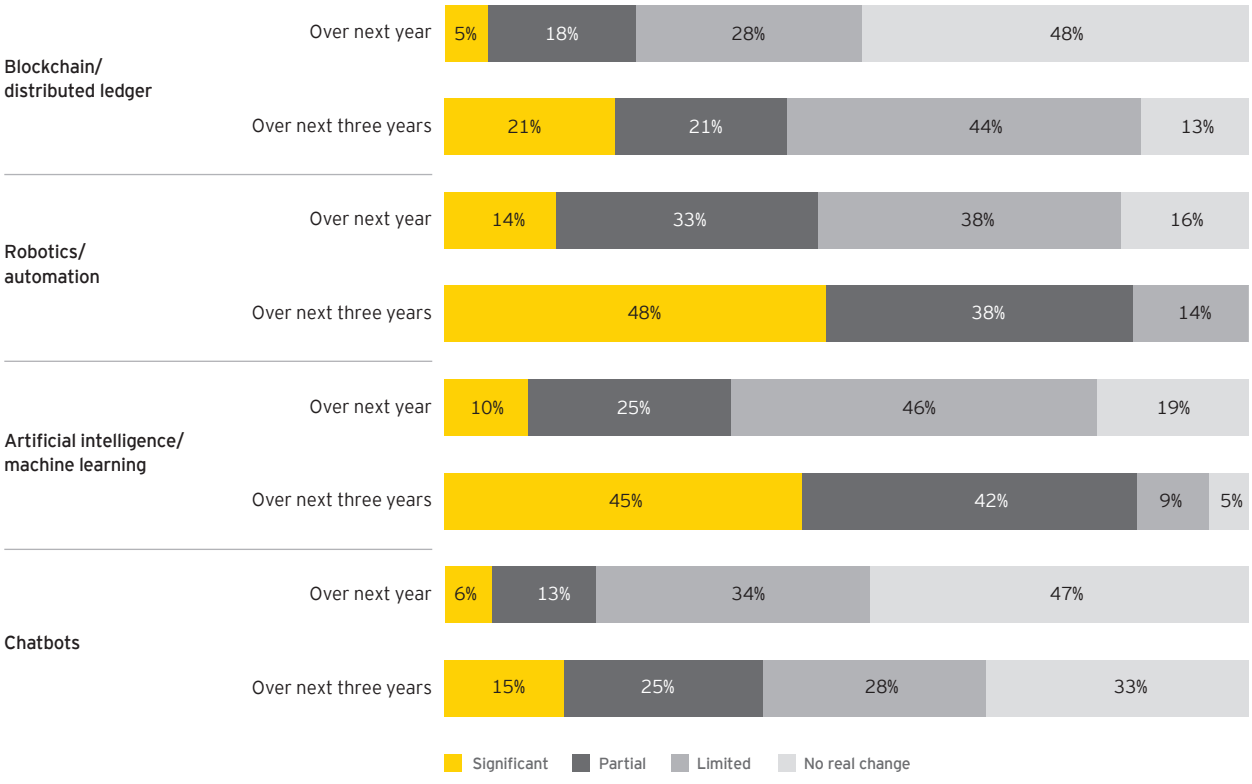
   - Surveillance and monitoring (49%)
   - Sanctions screening (43%)
   - Know-your-customer (32%)
   - Conduct risk analytics (31%)
   - Integrated stress testing capabilities (23%)
   - First- and second-line-of-defense testing (22%)
   - Tracking new regulations to aid change management (22%)

   Banks expect new techniques and technologies will drive down costs in risk management, notably through the use of automation (87%), digitization (64%), machine learning (59%), risk models using AI (57%), straight-through processing (54%) and augmented risk scoring (29%).

   Industry utilities that leverage technologies, such as in KYC, AML or third-party assessments, will also play a role (34%), as will offshoring (23%) and outsourcing (16%).

4. **Become technology innovators:** while many risk functions are cautiously adopting new technologies, others are moving fast. One bank executive highlighted that his "risk function is preparing to test new ideas and proofs of concepts, and is partnering with several companies, including start-ups, to renew its risk analysis approach." Another noted that a third of its risk staff are already in analytics, and are building models with machine learning. That bank's ramp-up of new technologies has been material – last year, there were 7 to 8 proof of concept projects, and this year there are 40. "This is moving at a [fast] pace," concluded that executive.

Figure 9: Impact of technologies on risk function



Overcome implementation challenges

Notwithstanding the positive potential that technology brings, banks are still grappling with the pace at which new techniques and technologies should be implemented across the firm or within risk management.

G-SIBs are somewhat more concerned (41%) about the maturity of the technologies than non-G-SIBs (27%), and appear more uncertain of their buy or build strategy (41% vs. 17%) and the impact of adoption on the firm's resiliency (35% vs. 12%). Scale, though, is their advantage — only 35% of G-SIBs cite cost as a challenge, whereas 58% of non-G-SIBs view this as a major hurdle.

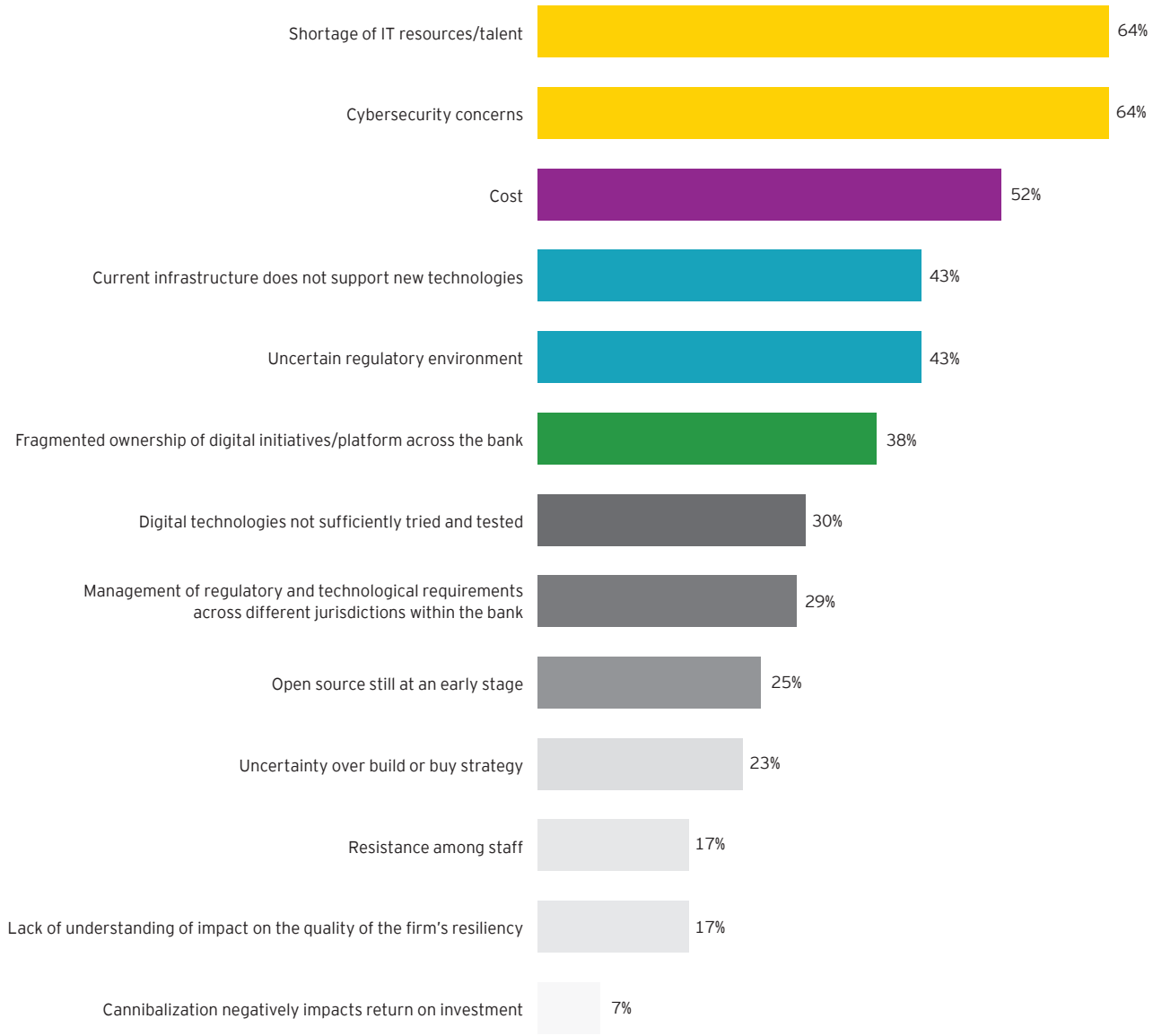
Implementing new technologies is not a simple exercise, and will require banks to convince regulators that new technologies are at least as well controlled as existing approaches. Almost a third of banks highlight that digital systems are not sufficiently tried and tested. Existing infrastructure (43%) and an uncertain regulatory environment for technologies (43%) are real hurdles. Many banks still rely heavily on mainframe computing to run much of their operations, so the pathway to changing core technologies is not an easy one.

