EY
Building a better working world

IIF
Institute of International Finance

An endurance course: surviving and thriving through 10 major risks over the next decade

Tenth annual EY/IIF global bank risk management survey

Contents

Executive summary

For 10 years, EY and the Institute of International Finance (IIF) have been observing and reporting on changes in how banks manage risk. There has been a lot of progress over the decade.

Financial risks will always be cause for concern in banking. But today, globally, banks are much better positioned in terms of capital and liquidity. Dependence on short-term funding is down materially. Banks have greatly de-risked and de-leveraged their balance sheets, and non-core assets and operations that were amassed in the heady growth years before the financial crisis have been pruned back. Risk management practices around capital and liquidity have been strengthened significantly, in part because of robust regulatory-driven stress-testing across the industry. Accounting changes are supporting banks' ability to build counter-cyclical buffers against future expected credit losses (see sidebar on accounting for credit losses, page 13). These changes have, in principle, been done with unprecedented levels of global regulatory coordination.

Risk leaders and their teams have been innovating approaches to new, or newly emphasized, nonfinancial risks. First among those are cyber risks — without question, this is now the top keep-me-up-at-night risk for many boards and chief risk officers (CROs). Conduct, compliance and fraud, and financial crime and money-laundering risks have also necessitated new ways of thinking and operating. If mishandled, all of these risks can create significant reputational risk for banks.

Taking the positive view of risk management over the past decade, banks are healthier than they were pre-crisis. Congratulations are in order to CROs and their teams and more broadly to those that helped strengthen banks' three lines of defense and governance. The business — the first line of defense — is playing a much more central role in managing the risks it creates.

A more forward-looking view would be less favorable. In some ways, strengthening risk management in the last decade was fairly straightforward. Management could get budget and other resources simply by pointing to specific regulatory or supervisory requirements that needed to be implemented. Meeting those requirements was not easy, for sure, nor comfortable or without stress. After all, regulatory timelines were often short, while expectations were high. But many of the changes were, in practice, rather foundational.

Managing risk over the next decade could prove to be much more challenging. For one, a financial downturn of some kind seems likely in the next few months or years. CROs and their teams will have to show that they can guide the bank to take actions to manage down risks and exposures well before banks have to access their capital and liquidity backstops. This will test the stature and influence of risk management across all banks.

Industry leaders and regulators can already see a host of other significant risks that will require strong risk management over the next decade. Consider the implications of the ever-growing dependence on a complex web of third, fourth and fifth parties or the fact that cyber and privacy risks are becoming more challenging by the day. The industry's transition to more digital strategies, business models and operations is creating new risks, such as those associated with industrializing the use of machine learning (ML) and artificial intelligence (AI) across the enterprise or using cloud across swaths of bank operations. Adapting risk and compliance approaches to enable new businesses, products and pricing models that deliver against vastly different customer needs and preferences will not be easy, especially as banks seek to strengthen operational resilience while doing so. Beyond all these challenges, several tectonic shifts, such as those associated with climate change and geopolitics, will impact banking far more than they have in the past.

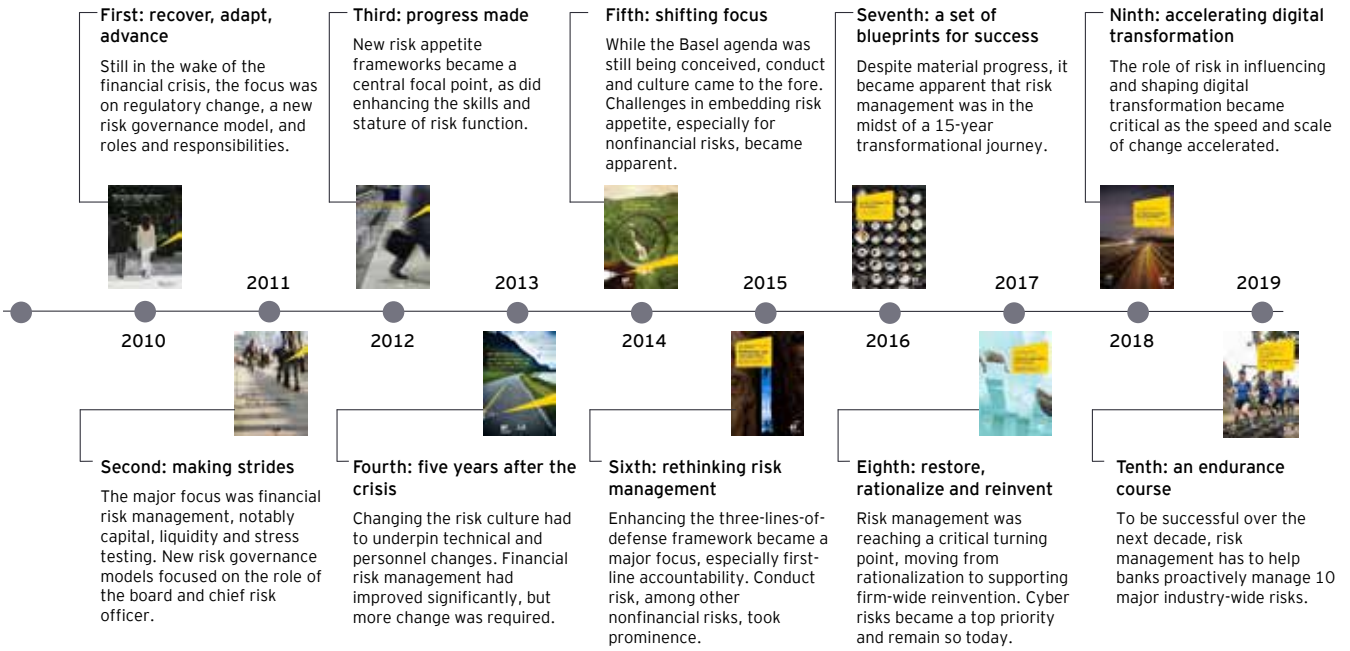
Dealing with any one of these risks individually will greatly test risk management. But their coincidence will call for risk management to:

- Manage a much broader and more complex set of risks, each of which is changing at a fast pace
- Be much more creative and innovative in how those risks are measured and managed, including being more predictive
- Deliver risk management effectiveness efficiently

The next 10 years will be interesting to watch — and challenging to manage. There's no off-the-shelf playbook for managing many of these risks. It will call for endurance and agility for banks to survive and thrive.

A decade of two halves

Figure 1: A decade of risk management transformation



As shown across the 10 years of global bank risk management surveys conducted by EY and the IIF, risk management within the global banking community has been on a transformational journey since the last financial crisis (Figure 1).

In the first half of the decade, the initial focus was on financial risks: capital, liquidity, counterparty risks, and associated issues, such as stress-testing and model risk management. Early improvements were made in terms of governance, with greater involvement of boards, and enhancements to the CRO's role and stature (and, by inference, the CRO's team). This engendered a significant emphasis on having a strong, independent second-line risk management function with an effective leader who has unfettered access to the board. These changes required an early focus on roles and responsibilities, which in turn precipitated a decade-long journey to build out an effective three-lines-of-defense operating model.

Several years in, banks and regulators recognized the need to create and implement effective risk appetite frameworks (RAFs). These quickly became the cornerstone of enhanced enterprise-wide risk management. Most banks introduced an RAF for the first time, forcing them to clearly articulate key risks facing the bank and, within that, gain agreement between the board and senior management that they were willing to take risks and accept specific levels of exposure across primary risk areas. Albeit a simple concept at one level, these frameworks revolutionized risk management. Efforts are ongoing as to how best to translate board guidance on appetite into actionable decisions deep in the organization.

Midway through the decade of change, culture came to the fore. The new or enhanced capabilities aided better risk management. Ultimately, there was recognition that culture matters because it is the foundation for behaviors that support appropriate, balanced and informed risk taking and, where necessary, escalation. Continued and significant instances of misconduct sharpened the focus on conduct risk and banks started to develop new risk approaches to influence behaviors. Those efforts continue today because this remains unfinished business for many banks.

In the second half of the decade, there was a material shift from financial to nonfinancial risks, as shown in Figures 2 and 3. The former have not gone way, of course, and the associated regulatory reform program continues, with jurisdictions now focused on finalizing and implementing global standards. But the energy in risk management shifted to the panoply of risks that had, for many years, been subsumed under the banner of operational risk. The initial focus was on compliance, conduct and fraud; later, cybersecurity and other IT risks captured the industry's attention. Today, the CRO's key priorities include strengthening operational resilience, privacy and cloud, and the transformation to digital, to name but a few. Along the way, boards became highly attentive to business-model risks, reflecting their core role of overseeing long-term strategy and a sustainable competitive positioning.

Figure 2: CRO 12-month risk priorities, 2012 to 2019

Rank	2012	2013	2014	2015	2016	2017	2018	2019
1	CRE	CRE	CRE	REG	REG	CY	CY	CY
2	LIQ	RA	RA	RA	CY	REG	CRE	CRE
3	RA	REG	OR	CRE	CRE	CON	REG	DIG
4	MR	OR	REG	OR	RA	CRE	OR	CON
5	REG	LIQ	RC	CAP	OR	OR	TECH	REG
6	TECH	CAP	CAP	LIQ	TECH	CUL	CON	OR
7	STR	MR	MR	TECH	STR	TECH	RA	CUL
8	CAP	STR	LIQ	STR	CON	ERM	BM	PRI
9	RC	TECH	STR	MR	CUL	RA	CUL	RES
10	OR	RC	TECH	CY	ERM	STR	STR	MO

Key	
Financial risks	
CAP	Regulatory capital management
CRE	Credit
LIQ	Liquidity
MR	Market risk
MO	Model
REG	Regulatory implementation
STR	Stress testing
Nonfinancial risks	
BM	Business model
COM	Compliance
CON	Conduct
CUL	Culture
CY	Cybersecurity
PRI	Data privacy
ERM	Enterprise risk management
OR	Operational
RES	Operational resilience
REP	Reputation
RA	Risk appetite
RC	Risk controls
TECH	Risk technology architecture
DIG	Transition to digital strategies

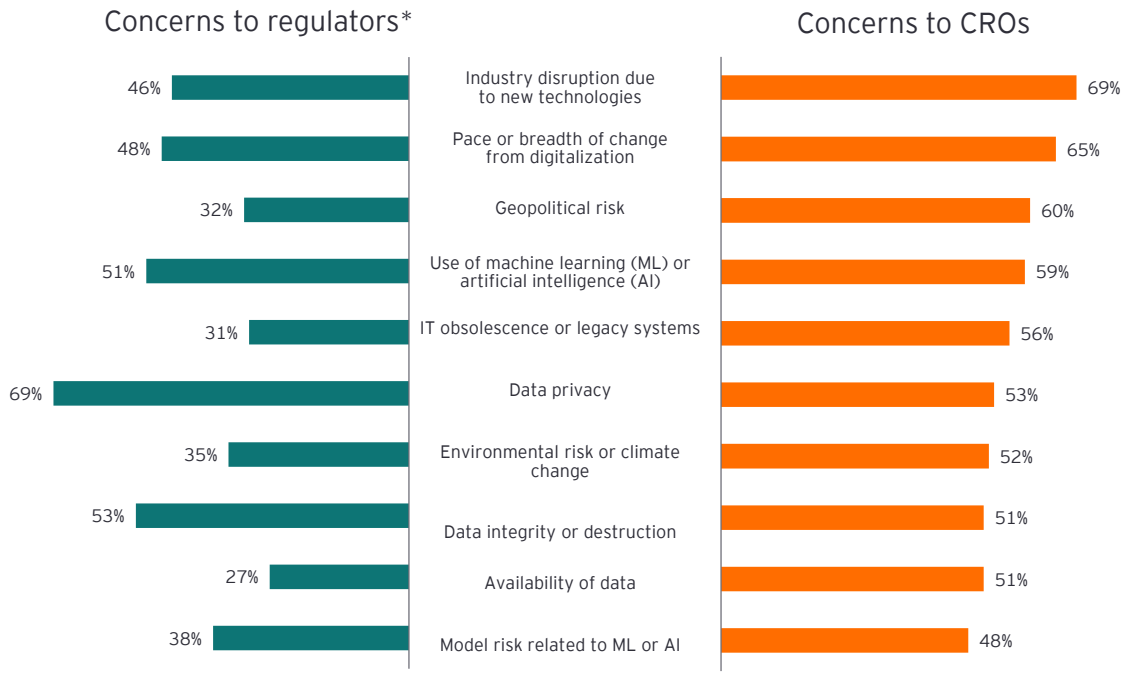
Figure 3: Board 12-month risk priorities, 2013 to 2019*