The most significant implementation challenges relate to talent and cybersecurity, as shown in Figure 10. On talent, specific — and in some cases, new — skills will be required, including professionals with a mixture of banking operations and controls acumen (70%), agile analysts and product development facilitators ("scrum masters") (59%), and professionals with knowledge in providing digital services (38%) and in increasing customer reach (25%). These skills will have to be complemented with knowledge of how risk is managed, as well. Banks — especially traditional banks — will have to fight hard to attract and retain such talent in light of tough competition from technology companies and FinTech firms.

Cybersecurity concerns are viewed as equally challenging in terms of slowing technology adoption. While, in general, new systems may prove more robust than legacy systems, they also present new challenges, especially in terms of data protection, more open systems, and the potential for processes such as robotics and machine learning to be corrupted by attackers.

In practice, some firms will run ahead of others. Some want to be market leaders, while others want to be what one CRO called "fast followers." In part, any reticence to move quickly relates to the fact that major moves may not occur "before the technology, and the risks associated with it, are properly understood."

Figure 10: Challenges in implementing technologies



Operationalize the three lines of defense

Last year's survey highlighted the industry's widespread acceptance that the overall governance and control model that is needed to underpin risk and compliance was the three lines of defense.

The framework is clear. The first line — notably the business leaders, as well as the support groups, such as technology — is directly accountable for owning, understanding and managing the risks of running their business. The second line — notably risk and compliance — is responsible for aggregate enterprise-wide risks and for independently and effectively challenging the first line's approach to managing risks. The third line — internal audit — provides assurance over the firm's overall risk governance and control environment.

What was also clear last year was that some of the more fundamental shifts — moving significant resources to the first line to support first-line accountability, or building up the second line to properly manage aggregate risks — had, for the most part, been made. Indeed, this year, most (76%) G-SIBs stated they have completed or nearly completed the transformation of their three-lines framework.

However, the industry is finding that the devil is in the detail. Operationalizing the model, and making it effective ***and*** efficient is, if anything, more challenging than designing the broad-brush framework. Four elements stand out:

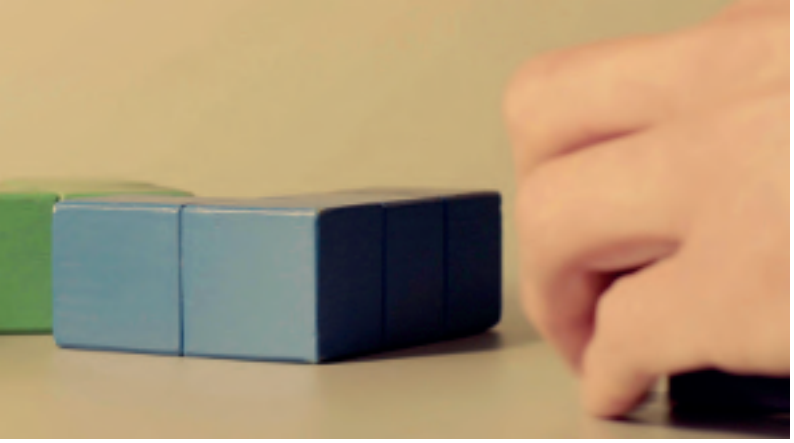
- **Make risk management smarter, faster and more cost-effective:** while the industry is acutely aware of the increased cost of compliance and risk management, it is equally concerned with making risk smarter and faster. Reducing costs cannot undermine the need for strong risk management and controls.
- **Wean off people-dependent risk management:** banks have depended heavily on adding headcount in risk and compliance, and found it hard to cease doing so. Tight regulatory and remediation deadlines meant people-driven solutions were hard to avoid. There are signs, however, that some banks have now found ways to stop — or in a few cases reverse — headcount growth, a recognition that, long term, a highly people-dependent risk model is not sustainable.
- **Develop a new talent strategy:** stalling or reversing headcount growth does not mean talent is less important. If anything, it will be more so, since those that remain must be able operate in a vastly different context than today, one in which risk and technology, not just risk, skills are critical. Long term, banks will have to compete much harder to recruit, retain and motivate talent.
- **Drive standardization:** an important vehicle for weaning off a people-dependent model will be standardization. Banks have made real progress in standardizing risk and control approaches, but have a ways to go to enable technologies, such as eGRC platforms. A major focus is now standardizing, automating and centralizing testing capabilities.

Make risk management smarter, faster and more cost-effective

The industry is focused on making the three-lines model work in a way that is "smarter, faster and cheaper," as one executive put it. Cost is important, but the target operating model banks are aiming for is better for less, not just the same for less.

The primary drivers of changes to the operating model are making the first line accountable for end-to-end financial and non-financial risk (47%, up from 38% last year) and creating fully independent second-line functions (33%, up from 23%). In both cases, a major focus continues to be on managing non-financial risks, such as third-party risk management, cybersecurity, conduct and other operational risks.

The most significant challenges to operationalizing the three-lines model relate to duplication (46%), overcoming past practices (43%) and the need to redesign controls that are no longer fit for purpose as they move to the first, from second, line (41%). Banks still grapple with clearly defining and communicating roles and responsibilities, especially between the first and second lines.



Wean off people-dependent risk management

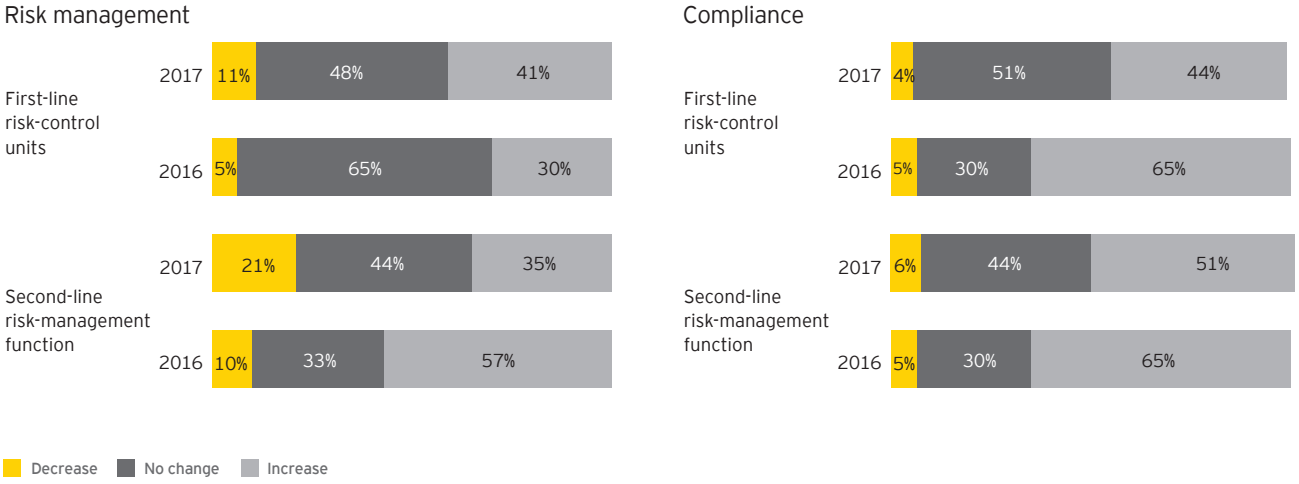
For most of the years following the financial crisis, banks ramped up the headcount in risk and compliance. One bank reported growing to 27,000, post-crisis, from 8,000, pre-crisis, although the number has since declined significantly from the peak. While that example may be extreme growth, every bank has materially increased the number of professionals managing risk.

There are areas where the build-out continues, notably in the second line for cyber risk management, third-party risk management and model risk management. This reflects the recognition by banks that such risks require an independent, second-line perspective, as is expected by supervisors.

However, there were early signs last year that, overall, the tide is turning away from simply adding more headcount. This year's survey suggests that was not an anomaly, although trends are still somewhat unclear. As Figure 11 shows, in risk management more banks have been decreasing headcount over the past 12 months as the risk build-out and remediation work has slowed, but adding more in the first line to support first-line accountability. In compliance, there are signs that headcount is stabilizing.

Banks cite different drivers for headcount changes between risk and compliance. While both are primarily driven by regulatory pressure, banks view increasing risks and added business complexity as the other major reasons to alter risk management headcount. By contrast, banks view headcount changes in compliance to be more related to specific conduct-related events and fines (their own or in the industry) or higher expectations from the board of directors.

Figure 11: Headcount changes over the past 12 months



"New technologies will lead us to a new type of workforce in the second line."

— US risk executive

Develop a new talent strategy

Changes in the talent needs in the risk function will be significant in the coming years. The move to digital and new technologies will mean the talent model will depend more "on data analytics with only a few domain experts to help interpret." Some banks are already seeing this change: "The bank is redeploying traditional risk managers to a very different agenda than what they are used to." Differing skills will be required. The mix of skills and competencies will need to shift. Cognitive skills will become as important as technical risk competencies, as shown in Figure 12. These shifts need to be reflected in banks' overall talent management and succession planning processes.

One executive put the future talent challenge in bold terms, viewing it as one of the primary long-term challenges facing the industry:

> "To make this [digital] transformation, banks need committed people willing to engage in this transformation — willing to respond to or lead this effort. Banks need to both retain and motivate key talent they already have and attract new talent. They have to convince younger people — namely, millennials — that banking is still attractive and a place where they can excel. Key skills banks need are around new technologies, risk analytics, machine learning, AI, and so forth. There is also a need for a significant shift of competencies — with people who can actually use and operate those technologies, while having a sensitivity for risk."

In the end, even with the best technology, banks depend on people. To deliver value to customers. To innovate. To implement, maintain and protect systems and data. To manage risk. To lead. Even if the industry needs fewer people in 10 years — a still debatable outcome — it needs top talent. Banks and the industry at large have to develop a formula to keep banking an attractive long-term career avenue, providing challenging, rewarding and meaningful career opportunities. In many of the most important areas, the war for talent will intensify, especially for professionals connected with technology. The war for leadership talent will remain intense. Banking continues to lose talent to less-regulated parts of the industry. Said one executive, "regulatory fatigue is pushing many to leave the industry and work in non-financial or less financial areas." A new value proposition is required, likely one that ties to the banks' and industry's core purpose and mission — to finance the economy and meet the financial needs of individuals through the long term.[5]

Drive standardization

Over recent years, the industry has been moving toward common enterprise-wide risk and control approaches. These include common risk-and-control assessments, risk identification processes, process-risk-and-control taxonomies, issues management, and standards for effective controls. Overall, many banks stated that the first wave of these changes is substantively complete.

The next challenge will be driving broad-based adoption. Few firms have been able to implement enterprise-wide risk and control approaches fully because the technologies that enable adoption are still being rolled out. Only 7% of banks have fully implemented their eGRC platforms, reflecting the fact banks now realize that common risk taxonomies and control frameworks are actually a precursor to platform implementation. It may also highlight that few, if any, of the currently available eGRC platforms meet banks' needs. A similarly low percentage of banks have fully implemented a common data analytics platform.

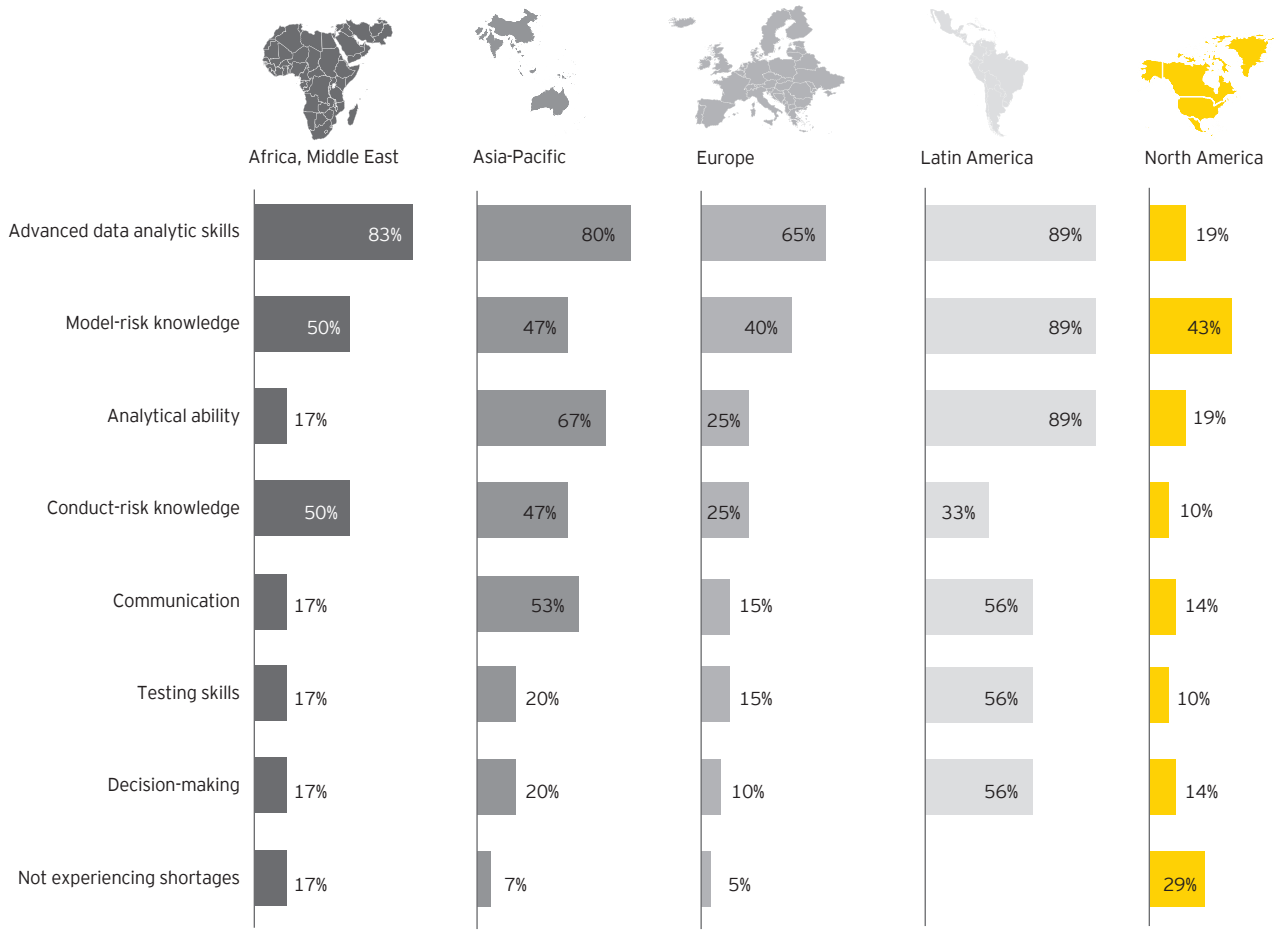
An emerging area of standardization is around controls standards and testing. Banks have started to build centralized testing teams within a number of key areas across the firm:

- Compliance testing (66%)
- Internal audit (52%)
- Operational risk (51%)
- Technology risk (38%)

A small minority (14%) has centralized all first-line testing.