Rank	2013	2014	2015	2016	2017	2018	2019
1	RA	RA	COM	REG	CY	CY	CY
2	LIQ	COM	RA	CY	REG	REG	CRE
3	REG	LIQ	CRE	RA	BM	RA	DIG
4	CAP	CAP	LIQ	CUL	RA	CRE	CON
5	OR	OR	CUL	CRE	CRE	CON	REG
6	STR	STR	CON	CON	CUL	OR	CUL
7	ERM	REP	OR	CAP	CON	BM	OR
8	CUL	CON	CAP	STR	REP	REP	BM
9	TECH	CUL	TECH	OR	OR	CUL	RES
10	REP	ERM	STR	TECH	STR	CAP	RA

* CROs' views of boards' priorities

The increased focus on nonfinancial risks is even more striking when looking beyond the next 12 months to the emerging risks over the next five years or more. Figure 4 highlights longer-term risks, including political upheaval, climate change and industry disruption. There is a multiplicity of data challenges, whether related to privacy risk, data availability or data integrity listed as emerging risks.

Figure 4: CRO and regulator priorities over the next five years



* CRO's views of regulators' concerns

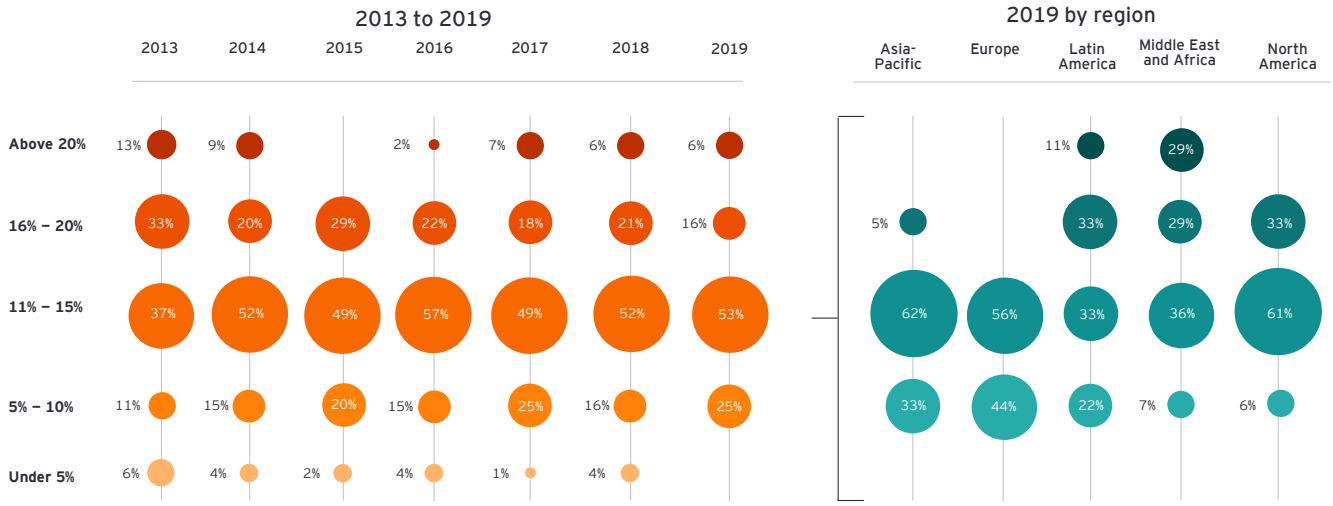
Amid a period of convergence, regional variation abounds

In some ways, the past decade can be characterized as being about convergence. The regulatory reform agenda may not have been implemented in a fully consistent manner globally, and will likely never be, but overall the agenda created an unprecedented level of convergence of regulatory requirements, especially around prudential matters (e.g., capital and liquidity), board and internal governance, and risk management. The resultant narrowing variety of bank strategies and business models, and the sale of non-core or riskier businesses and of less liquid assets, was a common feature of banking globally.

The net effect was growing industry convergence toward lower targeted (though not always achieved) returns on equity (ROEs), as shown in Figure 5. Gone are the days of banks promising to deliver pretax 20% to 25% ROEs, which had been commonplace pre-crisis. Target ROEs fell materially, other than for banks that were in regions that were, initially, less subject to regulatory reform or that had local market growth. Over the decade, banks globally started to converge on 10% to 15% target ROEs. Those banks with greatly depressed ROEs initially, slowly improved their economics, while those promising higher returns found the regulatory agenda caught up with them and eroded their economics.

However, what appears to be industry convergence hid significant regional divergence. From an ROE perspective, the differences are material. Today, banks operating in Latin America and Middle East and Africa are quite profitable, with about half (44% and 58%, respectively) expecting ROEs above 15%. North American banks are also healthy, with only 6% unable to deliver at least 10% returns. By contrast, European banks are still experiencing fairly anemic growth and performance: 44% think they cannot yet deliver ROEs above 10%, and none are expecting to achieve returns above 15%.

Figure 5: Banks' target returns on equity over subsequent three years

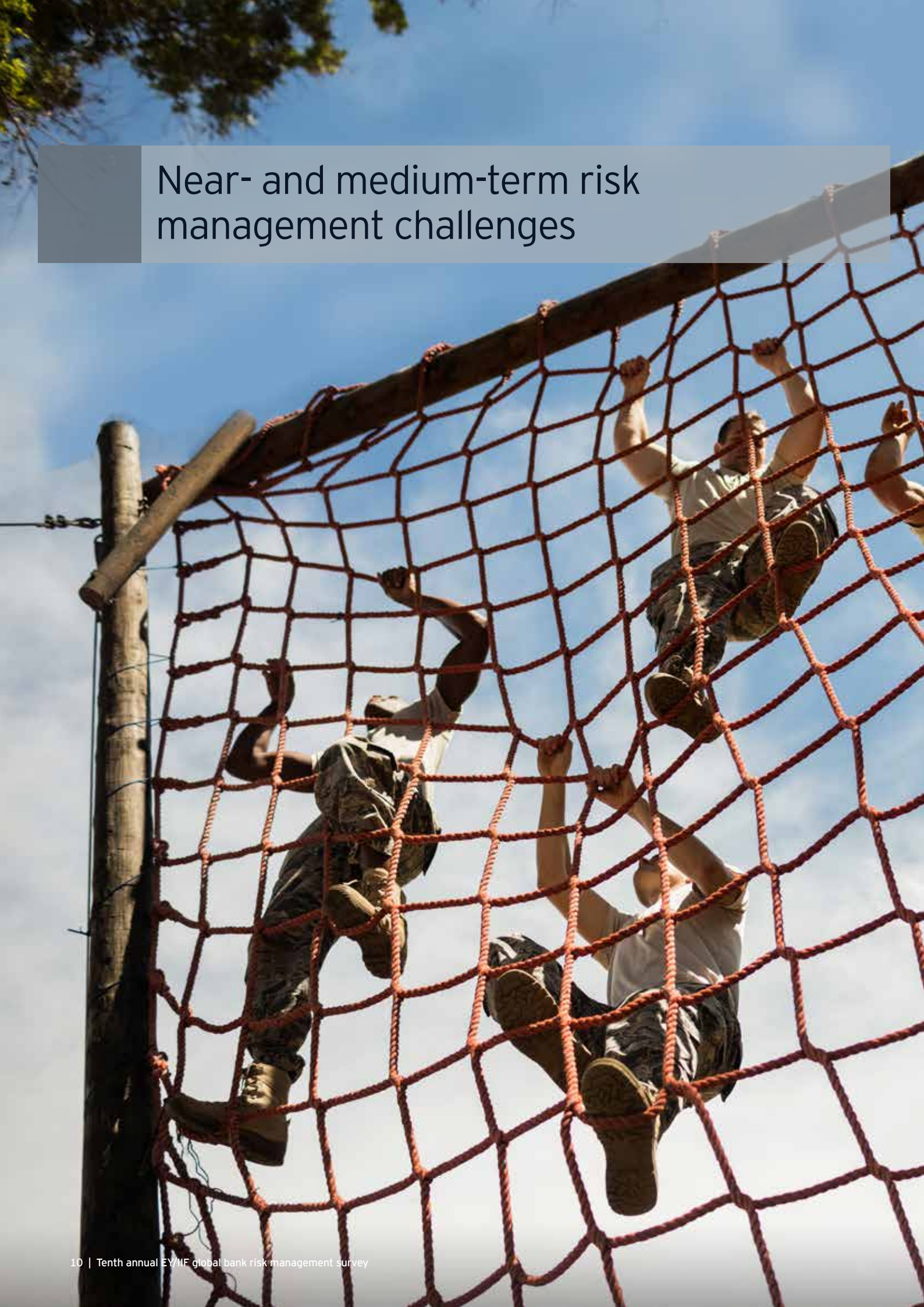


CRO priorities have varied regionally over the years. Banks in the Asia-Pacific region had a mix of issues to deal with, including a strong regulatory focus on market and consumer conduct, geopolitical tensions, and, more recently, the local impact of global trade wars. European banks, meanwhile, continued to grapple with challenging economic conditions: first the sovereign debt crisis, then stagnant growth and lately a prolonged Brexit, which is causing continued uncertainty for market participants. Latin America has faced domestic and political instability in many countries. Middle East and Africa experienced a mix of political instability, yet growth in some areas. The North American regulatory agenda, especially in the US, was broad based and impacted banks sooner than many other countries (perhaps with the exception of the UK).

In addition to new regulations – some local and others part of the broader Basel agenda – supervisors set out demanding new expectations across an array of areas such as capital and liquidity management, many of which affected risk management. Yet, in practice, the pace of implementation across regions has not been uniform.

As a result, while an overall industry journey of enhanced risk management has been visible across regions, local priorities varied materially over the past decade.