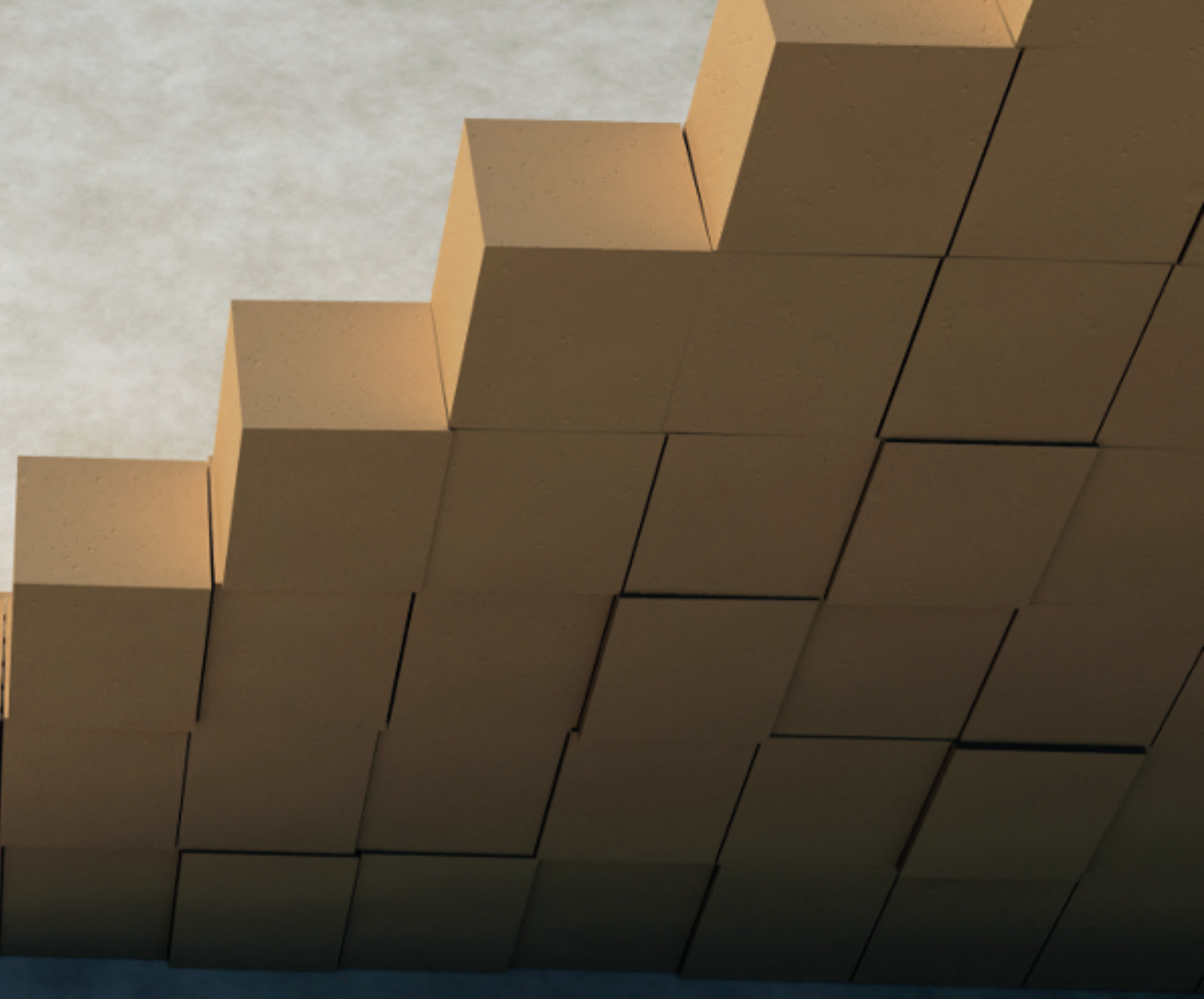
[5] "Transforming talent. The banker of the future," EY website.

Figure 12: Talent shortages in risk and compliance



To date, these teams are still relatively small: 71% and 59% of compliance and risk testing groups, respectively, are below 50 professionals. However, the opportunities to standardize and centralize testing to reduce duplication and improve the quality of testing are significant. Technology will be a driver of change in testing. A majority (61%) of banks are evaluating where automation can be used in testing, and almost a quarter (22%) are piloting such an approach. However, none of the banks surveyed has fully implemented this approach yet.

More than half of the banks are considering or already building centers of excellence for control activity standards and testing. A range of risk capabilities could be housed in such centers, including operational risk control testing (80%), model validation (53%), model inventory management (50%), information-risk control monitoring (47%) and performance monitoring (27%).



Manage non-financial risks, like conduct, cost-effectively

As noted in last year's survey, the industry has developed new ways to manage non-financial risks, such as conduct, compliance, operational and cyber risks. This innovation continues this year:

- **Manage, not simply decrease, conduct risk:** to date, banks have reduced intrinsic conduct risk by de-risking, for example, by simplifying products or withdrawing from certain geographies, markets or customer groups. De-risking can only go so far. In the end, banks need to manage conduct risks. This calls for a breadth of new approaches and a strong focus on managing conduct risk cost-effectively.
- **Continue to focus on culture:** no amount of policy, process and controls can control all behaviors. Culture matters. Banks continue to invest in efforts to shape and strengthen firm culture, and they link employees' behaviors — good and bad — to pay decisions and individuals' annual performance reviews.
- **Leverage risk appetite frameworks to manage non-financial risks:** The industry is still striving to develop new techniques to embed firms' risk appetite firmly in day-to-day decision-making, and to maintain a risk profile within approved appetite levels. The quantification of non-financial risks remains a challenge, especially in terms of properly valuing such risks within the risk appetite context.

Manage, not simply decrease, conduct risk

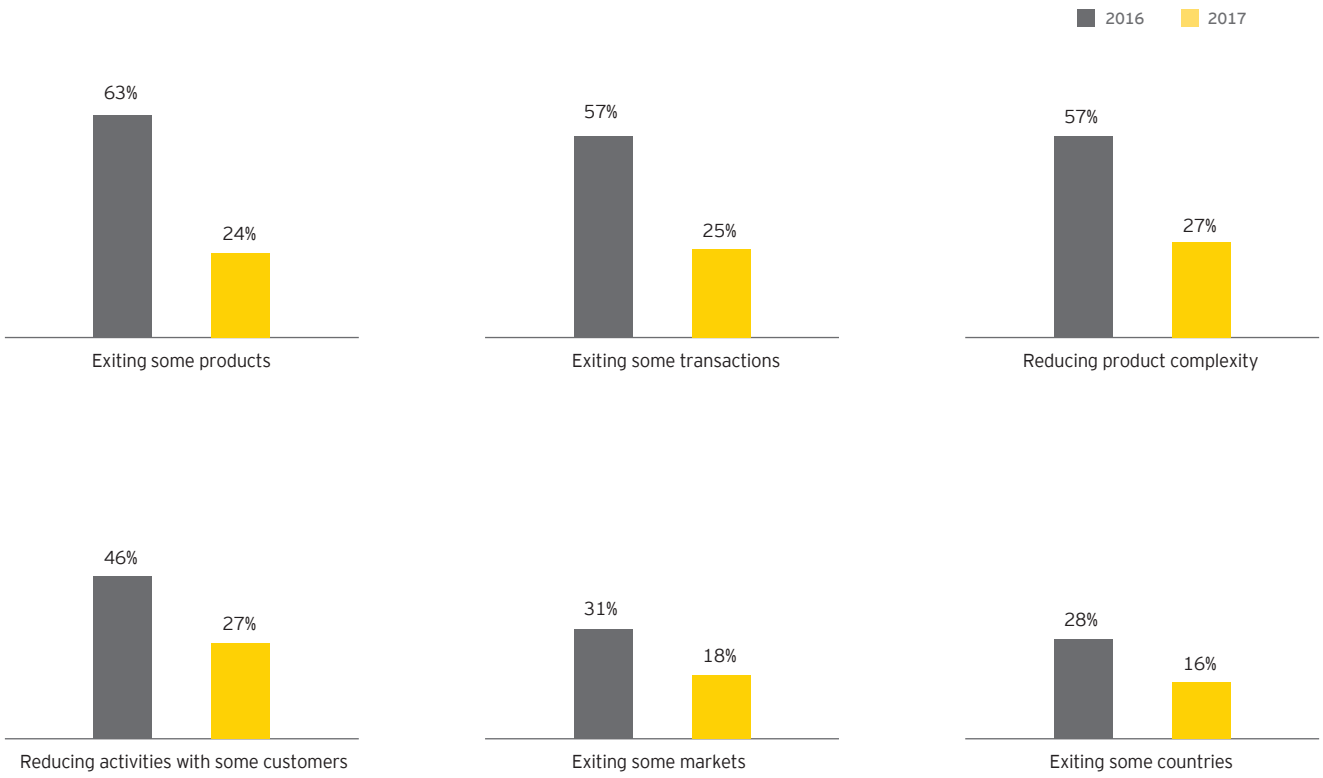
To date, a major strategy for the industry to reduce intrinsic conduct risk has been to de-risk — that is, to withdraw or greatly reduce the banks' services in specific geographies, markets, products or to groups of customers. To some extent, this reflects heightened AML risks and fines, but it also relates to specific products or services that banks perceive carry higher risk from a conduct regulation perspective, such as financial advice.