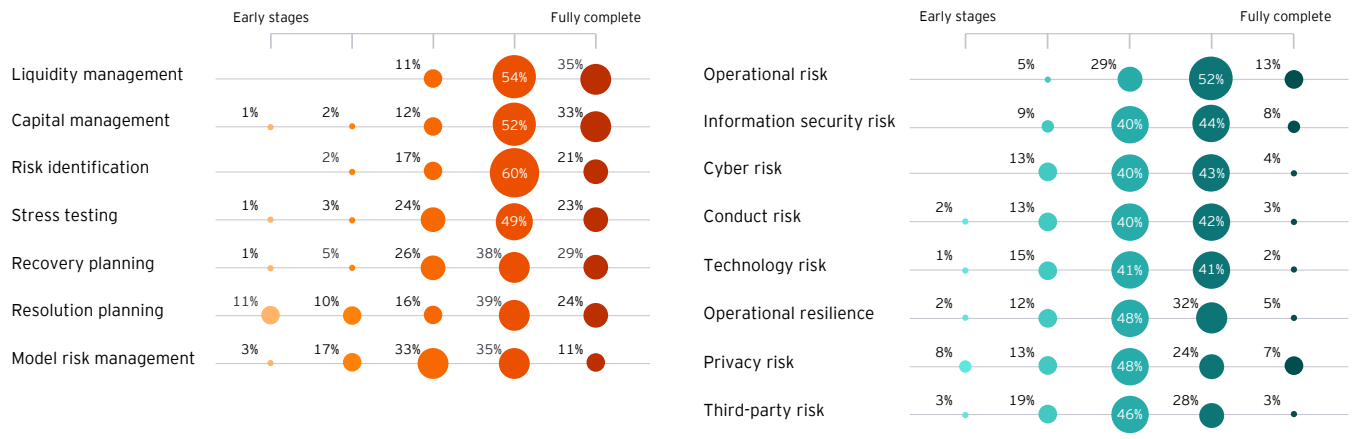
Near- and medium-term risk management challenges



While there has been a substantial amount of regulatory change, on reflection, CROs are fairly positive on the overall impact. "Increased discipline with respect to stress-testing, capital and liquidity management is a positive for the industry as a whole," said one CRO about prudential regulation. "For a given product, the degree of thought that is now put into these issues would have been unrecognizable 10 years ago. It's amazing the number of lenses that products are now put through," said another about the impact of consumer protection and conduct regulation.

The quality of risk management undoubtedly has been enhanced. Reflecting the changing focus from financial to nonfinancial risks, risk professionals highlight differing levels of progress in implementing risk management across these types of risks. As shown in Figure 6, enhancements to financial risk areas are generally at an advanced stage, if not complete. By contrast, there is still much room for improvement in managing nonfinancial risks. Cyber risk is a recent example where banks have been building up their expertise and approach. The real challenge for CROs and their teams is building approaches that capably span both financial and nonfinancial risks.

Figure 6: Progress in implementing risk management processes



More effective, but certainly not efficient

Notwithstanding the fact that risk capabilities have matured overall, most banks have designed their risk management approach in light of new regulations or supervisory findings – and in short timeframes. As a result, enhancements were often implemented using highly manual processes and suboptimal approaches, many of which are cumbersome and expensive to operate, especially in an environment where scrutiny on costs remains high.

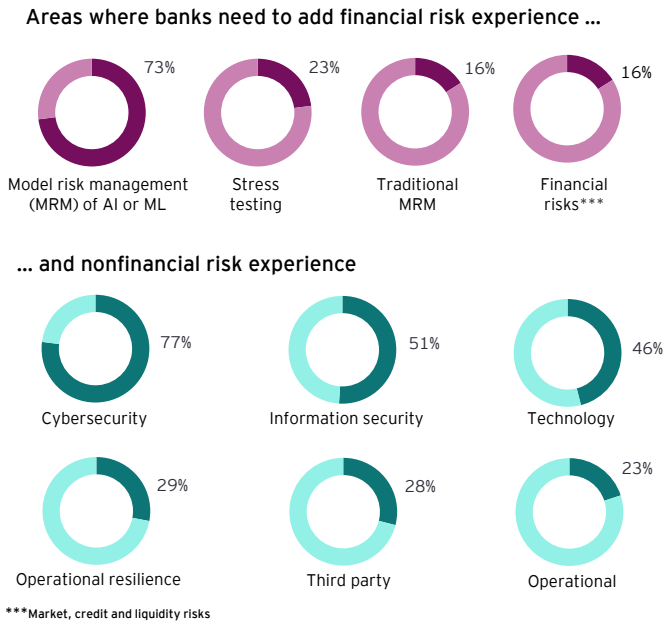
As a result, banks are seeking opportunities to become more efficient by rationalizing processes and increasing automation. Doing so not only enhances efficiency, but also promotes sustainability of the process or approach. Almost three-quarters (73%) expect to improve the efficiency of risk management over the next three years. Other priorities include:

- Improving risk management's ability to inform decision-making (56%)
- Integrating risk activities across the control functions: risk, compliance and audit (55%)
- Completing the implementation of governance, risk and control technologies (55%)
- Enhancing board (24%) and senior management (22%) oversight

Altering the talent strategy will be a key area of focus, as well. A large majority (69%) expect to add specialist talent, and nearly as many (62%) will work to obtain the right mix of skills. As one risk leader said: "We will see a greater focus on skills around machine learning, data privacy, IT, data security, the climate change agenda, and so on. That will bring different kinds of thinking and approaches. The way change and disruption is managed will evolve, from the traditional, linear project management approach to a more agile, making-it-up-as-you-go-along approach." Figure 7 shows the skillsets that will likely be most in demand in the coming few years.

> "We are looking at our own people and wondering whether we need to re-skill them or get new skillsets.
>
> – Risk executive

Figure 7: Specialized talent banks feel they still require today



Libor transition: from misconduct to market illiquidity

Perhaps one of the most startling instances of industry misconduct by a small set of individuals was the manipulation of interbank rates. While much of the alleged misconduct that grabbed headlines in the wake of the financial crisis predated it, rate rigging continued to unfold several years after. It shocked everyone.

What started out as misconduct quickly turned into a market liquidity issue. Post-crisis, transactions in the interbank market declined precipitously, and ironically, this led to a heightened dependency on quotes from panel banks based on expert judgment – and those panels have increasingly become reticent to submit quotes for fear of legal or reputational risks. Liquidity has continued to dry up, and concerns have surfaced that fallback language in legacy contracts is generally weak, which could significantly disrupt financial markets in the event of a permanent cessation of the London Interbank Offered Rate (Libor).

As such, policy-makers, regulators and industry participants have been working together on the transition to alternative reference rates for several years. However, there is still much work to be done. While banks (and in particular larger institutions) are generally more aware of the issue than they were a year ago, substantial hurdles remain. The fact that various jurisdictions are taking differing approaches adds complexity[1]. Given that Libor underpins in excess of US$400 trillion in contracts, the transition has to be successful, for everyone's sake. Transitional challenges include having to:

- Make sufficient resources available, such as key personnel or budget (46%)
- Validate that business-as-usual data- and time-series management processes support new risk-free rates (45%)
- Identify and model new risk factors (39%)
- Incorporate new risks into end-to-end risk management processes (37%)
- Adapt key firm-wide forecasting activities, including stress-testing (25%)

There is a range of risks that need to be managed through the transition (see Figure 8).[2]

Figure 8: Risks most challenging to manage during Libor transition

[1] "Libor transition: progress but challenges remain;" IIF study on Libor transition: https://www.iif.com/portals/0/Files/private/cmm_aug18_vf.pdf.
[2] "Libor transition: A certainty not a choice," EY website, https://www.ey.com/Publication/vwLUAssets/ey-ibor-transition-a-certainty-not-a-choice/$File/ey-ibor-transition-a-certainty-not-a-choice.pdf.

Accounting for credit losses

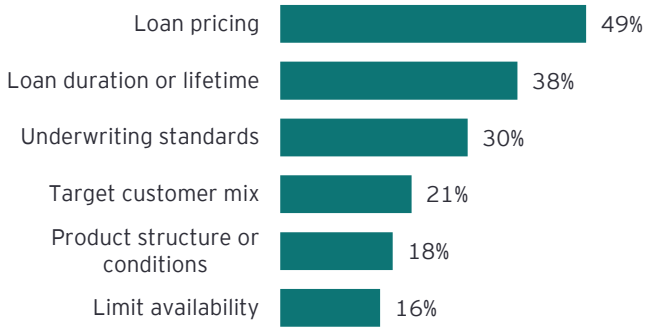
Alongside regulatory reform, banks globally have been working through changes in accounting standards for recognizing expected credit losses. Banks reporting under International Financial Reporting Standards (IFRS) are a few years ahead in adopting IFRS 9 compared with peer banks, who will adopt the current expected credit loss (CECL) model issued by the Financial Accounting Standards Board (FASB).

The industry is split on the likely long-term effects on risk management and loan pricing of the new rules. Almost as many expect the impact to be limited, as those predicting that it will be much greater in the future. Indeed, one in five (19%) already expect the impact to be very high.

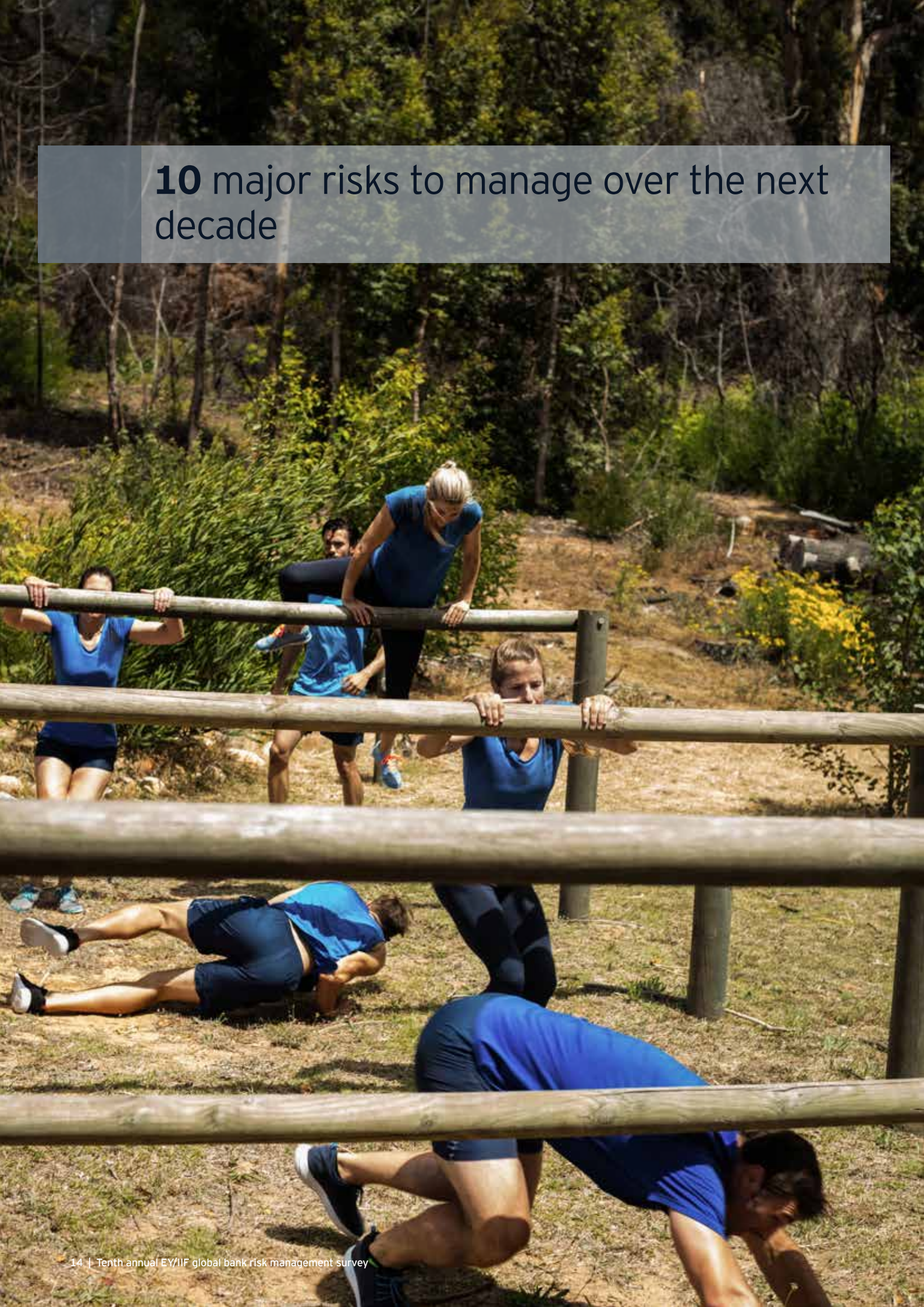
In terms of banks' capabilities to measure and report impairment, banks highlighted several areas of additional complexity, such as modeling (72%), forecasting and stress-testing (68%), and portfolio monitoring and reporting (44%). About a third of banks expect data management and pricing methodologies will be affected. This will likely drive the need for stronger capabilities in the short term and also result in a need for standardization and simplification as the new accounting standards take effect.

It will take time to determine the full impact, in part because it is difficult to evaluate the likely interplay between accounting standards for credit risk and recent changes in capital requirements. Figure 9 highlights how banks believe loan markets could be affected.

Figure 9: Most likely significant impacts on loan markets



10 major risks to manage over the next decade



The last financial crisis has been thoroughly studied, and the risks that crystalized in bringing it about are now well known. For example, at the time, personal and corporate debt reached unprecedented levels; the financing of home-ownership was unsustainable, at least in the US; structured finance products became too complex; both regulation and monetary policies were too loose; and board governance was weak. The list could go on.

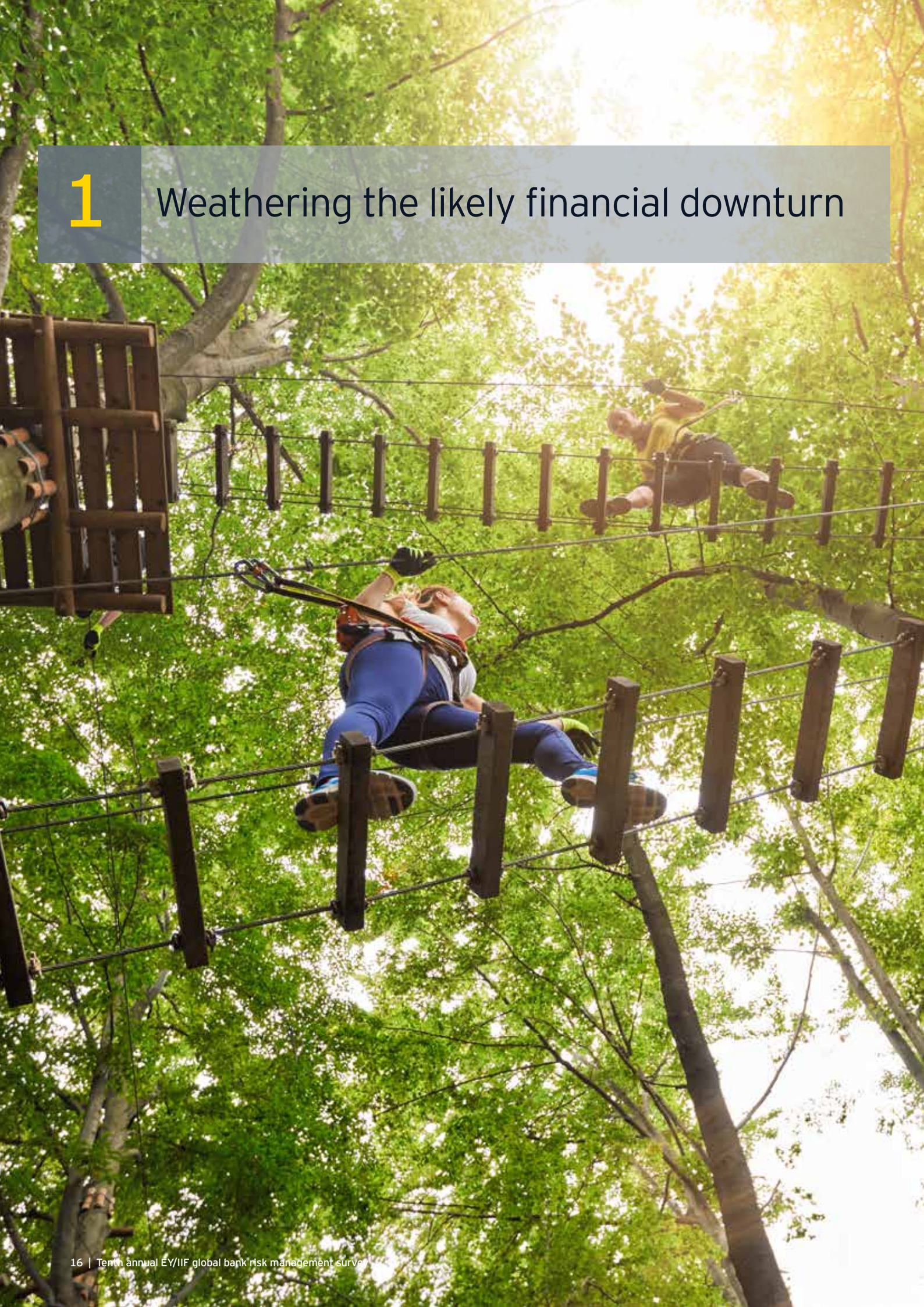
While it is easy to say in hindsight that everyone should have seen that the coming together of these issues was not going to end well, it is also reasonable to observe that not one of these issues was hidden and out of sight. The risks were not unknown, they were simply not understood or addressed.

Given the importance of anticipating risks and managing them pre-emptively, and to mark the 10th anniversary of the global bank risk management survey, EY and the IIF identified 10 major risks that will greatly test bank risk management over the next decade. These issues are akin to those that many, both inside and outside the industry, missed or understated prior to the last financial crisis. They are known, crucial issues that banks will need to manage as well as they do now for capital and liquidity. These are not unknown-unknowns.

These 10 major risks and issues over the next decade are:

1. Weathering the likely financial downturn
2. Operating in an ever-expanding ecosystem
3. Protecting privacy to maintain trust
4. Fighting a cyber war in banks and across the system
5. Navigating the inevitable industry transition to cloud
6. Industrializing data analytics across the business in a controlled manner
7. Delivering services to customers, clients and markets without disruption
8. Adapting to the effects of fast-shifting geopolitics on banks and their customers
9. Addressing the impact of climate change on banks and society
10. Meeting emerging customer demands for customized, aggregated lifetime offerings

Each of these issues is discussed on the following pages, with a view to the specific challenges and uncertainties they present, some of the evolving ways to manage those risks and, importantly, the role of second-line risk management in doing so. Others, especially the first line, have more of a responsibility to manage these risks. But second-line risk management has a prominent role in helping banks keep these risks on the agenda and successfully navigate through the next decade and beyond to deliver long-term survival.



1 Weathering the likely financial downturn

The banking industry globally is unquestionably better placed to manage through a financial downturn than it was a decade or so ago. Back then, there was a heavy dependence on business model and revenue diversity as a mechanism to drive profitability and deliver firm strength and an apparent broader distribution of risk across the system to alleviate concentrations. Capital was a back story. Indeed, credit ratings for banks showed an inverse relationship between capital levels and credit ratings (the larger the bank, the lower the proportion of capital rating agencies required they hold). Everyone remembers how that turned out.

Risk executives are quick to acknowledge that the global regulatory reform agenda was positive overall. "Increased discipline with respect to stress-testing, capital management and liquidity management is a positive for the industry as a whole," noted one risk executive. Regional differences still exist, but generally banks have far more capital and liquidity than they had for decades, especially large, systemically important banks. As one CRO stated, banks are "better prepared for an economic downturn – they are more thoughtful on capital usages, and there is a better understanding of credit concentrations and behavior of counterparties when stressed."

Better placed, but a severe downturn could highlight cracks

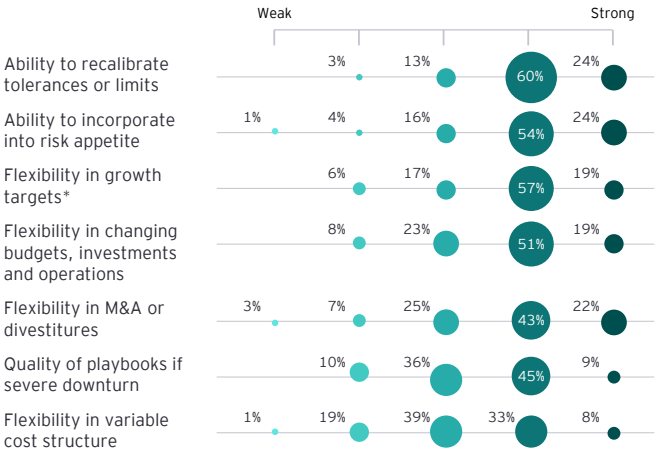
Notwithstanding efforts by central banks and policy-makers globally, it is a near certainty that the next financial downturn will occur within a few years. Cycles may have been altered through tougher regulation, stronger central banking prudential powers, and more active interest rate management, but economic cycles are inevitable. The question, as always, is not if, but when and how severe. Indeed, conditions today portend economic challenges ahead. One executive summed up the current situation well: "In terms of the macroeconomic environment, we are seeing a move away from greater globalization, toward an increasingly de-globalized world, and a tougher economic environment on all fronts." Low or negative interest rates make it even harder on banks.

Banks are relatively sanguine about their ability to weather an economic downturn, as noted in Figure 10. From a risk perspective, the groundwork laid over the past decade means risk leaders feel relatively well-prepared to manage risk thresholds and limits – mechanisms are now in place to facilitate such changes as external conditions shift. Similarly, overall, banks feel well-placed to dynamically adjust growth targets, budgets and investments, and M&A activity. This flexibility, if real, will prove important.

> "Our board members do not have the same experience as management — most were not here last time. The business has changed substantially.
>
> – Risk executive

A severe economic change may challenge banks, however. Regulatory stress-testing models suggest that banks can withstand severe economic shocks, but when asked, some banks are less confident about the quality of their playbooks during a severe downturn. They also acknowledge they still have relatively inflexible cost structures. Banks would do well to revisit their playbooks now and make necessary enhancements.

Figure 10: Adaptability of bank to an economic downturn



* By portfolio and market or client.

Crystal ball watching: a basket of leading and lagging indicators

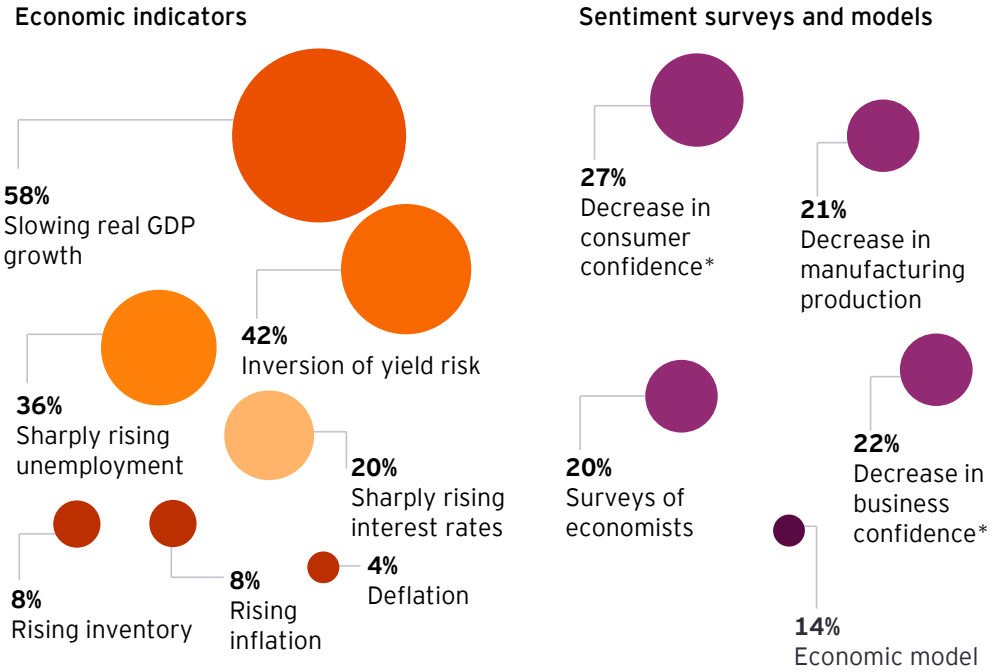
Risk managers have an important role in enhancing downturn readiness. Within their own domain, they have to validate that their risk monitoring captures emerging risks early enough to inform decision-making. They can also evaluate their risk tools to check whether they allow for sufficiently fast changes to risk thresholds and limits, when indicators start to turn negative.