But banks can only de-risk so far. Indeed, international standard-setting bodies like the Financial Stability Board (FSB) have become increasingly worried that de-risking has gone so far that it is undermining the necessary connectivity in global correspondent banking, where the number of bank-to-bank relationships has been reduced materially in recent years.

Eventually, banks will need to stabilize their strategy in terms of what they deliver to whom and where, and then manage the conduct risk associated with that strategy. Banks are hitting the boundaries of de-risking, as seen in Figure 13. Instances of banks exiting products, transactions, customer segments, markets and countries are significantly lower than last year.

Faced with much more limited options to reduce intrinsic conduct risk, banks continue to implement a broad set of initiatives to actively manage conduct risk. A majority (61%) now have a separate or distinct conduct risk framework. Such frameworks are helping the industry define what constitutes conduct risk, determining where and how this risk arises, firms' appetites for such risk, and how best to measure, monitor and ideally predict this risk. Enhancement opportunities exist across a range of areas, including more effectively managing retail sales practices (74%), money laundering (65%), fiduciary obligations (56%), internal fraud (49%), sanctions (47%) and corruption, e.g., facilitation payments (44%).

Figure 13: Actions to reduce intrinsic conduct risk



The industry is at a relatively early stage in advancing and implementing those frameworks, as shown in Figure 14. G-SIBs are, as expected, more advanced than non-G-SIBs, reflecting the fact that many have experienced higher-profile conduct issues and have paid the bulk of fines and settlements, so have had to invest in enhancing their conduct risk approach.

The accountability for conduct risk falls squarely with the chief compliance officer (52%), reflecting the fact that some of these risks are predominantly associated with being noncompliant with laws or regulations. However, other banks view it more through the risk management lens, with nearly a third viewing the CRO (28%) or head of operational risk (7%) as the executive primarily responsible for conduct risk. It will be interesting to see if or how accountability shifts in the coming years.

Regardless of who owns conduct risk, one of the main challenges, going forward, will be managing conduct risk cost-effectively. After all, conduct risk is often inherent in strategies or business models, difficult to identify, sometimes systemic in nature (i.e., cultural) and difficult to insure against. Yet conduct failures can be highly costly in terms of fines and remediation, and can take years to address fully. With this backdrop, risk leaders are starting to identify ways to manage the cost of controlling conduct risk, as shown in Figure 15.

Figure 14: Maturity of conduct risk management

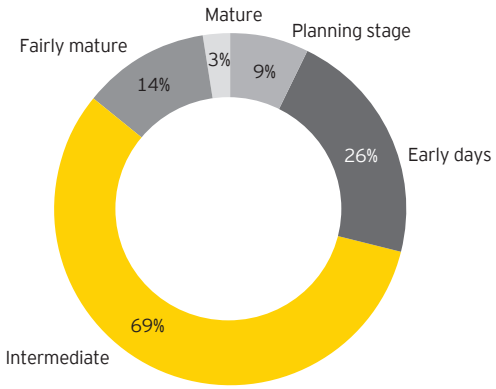


Figure 15: Ways to manage conduct risk cost effectively

Continue to focus on culture

Banks have been working on clearly defining and enhancing their risk culture for the past several years. The primary mechanisms used to improve or solidify their risk culture include enhancing communications and training regarding risk values and expectations (57%), strengthening accountabilities in the three lines of defense (56%), enhancing messages and tone from the top (53%) and embedding risk appetite more consistently across the organization (49%).

The fact that new ways to manage conduct risk are being implemented does not reduce the importance of complementary efforts to align employee behaviors with enhanced board and regulatory risk culture expectations. No amount of process or controls can make up for bad behavior or bad company culture.

Regulators, too, remain focused on culture. Surveyed banks felt that, in their experience, regulators are interested in the board's role in culture (70%), second-line risk's role (64%), the risk appetite framework and its impact on behaviors and decision-making (53%), first-line management accountability (50%), and measurement of culture and behavior (50%).

Work still remains to be done. Only a minority of banks believe they have achieved their target state culture, although more (29%) North American banks believe they have done so compared with banks in other regions (Europe and Asia-Pacific, 20%; Latin America 11%; and Africa and Middle East, 0%).

One area of continued focus is on aligning behavior and compensation. In the years immediately following the financial crisis, the industry made significant changes to the structure of compensation, particularly for executives. Deferrals and performance-based clawbacks have become commonplace and pushed down deeper into the organization.

The emphasis in recent years has been on embedding cultural – or non-financial – factors into compensation decisions and annual individual performance assessments. A clear majority (79%) now adjust pay downward for non-financial factors and tie bonus decisions to non-financial, as well as financial, metrics (74%). Factors considered include:

- Culture and behaviors (90%)
- Risk (83%)
- Internal audit findings (70%)
- Regulatory or supervisory findings (67%)
- Controls (60%)

Organizations continue to incorporate risk-balancing features into incentive compensation programs for employees beyond the executive level. The challenge remains how to incorporate these factors fairly, systematically and consistently across the firm, without adverse effects (e.g., reductions in one group's bonus pool or an individual's bonuses do not lead to unwarranted increases in other areas or to other individuals). Refinements to methodologies will continue in the years to come.

Leverage risk appetite frameworks to manage non-financial risks

While most (85%) banks state that they quantify non-financial risks, in general, the industry is still in the early stages of developing ways of doing so effectively, efficiently, meaningfully and consistently.

The focal point has been the continued implementation of firms' risk appetite frameworks. Those frameworks were a relatively new innovation for many banks post-crisis and have since become the framework within which the board and senior management can approve their appetite across an array of risks and monitor the firm's adherence to those parameters.

The remaining challenges are ones the industry has grappled with for the past few years, including:

- Expressing risk appetite for different types of risks (66%)
- Cascading appetite down into the operations (62%)
- Using the risk appetite framework as a dynamic tool to manage risk (52%)
- Linking appetite to strategy (48%)
- Effectively relating risk appetite to risk culture and behaviors (42%)
- Determining the right quantitative metrics (35%)

For the most part, although generally G-SIBs are much more advanced, G-SIBs and non-G-SIBs face similar challenges. The one major exception is linking appetite to strategy, with more G-SIBs (65%) finding it more difficult than non-G-SIBs (43%). Likely, this reflects the fact G-SIBs have more complex businesses, operating models and products.

Figure 16: Approach to using extreme loss estimates or stress as key metric

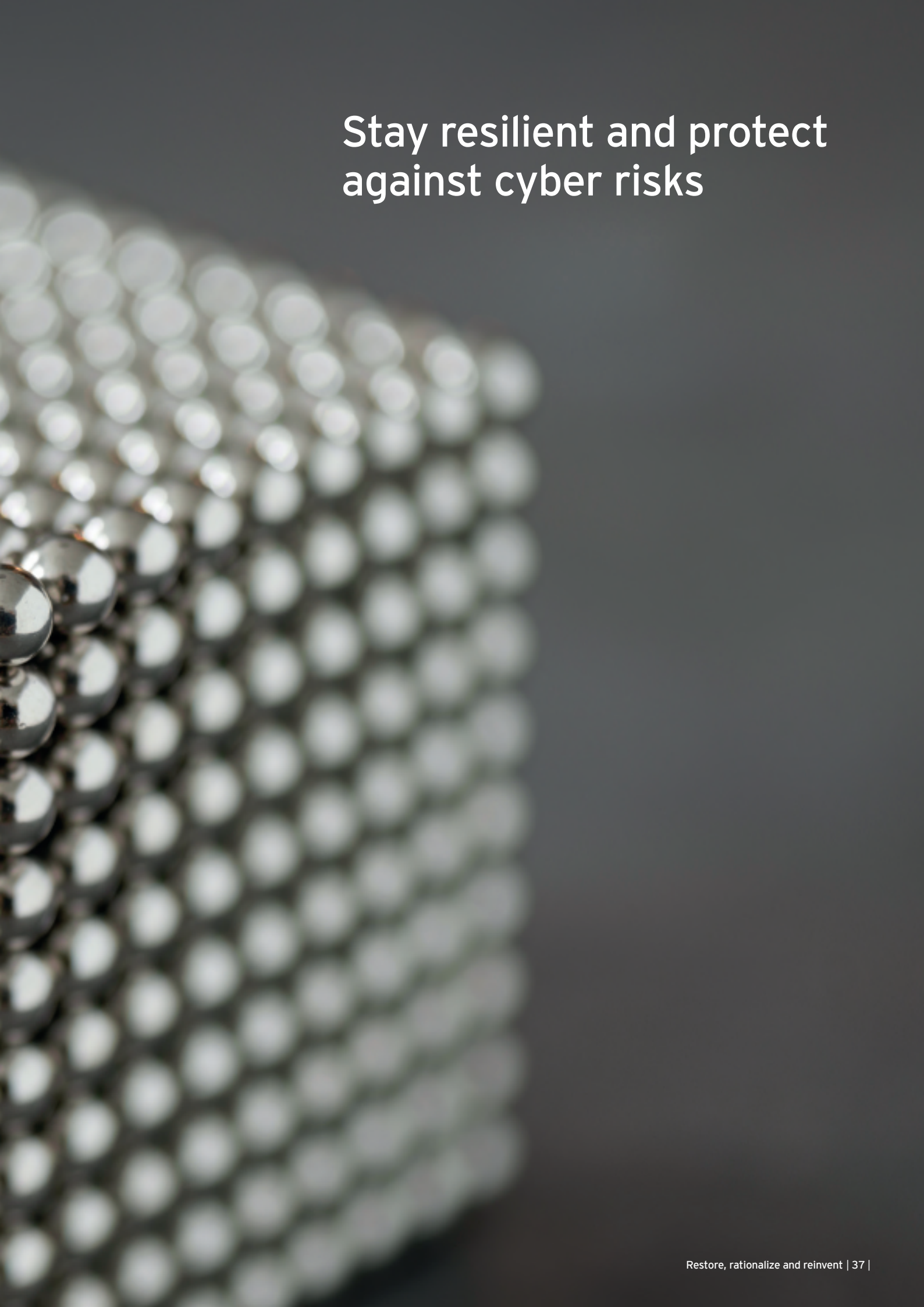
Much of the industry's progress in implementing the frameworks has been at the top of the house. A broad and relatively consistent set of metrics has been adopted across the industry to define the primary boundaries for risk or to monitor the firm's risk profile. Recent innovations have focused on embedding extreme loss estimates into risk appetite frameworks, as shown in Figure 16.

Addressing non-financial risks within the risk appetite framework remains challenging. Banks highlight a set of non-financial risks that remain difficult to quantify, notably reputational risk (71%), conduct risk (53%), strategic risk (42%) and cyber risk (36%). They are deploying a number of techniques to quantify such risks, including scenario analysis (62%), scorecards that are not modeled (45%) and modeled approaches (40%). Very few (9%) use regression analyses.

With regard to tracking actual levels of non-financial risks with the approved appetite for such risks, a range of techniques is now used:

- Tracking of a list of specific metrics against thresholds or for trends that suggest increasing risk levels (76%)
- Regular assessment and reporting by key subject-matter experts, including independent risk (63%)
- Internal and/or external incident capture and post-mortem analysis (61%)
- Risk profiles that reflect inherent risk changes and changes in the control environment (45%)
- Use of analytics to identify outlier behaviors and potential shifts in culture or subcultures (13%)

Stay resilient and protect against cyber risks



"Resiliency relates to being organizationally resilient, in the broadest sense."

—North American CRO

Ten years from the financial crisis, banks are grappling with three distinct challenges in delivering services to customers and markets:

- **Focus on operational resiliency:** for much of the past decade, the resiliency focus has been on going- or gone-concern situations, which was appropriate given the depth of regulatory issues coming out of the financial crisis. However, bank executives and regulators are increasingly focused on business-as-usual (BAU) operational and technological resiliency: not what happens in extreme circumstances, but what happens day to day. As banks consider what enhancements are required to deliver firmwide BAU resiliency, they recognize some fundamental changes are required across the three lines of defense, coupled with a stronger focus on critical processes and systems.
- **Emphasize cyber resiliency:** daily news of cyber attacks on banks and global ransomware attacks across industries has pushed cyber risks to the top of board and CRO agendas. In implementing a three-lines-of-defense approach to cyber risk management, banks face growing talent issues. Boards are challenged to oversee cyber risks, in part because of ongoing limitations to cyber risk reporting.
- **Actively manage critical vendors:** within the context of operational and cyber resiliency, the industry and its regulators are focused heavily on banks' abilities to identify and manage vendors critical to the ongoing delivery of key services to customers and markets. Banks continue to struggle in this regard, but know they need to greatly improve their capabilities within the context of a continued evolution of third-party risk management.

Each presents distinct, although overlapping, challenges.

Focus on operational resiliency: staying resilient day to day

Until recently, the primary regulatory focus has been on financial resiliency (via capital, liquidity and leverage regulation) and operational resiliency in extreme — going (recovery) and gone (resolution) — scenarios (via the development of recovery and resolution plans (RRPs)). The industry continues to develop strategies to accommodate recovery or orderly resolution in extreme scenarios. For some of the largest banks, the work involved, including simplifying legal structures and operations, will take years to complete.

However, well-publicized technology outages at major financial services firms over the past few years are making the industry rethink day-to-day operational resiliency.

Post-9/11, there was a major focus in the industry — globally, not just in the US — on enhancing traditional resiliency programs. Regulators pushed for enhancing planning and capabilities. This included business continuity (BC), crisis management (CM) and disaster recovery (DR). Significant strides were made, such that the industry, overall, views its core plans and policies as fairly mature (57%) or mature (26%).

But, after making investments in response to regulators' pushing for stronger DR capabilities, executives are now asking "what about BAU resiliency?" as one executive put it. Addressing this issue calls for different thinking. Resiliency has to be viewed from an enterprise, rather than technical, perspective.

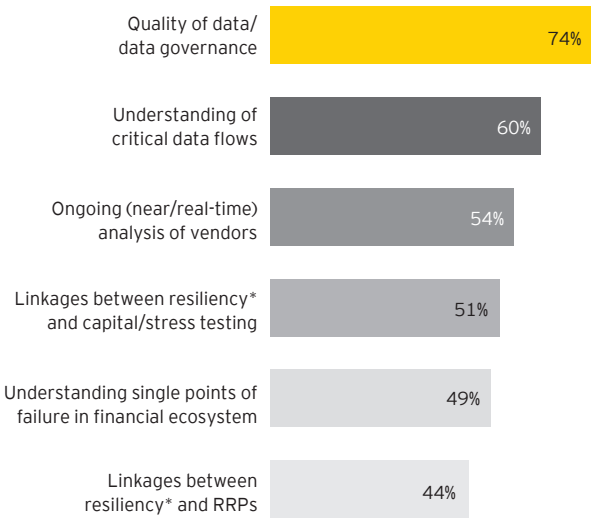
From this broader perspective, core competencies, such as BC, CM and DR, remain critical. Those plans and processes need to be robust, well-tested, well-communicated and adaptable. Moreover, continued enhancements in those areas are central to broader efforts to improve resiliency. For example, in a world of cloud technologies and advanced storage capabilities, firms will need to review their data center and DR strategies and may need to make changes in the next few years that are at least as noteworthy as those made over the past decade.

The more significant work, however, relates to a broader set of areas that need enhancing to materially advance the quality of banks' day-to-day operational resiliency. As shown in Figure 17, foundational elements, such as data quality and governance, mapping critical process flows, as well as stronger connections with other core disciplines, such as third-party risk management and links to stress testing, are even more important. Taken in this broader sense, maturity is likely much less advanced, because the bar keeps rising. As one executive admitted, "what we find is that, across the range of interrelated issues, we are quite mature in some areas and at a very early stage in others."