Risk leaders can also pressure-test corporate and business-line strategies and plans. Do those plans sufficiently capture macroeconomic risks on an ongoing basis, and are they sufficiently flexible to adapt to those risks? This is more than a kick-the-tires exercise. Those plans have to be downturn-ready, because they drive so much decision-making at corporate and business-line levels.

An interesting question is which metrics should CROs monitor? In some ways, the most highlighted metrics in Figure 11 are lagging indicators, such as slowing real GDP growth and sharply rising unemployment. CROs watch consumer confidence surveys but pay less attention to their corporate confidence, yet the latter is significant. That said, the focus on the inversion of the yield curve is very understandable, at least in some developed-country markets where it is very much a leading indicator, if history is anything to go by.

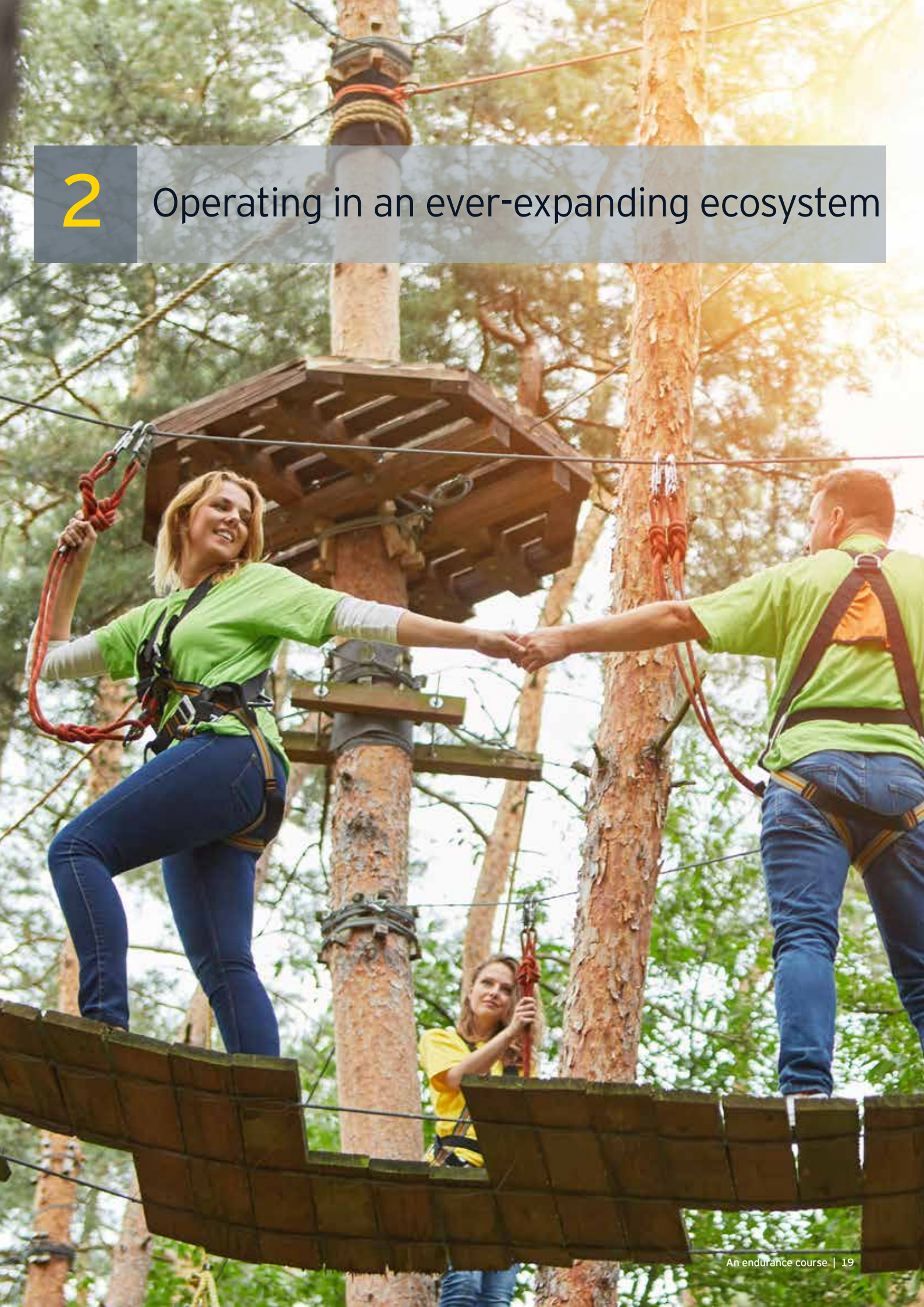
CROs would be well advised to review their set of macroeconomic indicators and validate that the set is a good mix of leading and lagging indicators. Otherwise, efforts to readjust risk thresholds and limits may be slower than needed, especially if the downturn becomes severe faster than expected. The economics profession may be a source of insight, particularly given its enhanced focus on using more real-time data capture and modeling.

Figure 11: Top indicators used by CROs to identify potential material economic downturns



* From periodic surveys

2 Operating in an ever-expanding ecosystem



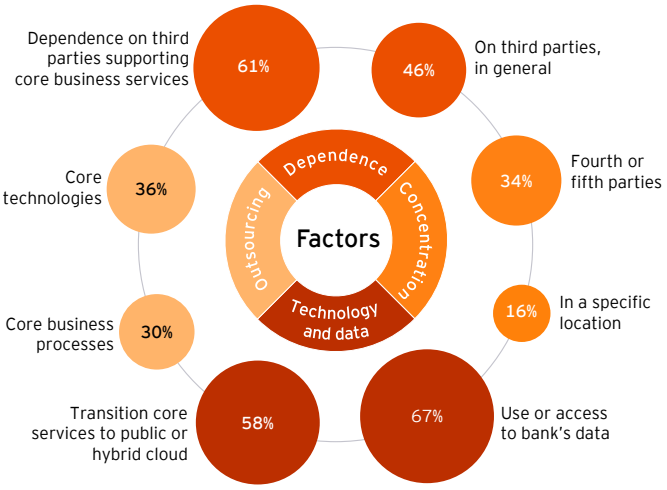
Third-party risk management is not new. The financial services sector has long depended on a complex web of external providers for core and peripheral services. Pressures on banks' economics — and management decisions to focus on core competencies — have propelled many banks to outsource key activities. Still, the current level of dependence on third parties is only a small fraction of what it will likely be in the future. The extended, or rather "hyper-connected," third-party ecosystem looks set to grow, perhaps exponentially, as the industry's value chain disaggregates.

Thus, as banks look out over the next decade or more, the scale of third-, fourth- and fifth-party risk will feel materially different. As one executive summarized, "We absolutely have to pay more attention to third and fourth parties. We've been rigorous in talking to our third-party suppliers and asking about the suppliers on which they have a critical dependency."

Risks abound

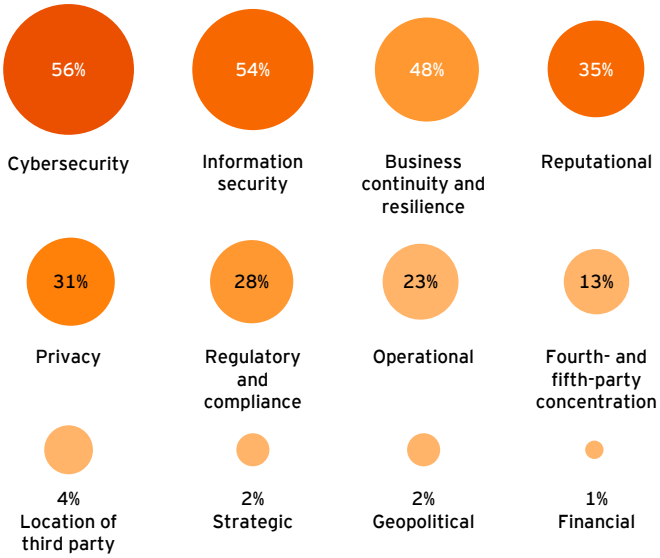
Most banks expect their risk profile will change materially because of increasing reliance on third parties. In general, factors such as overall dependence, concentration risk, issues related to data and technology, and outsourcing will have the most significant impact (see Figure 12).[3]

Figure 12: Third-party factors that will materially affect banks' risk profiles over the next three to five years



Managing these risks will prove challenging. "With the rise of FinTechs and their increased reliance on fourth, fifth and sixth parties, maintaining control is increasingly challenging," noted one executive. Indeed, sometimes banks "discover many of our suppliers have the same supplier of a core service — so actually that fourth party is probably even more important to us than the third party. So, how do you make sure they have the requisite controls, security levels, etc. to make sure they don't make you vulnerable?" Figure 13 highlights the most important risks associated with third parties.

Figure 13: Top third-party risks



Risk management can make a difference

The industry's decade-long transition from procurement to vendor management to third-party risk management has shone a light on the role of second-line risk management. Today, almost half (47%) of banks have their second line set the policy framework, rather than the first line, and about the same proportion (52%) challenge how the first line implements the bank's third-party risk management framework. Larger banks have taken on these roles somewhat more than their smaller competitors, suggesting the industry is maturing toward a model where the second line takes a more prominent role as banks grow in size. About a quarter (28%) of banks' second-line functions focus on identifying emerging risks and trends associated with third parties, while nearly as many set firm-wide risk appetite statements (23%) and metrics (22%) around those risks.

A small proportion of risk functions, particularly in smaller banks, have a focused role around critical third parties, whether it be assessing the actual vendors (15%) or the factors used to determine criticality (14%). The growing focus on strengthening firm-wide resilience will likely push this effort up, over time.

[3] "Global financial services third-party risk management survey," EY website, https://www.ey.com/Publication/ vwLUAssets/ey-global-financial-services-third-party-risk-management-survey/$File/ey-global-financial-services-third-party-risk-management-survey.pdf.

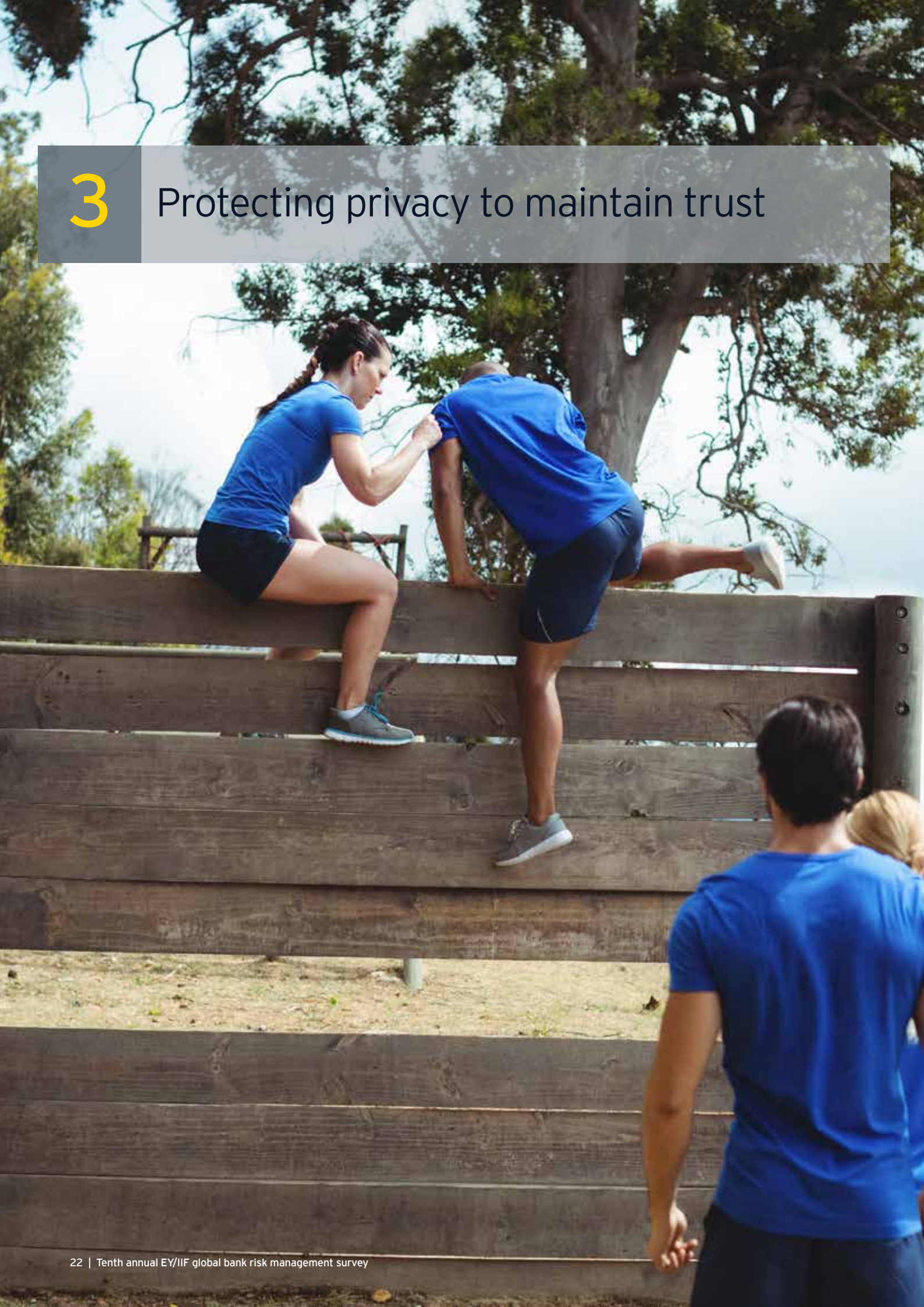
Managing what's critical

Not all third parties are the same. Some are materially more important to the bank than others. As such, almost all (97%) banks maintain a list of critical third parties. The criteria for making that list have changed over the past 10 to 15 years. Originally, it was heavily weighted toward total spending and financial impact. Today, key determinants include the impact on the firm's resilience strategy (66%), the type of data and systems accessed (61%), and the sensitivity of data used (54%).

Identifying critical third parties is increasingly difficult. In the context of strengthening resilience, banks now have to identify their most critical services, and then determine what processes, technologies, people and third parties support those services. It is sometimes difficult to reach internal agreement on which business services are critical, so doubly difficult to identify critical third parties.

If the identification process is challenging, then actually managing critical third parties is even harder. Adherence to conditions in service-level agreements is a primary lever for doing so (71%), as is getting the right contractual conditions in place, such as the right to audit (40%) or conduct site visits (28%). The challenge is ongoing monitoring and what tools to use. Surprisingly, less than one in five (18%) leverage issues management as a monitoring technique and less than one in ten (8%) use external risk data or ratings, even though these can be efficient and effective ways to identify potential issues at specific vendors. If managing critical vendors is the difference between sustained and disrupted critical business services delivery, surely this will need to change.

3 Protecting privacy to maintain trust



Five years ago, there was little public attention on privacy. Banks were not cavalier about privacy; they recognized they owed their customers and clients a duty of care to protect their private information and had mechanisms in place to support privacy commitments, in line with needs at the time.

However, the significant increase in the amount of personal data being processed and number of high-profile cyber events in recent years have propelled privacy concerns up the policy agenda. Five years ago, the loss of 10 million personal accounts was considered major news. Today, the loss of hundreds of millions of accounts does not seem so surprising to the public.

Banks recognize the urgency now placed on privacy. One in four banks (23%) rank it as a top risk in the next 12 months, and one in two (53%) view privacy as a key emerging risk over the next five years. This emphasis highlights that privacy is not simply a technical matter — it is about maintaining trust in the bank and the system at large. As one risk professional said, "What worries us most is the reputational impact if client data are hacked. As a bank, we sell trust to our clients. If we are not able to protect their personal data, that trust is going away."

Being exposed and noncompliant

Large-scale breaches remain banks' main concern, as shown in Figure 14. Banks recognize the reputational damage caused every time a firm in any sector has to admit to a major breach and loss of data. The quality and speed of response certainly matter, but a breach is a breach. As the industry has seen in numerous instances where the bank did not suffer a breach but rather a third party, the reputational damage can be the same. Customers often blame the bank.

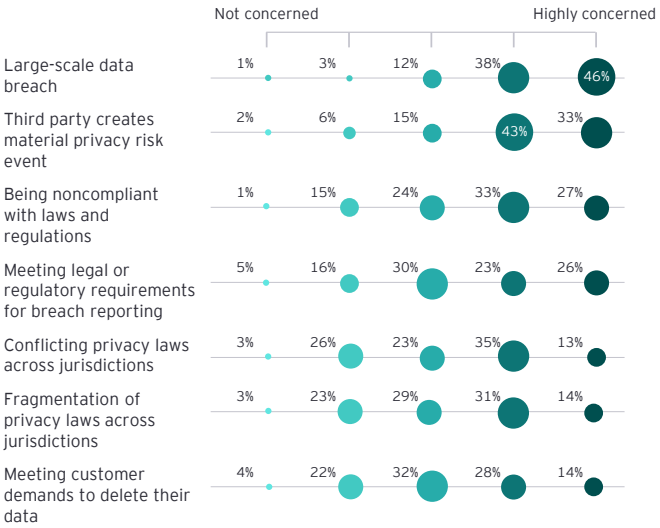
The regulatory and political focus on privacy matters creates additional new risks. Banks worry about being able to remain compliant with requirements overall and specifically relating to breach reporting and are concerned about the complexities of competing local and international requirements. The trend toward regulations that give customers control over their data, while expected, creates significant new challenges relating to data capture, use, movement and deletion.

Integrating privacy into the broad risk framework

As many firms have realized in adapting to the European Union's General Data Protection Regulation (GDPR), new regulations on privacy are much more stringent than those that existed previously[4]. The worldwide political focus on privacy will accentuate these demands.[5]

[4] "How GDPR impacts financial services organizations," EY website, https://www.ey.com/en_us/financial-services/6-ways-to-maximize-value-from-your-cloud-migration.
[5] "Public policy spotlight: the evolving data privacy landscape," EY website, https://www.ey.com/Publication/vwLUAssets/Ey-public-policy-spotlight-evolving-data-privacy-landscape/$FILE/Ey-public-policy-spotlight-evolving-data-privacy-landscape.pdf. "How The California Consumer Privacy Act compares to the EU GDPR," EY website, https://consulting.ey.com/california-consumer-privacy-act-compares-eu-gdpr/.

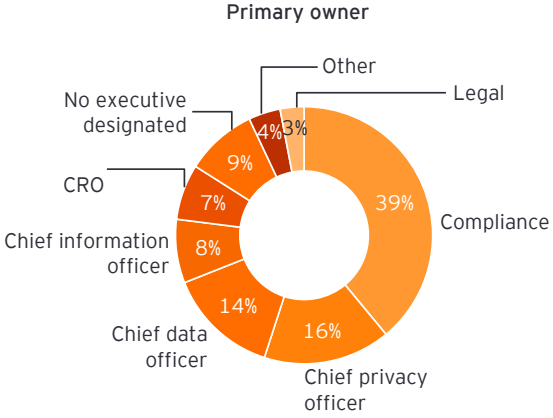
Figure 14: Most concerning privacy risks



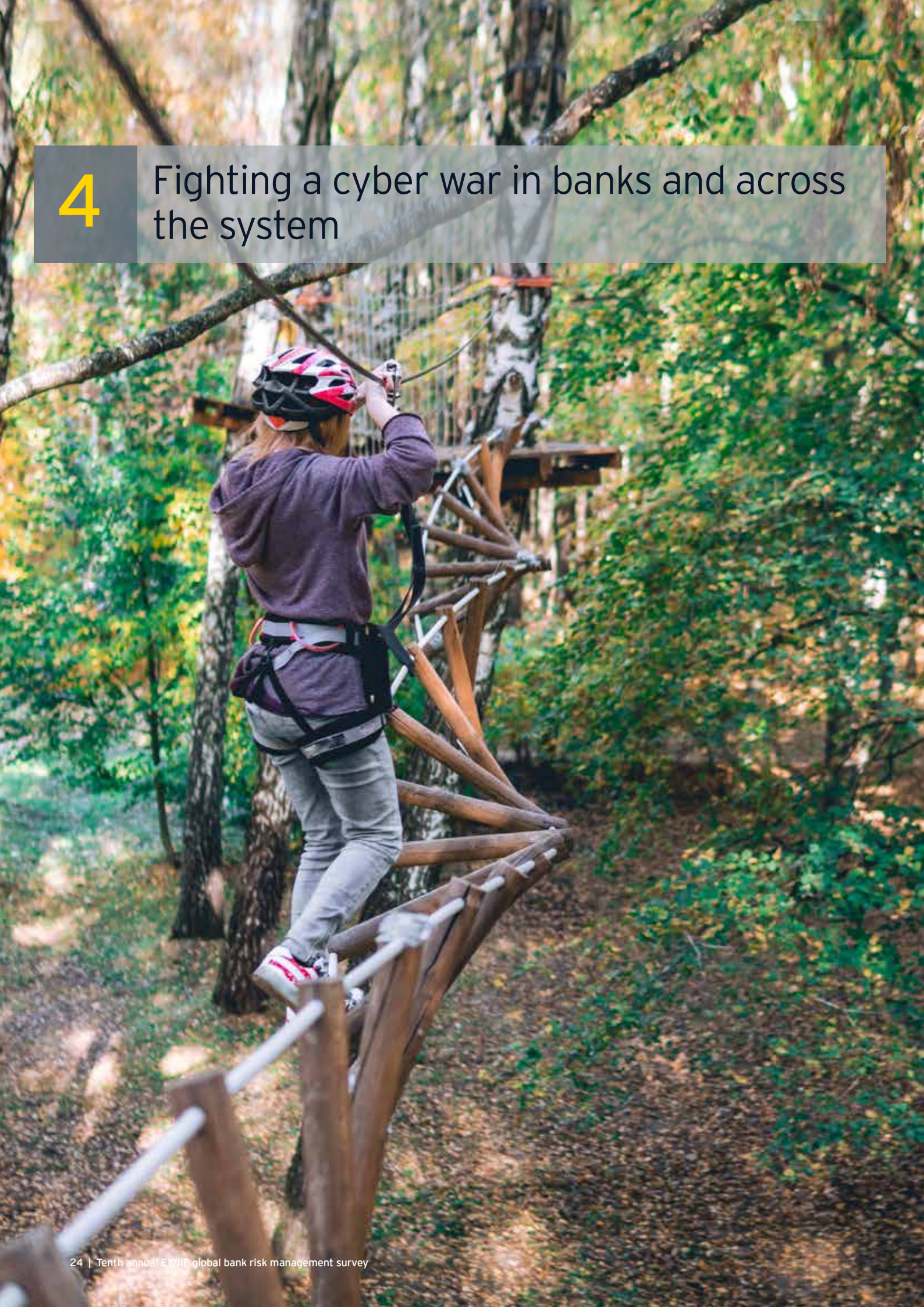
As banks have started to re-assess the adequacy of their privacy programs, many have concluded that more needs to be done to fully integrate privacy into business-as-usual operational and risk management activities. Only about a quarter (28%) of banks feel they have adequately incorporated privacy risk into their enterprise risk management (ERM) framework. Most are in the midst of enhancing their approach, some materially. Over the next three years, almost three in five (57%) banks expect to enhance the degree to which privacy is embedded in ERM, to build stronger data analytics and to establish more robust control frameworks. Almost as many (54%) expect to automate processes.