As the expectations for enhanced operational resiliency and the need to integrate resiliency across the enterprise grow, there is a clear move to broaden ownership and oversight of resiliency. Second-line risk management is taking a much more prominent role, partnering with first-line operations and IT, as well as other enterprise-wide functions. Often, accountabilities are shared across the first and second lines for business continuity, crisis management and overall resiliency, although the second line clearly plays a primary role for the overall program (54%) and crisis management (55%). DR, by contrast, remains squarely in first-line IT (78%).

The ascendency of the risk function in the resiliency domain reflects the fact that, in the end, a risk-based, enterprise-wide view is needed to prioritize where firms focus their attention and investments. Not everything can have high availability, fast recovery times and the best cyber protections. Prioritization is important. Getting a top-down, holistic view of the critical processes — from customer, business, regulatory and risk perspectives — is important, so that those processes (and the applications, infrastructure, people and vendors that support them) can receive differential investment and attention. The industry has a long way to go in this regard.

Figure 17: Areas to enhance to have a robust firmwide resiliency program



**For those options, resiliency relates to business continuity plans, crisis management and disaster recovery.*

Emphasize cyber resiliency

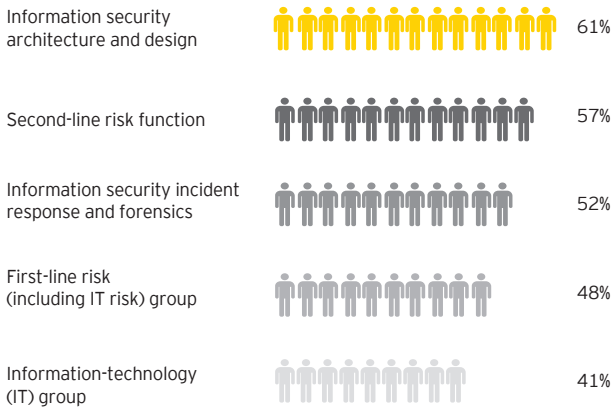
Cyber risk is now the No. 1 risk for CROs and boards, reflecting the prominence of global ransomware attacks and an overall heightened level of cyber attacks on the industry.[6]

As highlighted in last year's survey, the industry is moving quickly toward adopting a three-line approach to cyber risk management.[7] As it does so, more of the organization is now centered on cybersecurity. Many functions increased their focus on this risk in the past year: second-line risk (79%), information technology (74%), first-line risk (73%), data management and governance (68%), internal audit (57%) and first-line business management (49%). In turn, this is creating a range of talent shortages, as shown in Figure 18.

The second-line risk focus is significant. Said one CRO, "It is important that risk management engages to create a common sense view of cyber. Not just a technology perspective. Risk management has to think about risk appetite, understand the issues and help to educate others" on the enterprise risk dimension of cybersecurity.

Boards have stepped up their role in overseeing cyber risk management,[8] with the majority now routinely reviewing cyber risk metrics (61%), meeting with the chief information security officer (59%), reviewing internal audit's efforts on cyber (56%), reviewing the cyber risk management framework (56%) and meeting with the CRO on cyber matters (50%). Even though boards are receiving more training and updates on cyber risks, they remain challenged in staying current with the threat environment, knowing the critical vendors, and understanding how technology or other investments reduce cyber risk.

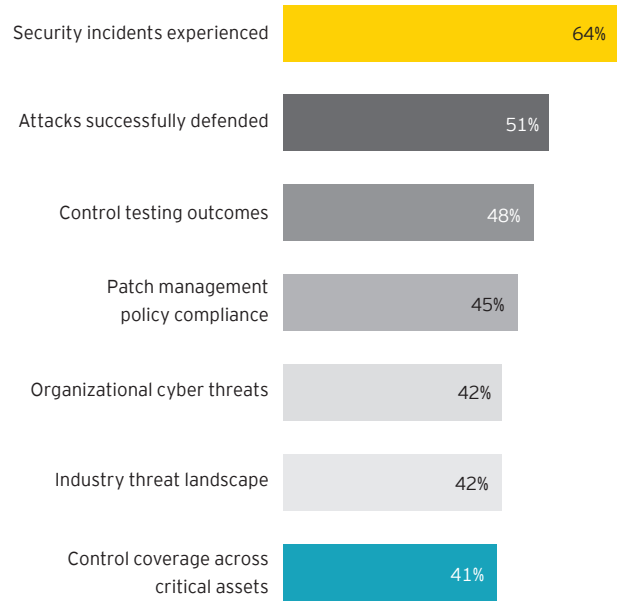
Figure 18: Expected talent gaps in cyber in next two years



[6] *Cyber resiliency: evidencing a well-thought-out-strategy*, EYGM Limited, 2017.
[7] "Cyber risk management across the lines of defense," EY website.
[8] *Governing cyber risk in financial services*, EYGM Limited, 2017.

Cyber risk metrics and reporting remain an overall challenge for boards and management, as well as for regulators. As shown in Figure 19, too often the metrics used are key performance metrics, not key risk indicators, and few, if any, are developed by the second line in the way that is consistent with the overall risk appetite metrics. This limits banks' abilities to understand actual enterprise-wide exposures to cyber risks.

Figure 19: Cyber metrics used in risk appetite statements



In some ways, cyber metrics inadequacies mimic broader challenges in quantifying non-financial risks. A good example is loss data. As one executive put it, "Our loss numbers focus on actual losses, rather than capturing, in addition, reputational damage or lost revenue." That is true for cyber attacks as well. Loss data typically relates to just the cost of recovery, rather than the overall cost to the firm.

Actively manage critical vendors

Third-party vendor management has been going through an accelerated evolution in recent years. In some ways, this can be characterized as going from simply procurement (sourcing, pricing and contracting), to vendor management (evaluating and managing), to vendor risk management (managing enterprise-wide vendor risk). The latter evolution has increasingly pushed framework development and overall monitoring to second-line risk, as noted in Figure 20, while the bulk of day-to-day vendor management has appropriately stayed with first-line vendor owners and procurement.

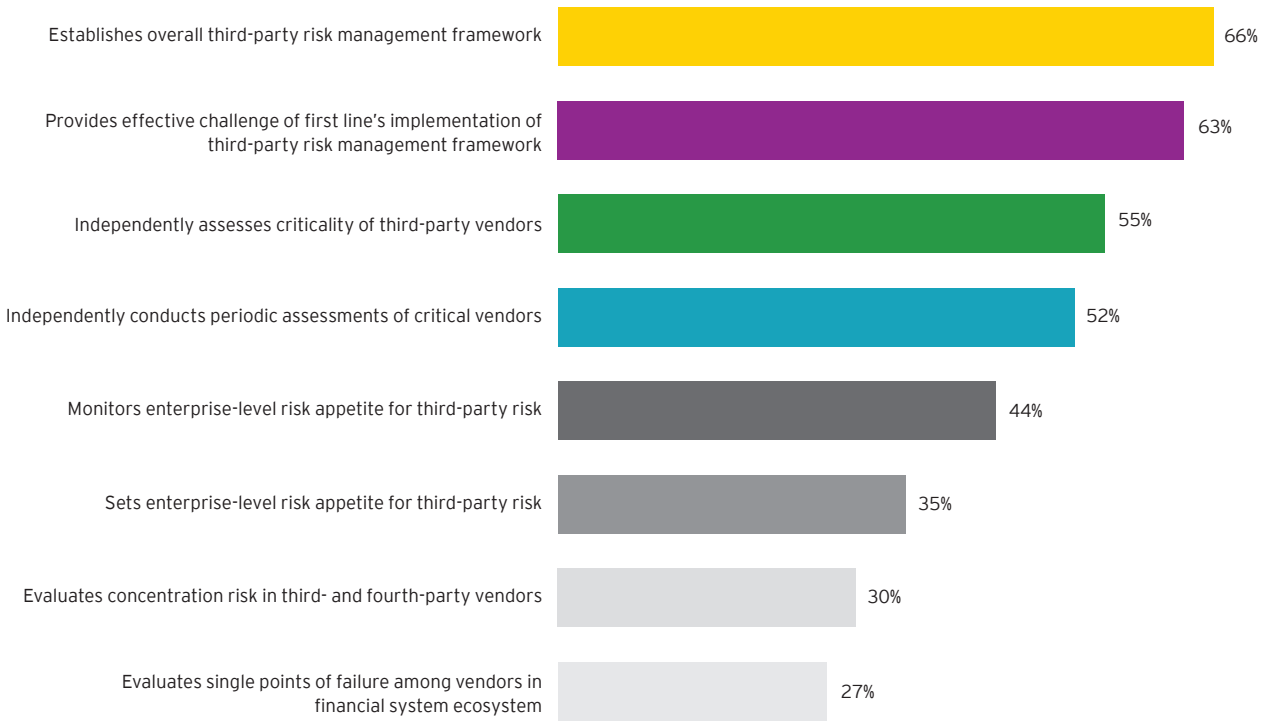
The most recent evolution has been toward a more significant focus on critical vendors. Initially, this focus came out of strategic sourcing analyses, where firms wanted to identify their most critical third-party providers to ensure the quality of service was optimal, as was pricing. More recently, the development of RRPs required the identification of vendors critical to the continued delivery of core operations in extreme scenarios. Lately, the focus has been on critical vendors and other dependencies in the financial ecosystem from an ongoing operational BAU resiliency perspective. "The bigger issue is with fourth and fifth parties, for which the bank is responsible, but over which it has very little control," highlighted a risk executive.