Second-line risk management has a pivotal role to play, initially by establishing the right risk framework (65%) or by greatly influencing or informing the privacy-risk framework (49%). It has to challenge the first line's approach (68%), validating privacy is being taken seriously, from product design to marketing and distribution. A real challenge is determining who, within management, is accountable for privacy. Currently, across the industry, there is a variety of leaders involved, as shown in Figure 15.

Figure 15: Executive primarily in charge of privacy risk



4 Fighting a cyber war in banks and across the system



Without question, cyber risks top CRO and board agendas. Five years ago, in 2014, cybersecurity did not even make the top 10 priority list for either group. Now it's by far the most significant risk and has been at the top for three years in a row. No other risk comes close.

An industry-level systemic risk

For several years, the focus has been on the degree to which banks are exposed to direct cyber risks. Dialogue then turned to the weakest link — which bank or third party in the financial services ecosystem provided the most significant risk to everyone.

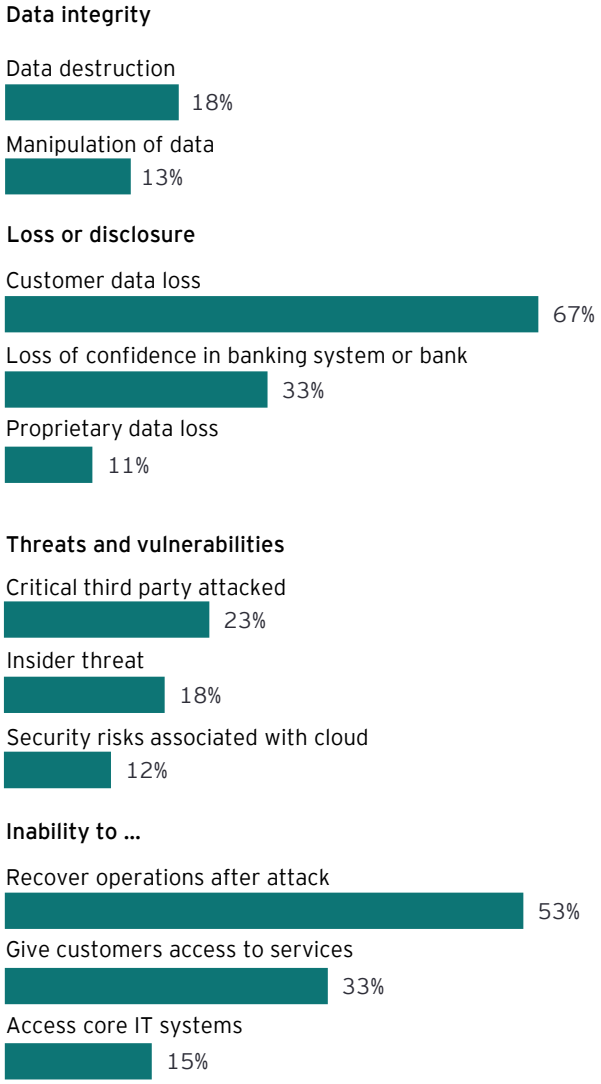
These risks remain important. However, the fact that bad actors, notably certain nation states, have shown a tendency toward destructive — not just criminal — behavior, means the focus has now shifted to industry-wide systemic risk. Four in five banks now believe a system-wide industry-level attack or material event is likely in the next five years, and almost a third (29%) view that as very likely.

The main (68%) concern remains banks having their own systems or data compromised and, thus, creating a systemic, industry-wide issue. But other concerns relate to an attack on a third party, other systemically important financial institution, or even another critical infrastructure industry, such as telecommunications or cloud provider. These concerns explain the heightened focus in regulatory and industry circles on industry preparedness and multi-firm simulations.

The real nightmare: losing data and operations

Given the confluence of privacy and cybersecurity concerns, it is not surprising that banks are most worried about the loss of customer data, as shown in Figure 16. However, banks are increasingly worried about access to, and the integrity of, data — about one in two (51%) banks cite those issues as key emerging risks over the next five years. The impact of cyber attacks on resilience is accelerating up executives' and boards' agendas; over half of banks (53%) worry about the ability to recover operations after an attack and a third about customers accessing services[6]. Indeed, bank leaders view cyber warfare as the top geopolitical risk globally, alongside China's rising global influence.

Figure 16: Top cybersecurity risks



Second-line risk management plays a central role in the three-lines-of-defense approach to cyber risk management. It has taken on a material role in establishing the overall framework (54%) and building cyber risks into the risk appetite (60%) and metrics (63%) frameworks. Boards expect the second line to have an independent view on the bank's vulnerabilities and threats (51%), and the first line's ability to manage those risks effectively (71%).

The challenge is an organizational one. As one CRO commented, "Cybersecurity is one of the biggest issues at the moment, especially when looking at the internal organizational approach. Who is responsible for what? What is the role of the second line? Answering these questions is significant because it is key to finding the right people with the right competence."

[6] "Advancing regulatory fragmentation to support a cyber/resilient global financial services industry."IIF study on Cyber Resilience: https://www.iif.com/portals/0/Files/private/iif_cyber_reg_04_25_2018_final.pdf.

Cyber capabilities need to mature more quickly

There are myriad ways in which banks manage against cyber risks. As a result, the maturity of their capabilities to do so varies materially across banks.

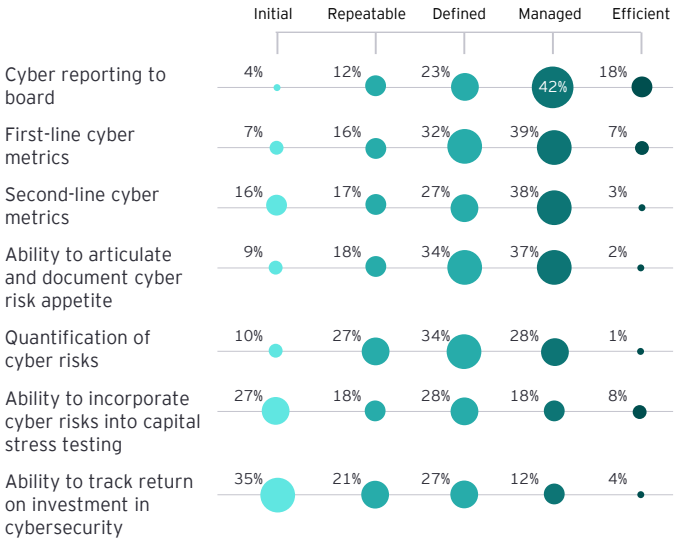
On the positive side, as shown in Figure 17, banks believe they have driven home the importance of having a firm-wide cyber-aware culture and have enhanced their ability to identify risks and vulnerabilities. They also think first-line – and to a lesser extent second-line – cyber reporting and metrics have matured, though they acknowledge there is a long way to go. Many banks admit in conversation that they still rely on key performance indicators (e.g., measuring the percentage of attacks defended against, regardless of severity) as opposed to key risk indicators (e.g., measuring the percentage of most-severe attacks defended against).[7]

Banks struggle most in areas such as data backup and restoration and identity and access management, the latter of which is essential to underpin a robust cybersecurity posture. In risk measurement, banks struggle to properly quantify cyber risks and integrate them into their capital stress-testing.

The most significant challenge (particularly for midsize and small banks) is evaluating the return banks are getting from their investments in cybersecurity. Those investments are clearly increasing. But are banks really getting the return – of whatever kind – they expect?

> “With today’s rapid technology developments, banks are constantly playing catch-up on cybersecurity.”
>
> – CRO

Figure 17: Maturity of cyber risk reporting capabilities*



* Initial (i.e., ad hoc and undocumented); repeatable (i.e., documented and globally respected); defined (i.e., defined as standard business process); managed (i.e., quantitatively managed using agreed-upon services); and efficient (i.e., allows for deliberate optimization)

[7] “Five considerations for cybersecurity reporting,” EY website, https://www.ey.com/en_gl/financial-services/5-considerations-for-cybersecurity-reporting.

5 Navigating the inevitable industry transition to cloud

For a variety of reasons, the banking industry is increasingly moving to cloud, but to date only a few banks have gone all-in.[8] Most have been exposed to cloud through third-party providers supporting enterprise-resource planning, human resource or other such services.

This is changing quickly. The benefits are simply too appealing – cost efficiencies, gains in reliability and resilience, the ability to leverage highly sophisticated analytics, and faster software deployment. Arguably, if implemented effectively, information and cybersecurity safeguards are also stronger. These benefits are hard to achieve if banks maintain their own data and backup capabilities.

Banks recognize they cannot accrue the scale benefits by remaining purely on private cloud. They have to move to hybrid (public and private) or public cloud capabilities.

Knowing and managing cloud transition risks

Materially switching to the cloud is not without risks. Banks worry most about risk to customer or bank data and believe regulators, in general, have the same concerns, as noted in Figure 18. Losing data is not the only risk – maintaining the integrity and availability of that data is also cause for concern. That said, banks are more concerned with reputational risk than regulators, while regulators are more concerned with the geographic location of data and data servers (understandably so, perhaps, given regulation is jurisdictional in nature). It will be interesting to see how regulators deal with cloud concentration and data location issues.

Figure 18: Concerns related to industry-wide adoption of cloud

*CROs' views of regulators' concerns

[8] "6 ways to maximize value from your cloud migration," EY website, https://www.ey.com/en_us/financial-services/6-ways-to-maximize-value-from-your-cloud-migration.

The impact on the bank's ability to maintain delivery of services to customers and clients is a risk that merits vigilance. While in theory cloud provides more resilience, especially when banks avail themselves of in- and out-of-region services, the issue is complicated by a material concentration in cloud providers. This may not be a concern for the bank's direct services but could be an issue if the bank's third and fourth parties also are subject to the same concentration risk and do not have the same levels of cloud resilience. Said one executive, "The board is comfortable with our strategy to use cloud more. But they want us to make sure we are not taking undue resilience risk and to know what the backup plan is if something fails. You have to have a backup plan for everything."

A third of banks are concerned their second line is not sufficiently engaged in the risks of transitioning at scale to cloud. Yet the second line can play an important role in challenging the first line's approach (62%), establishing the firm-wide strategy (31%) and monitoring enterprise-level risk appetite/risk metrics for cloud risks. (40%). Within the context of third-party risk, a notable minority of banks have their second line challenge the testing (28%) and assess the criticality (25%) of cloud service providers.