Banks predict the increased focus on critical vendors will have some significant long-term effects, including:

- Banks will need to build out first-line capabilities (67%).
- More industry-level collaboration will be needed on threat intelligence information-sharing (53%).
- Regulators will need to enhance their ability to conduct vendor assessments (51%).
- Banks will need to build out second-line capabilities (50%).
- Industry-wide disclosure standards will need to be developed (47%).
- Industry-wide utilities will need to be established to conduct assessments on behalf of multiple banks (46%).
- Banks will need more frequent attestation reporting or self-certifications by third parties (40%).
- There will be consolidation among vendors, e.g., in infrastructure or cloud computing (37%).

The extent to which these trends impact the industry will vary regionally. For example, industry utilities will likely develop faster in Europe and North America, reflecting the maturity and scale of the industry in those regions.

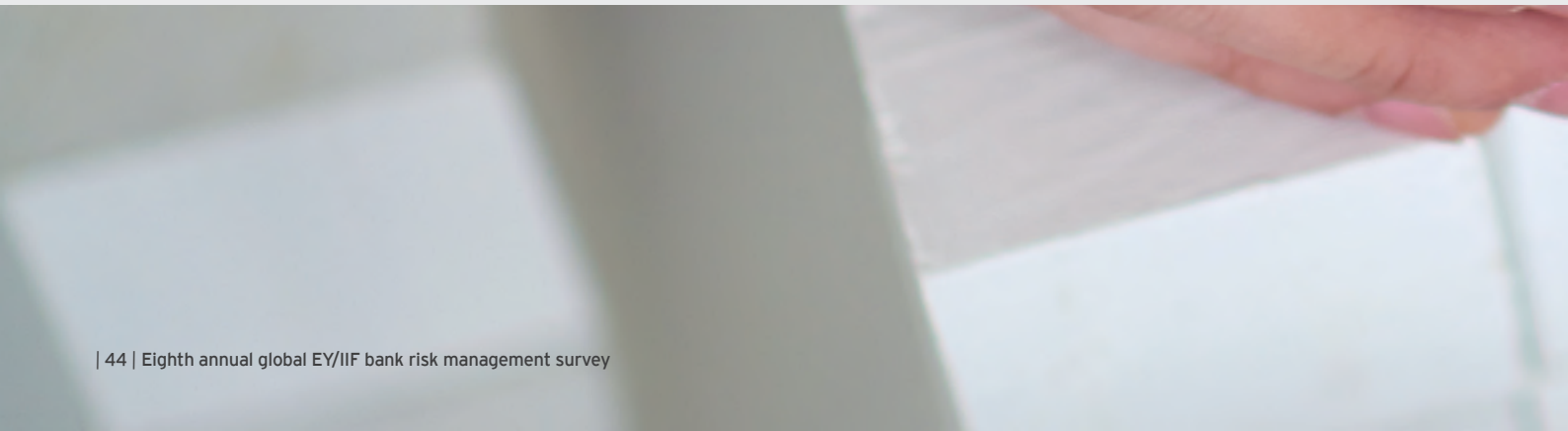
Figure 20: Second-line role in vendor management



Research methodology and demographics

EY surveyed IIF member firms and other top banks in each region, in conjunction with the IIF, from May 2017 through August 2017. Participating banks' CROs or other senior risk executives were interviewed by EY or completed an online survey, or both. In total, 77 firms across 35 countries participated, up from 67 firms in 29 countries in 2016. The charts in this report display data for banks that completed the quantitative 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 20 G-SIBs that participated. Of the others, 40 are domestic SIFIs. Participating firms represented a range of asset size (as of 31 December 2016) from 7% having $2t or more to 24% having $100b or less; the largest percentage (35%) was $100b-$499b. Most (82%) of the institutions operated in 4 or more countries, with 18% operating in more than 50 countries. Many (44%) viewed their institutions primarily as a universal bank, with 42% viewing their institutions as a primary retail and commercial bank and 6% primarily as an investment bank.



Africa/Middle East	Asia-Pacific	Europe	Latin America	North America
Al Rajhi Bank	Agricultural Bank of China*	BBVA	Banco BICE	Bank of Montreal Group
Arab Bank	Bank of Queensland	BNP Paribas*	Banco Bradesco	Bank of Nova Scotia (Scotiabank)
Arab Banking Corporation B.S.C.	Bank of the Philippine Islands	Commerzbank AG	Banco de Crédito del Perú	BB&T
DiscoveryPurple	Hang Seng Bank	Credit Agricole*	Banco de la Nación Argentina	Charles Schwab
FirstRand Bank	ICBC*	Credit Suisse Group AG*	Banco do Brasil	CIBC
Standard Bank Group	ICICI	Danske Bank Group	Banco General	Citizens Bank
	Macquarie	Deutsche Bank AG*	Banco GyT Continental	Comerica
	Maybank	DNB	Banco Nacional de Costa Rica	Desjardins
	Mitsubishi UFJ Financial Group*	Erste Group Bank AG	Itau Unibanco	Discover Financial Services
	Mizuho Financial Group*	HSBC Bank Plc*	Mercantil Servicios	Fifth Third Bank
	National Australia Bank	Intesa Sanpaolo		Goldman Sachs*
	Nomura Holdings International	KBC Bank N.V.		Huntington Bancshares
	The Norinchukin Bank	Lloyds Bank		JPMorgan Chase*
	Sumitomo Mitsui Banking Corp*	Nationwide Building Society		M&T Bank
	Suncorp	Nordea Bank AB*		Morgan Stanley*
		Piraeus Bank		National Bank of Canada
		Raiffeisen Bank International AG		Northern Trust
		Royal Bank of Scotland (RBS)*		PNC
		Skandinaviska Enskilda Banken AB (SEB)		Royal Bank of Canada (RBC)
		Société Générale SA*		State Street Corporation*
		Standard Chartered PLC*		Synchrony Financial
		Swedbank AB		U.S. Bancorp
		UBS AG*		
		UniCredit Group*		

*Designated as G-SIBs by the FSB.

EY contacts

Global

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

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

Emerging Markets

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

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

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

Americas (continued)

David Milne
Canadian Leader Quantitative Advisory Service
Toronto
david.milne@ca.ey.com
+1 416 943 3030

Bismark Rodriguez
Partner, Financial Services Risk Management
Panamá
bismark.rodriguez@pa.ey.com
+507 208 0100

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

David Scott
Partner, Financial Services
Singapore
david.scott@sg.ey.com
+65 6309 8031

Asia-Pacific (continued)

Gary Stanton
Executive Director, Financial Services Office - Advisory
Tokyo
gary.stanton@jp.ey.com
+81 3503 1954

EMEIA (Europe, Middle East, India, Africa)

Henrik Axelsen
Banking Union Centre Lead
London
haxelsen@uk.ey.com
+44 20 7197 7317

Maged Fanous
Partner, MENA Financial Services
Dubai
maged.fanouse@ae.ey.com
+971 (4) 7010599

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

Abigail Viljoen
Partner, Financial Services Africa
Sandton
abigail.viljoen@za.ey.com
+27 11 502 0887

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 andfor 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.

EYG no: 05673-174GBL
1708-2381714
ED None

ey.com/bankingrisk

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

IIF
INSTITUTE OF INTERNATIONAL FINANCE