Risks could strain cloud risk capabilities

In general, risk professionals are most concerned about adapting their risk capabilities (60%) and culture (58%) to cloud. They also know they need to adapt their security-risk capabilities (50%) and invest in interpreting and aligning to evolving regulatory requirements (36%).

Relative to other risks, banks are fairly critical of the degree to which core capabilities are integrated into their cloud strategy, as shown in Figure 19. Even in areas that might be expected to be fairly well integrated, such as business continuity, identity and access management, and data privacy, responses suggest that not all banks are as confident as one might expect. In areas such as systems development and infrastructure asset management, they admit to yet lower levels of confidence.

Addressing these capability gaps will be an essential factor in making boards, regulators and other stakeholders comfortable with a major, industry-wide switch to cloud. Undoubtedly, it will call for industry-level processes, alongside those of individual banks.

Figure 19: Confidence in integration of core capabilities into cloud strategy

6 Industrializing data analytics across the business in a controlled manner

For several years now, the industry has been excited about the potential of ML and AI. Until recently, the promise has been greater than the reality. For sure, banks have been identifying and testing proofs of concept and piloting them. There are ample use cases: anti-money laundering, fraud, conduct surveillance, and credit decisions, to name but a few. However, only some of these pilots have moved into full-scale production across banks.

Driving decisions, not just operations

As noted in last year's ninth annual global bank risk management survey, the industry is on the cusp of change. It is gradually moving to industrializing ML and AI across the bank, especially in first-line operations.

Initially, banks focused on the most obvious target — the low hanging fruit — automating operational tasks (for example, financial-crimes surveillance alerts). There is still scope in some banks to expand usage in these areas.

However, as shown in Figure 20, the next areas of growth will likely be real-time decision-making, such as credit decisions, or automating challenging areas such as compliance and audits. In these areas, more complex human judgments will be augmented by algorithms.

Figure 20: Use of ML and AI now and in five years

Scaling machine learning and artificial intelligence could be risky

ML and AI have vast potential. The industry has not yet fully grasped the degree to which these analytics could fundamentally change how banks operate.

Yet, risk professionals, regulators and policy-makers are very focused on the risks of scaling up these technologies. Banks' risk teams already see challenges in capturing new risks (64%) and getting the right talent to manage the risks (59%).

They also see the lack of historical data in how these models act under different market conditions (54%) and uncertain regulatory expectations (47%) as additional challenges.

There are also broader societal and political concerns. Public discourse is centered on "ethical AI" — the moral or ethical implications of greater dependence on robotics and AI.[9] Naturally, such concerns go well beyond financial services or technological issues. One CRO said, "We tried to have a more centralized approach in the risk analytics department, but you need someone to build regulatory models that meet all the regulator's requirements, and that conflicts with people who want to consider new methodologies that don't fit. It really is a culture clash."

[9]How do you teach AI the value of trust? How embedding trust from the start can help companies reap AI's rewards. https://www.ey.com/en_us/digital/how-do-you-teach-ai-the-value-of-trust.

Model risk management 2.0

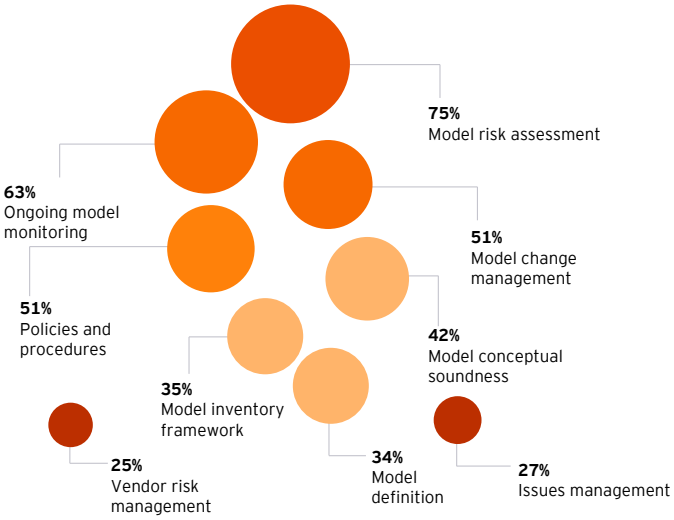
The broad use of models has been a central focus of the global regulatory reform agenda over the past decade. Regulators have been skeptical of internal models, noting that the spectrum of outcomes from such models across banks has been too significant and has hindered common capital and liquidity standards. Recent regulatory initiatives have shown a bias toward standardized approaches. The focus on models, inevitably, has pushed banks to greatly enhance their model risk management (MRM) approaches and capabilities.

However, banks recognize that risks associated with ML and AI are different. Almost three in five banks (59%) view the increased use of these data techniques as an emerging risk over the next five years and almost one in two (48%) point specifically to the associated model risks. Banks acknowledge that responsible innovation requires investment in governance and risk management around ML and AI prior to scaling its usage, not afterward. After all, difficulties with managing risks from AI-based models may hinder their use and acceptance.

Few banks have a solution in place. Less than one in ten (8%) believe they have a fully functioning governance process in place for these risks, and most of those admit to gaps in the coverage of risks such as compliance and data risk. As a result, many banks are currently evaluating the need for a new governance framework (36%) or are in the process of implementing one (28%).

Current MRM frameworks are also likely insufficient to mitigate risks associated with ML and AI. In the words of an executive, "There is probably value, but it is hard to build on it. We don't have enough experience to be comfortable with it ourselves, let alone convince regulators." Not surprisingly, a significant majority (93%) of banks expect to enhance their MRM framework across a range of areas noted in Figure 21.[10] Banks are recruiting specialized talent. They put MRM experience around ML and AI as the top in-demand financial-risk skillset (73% expect to add headcount in this area, compared with 16% for traditional MRM experience).

Figure 21: Model risk management enhancements expected over the next three years to address ML- and AI-related risks



In the end, a key component of gaining political and consumer acceptance is transparency. Customers and clients will want to know when their data informs AI (43%), and when AI is used interactions with their clients (29%). Banks also have to remain aware of the potential for hidden or unknown biases in data sets driving the wrong outcomes (46%), train their employees on the limitations of AI (37%), and remain attuned, and adapt, to public and government concerns (38%).

[10]Building the right governance model for AI/ML: How banks can identify and manage risks to build trust and accelerate adoption https://go.ey.com/30IfRgw.

7 Delivering services to customers, clients and markets without disruption

CROs have been shifting their attention toward the management of nonfinancial risks given the significant improvement in financial risk management over the last 10 years. Indeed, as highlighted by the EY/IIF survey results, cyber, privacy and third-party risks and risks associated with emerging technologies have certainly come to the fore.

Arguably the most significant change in tenor and tone of the regulatory and supervisory focus in recent years has been the shift from financial to operational resilience. Authorities – and increasingly customers and other stakeholders – are not only focused on the ability of banks to continue to intermediate markets and service customers during a severe financial shock, but also on their abilities to do so during a significant disruption to their operations.

From if to when: a shift in paradigm

Historically, operational resilience has been narrowly focused on banks' ability to protect against physical disruptions and resume specific systems, applications and capabilities.

Times have changed. In recent years, major banks and infrastructure providers globally have experienced an array of operational disruptions. The causes have been broad – severe weather events, cyber events, third-party outages, and legacy-system failures have been prominent. The impact – actual and reputational – has been significant. Bank management has had to admit failings to customers, regulators and, for some, politicians.

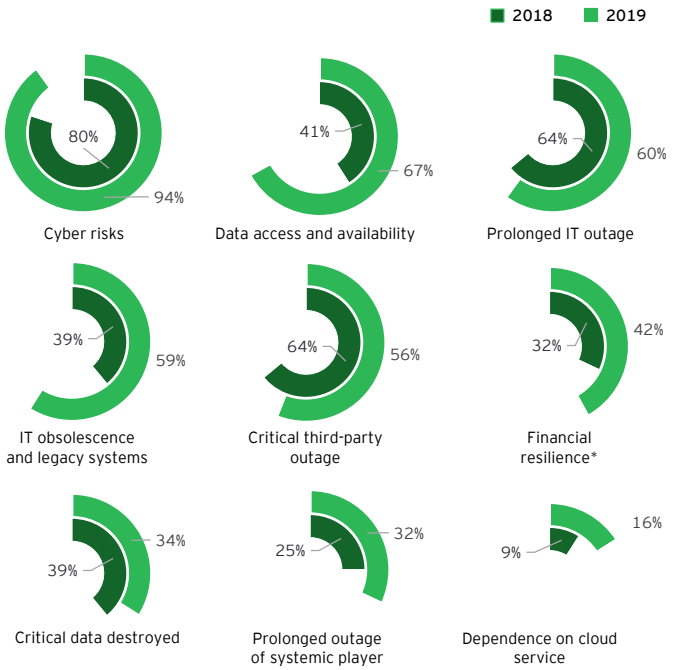
Regulators have quickly reset the fundamentals on how to manage resilience across the enterprise. They are now assessing banks' capabilities to continuously intermediate markets and deliver services to their customers and clients on the assumption a disruption of some kind will occur, not whether it will. The scope of resilience activities is also being challenged, with authorities seeking to understand banks' abilities to prevent, respond to, recover and learn from disruption, whatever the threat or vulnerability that might cause it.

Banks, naturally, have a range of concerns regarding what might trigger a disruption, as noted in Figure 22. Many of these concerns have increased since last year, notably for data access and availability, and IT obsolescence and legacy systems.

The concern that has grown the most over the past year relates to legacy systems and IT obsolescence. As one risk executive summarized, "Internally we are debating whether, given the pace of technological change, rather than continuing to fix and upgrade clunky systems, there is a way of building a totally different bank on the side. The [systems are] so entangled it is really hard to ever get where you want to get to, given the legacy systems." Depending on complex, legacy systems will become increasingly more challenging given the pace and scale of change in products and services.

[11]Ten ways to enhance firmwide resilience https://www.ey.com/en_gl/financial-services/ten-ways-to-enhance-firmwide-resilience.

Figure 22: Top resiliency-risk concerns

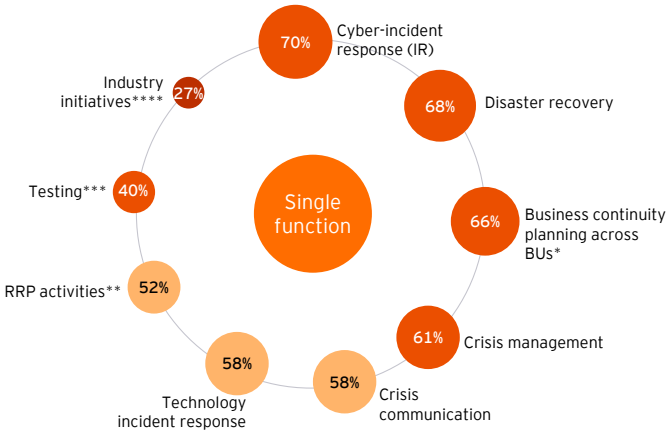


* For example, liquidity, capital and collateral

Concentrate on governance

The fact that so many factors can precipitate a disruption has brought firm-wide governance of resilience to the fore. At some level, this means the way in which boards of directors oversee and challenge the bank's resilience strategy and framework. But more practically speaking, it means how management will integrate resilience across the bank. Many of the firms are moving to centralize aspects of resilience, as noted in Figure 23.[11]

Figure 23: Functions being integrated to strengthen resilience



* Business units
** Recovery and resolution planning
*** Including simulations and table-top exercises
**** For example, Sheltered Harbor in the US or industry-wide cyber simulations

Apply a strong risk lens to resilience

Inevitably, second-line risk management will have to step up its focus on risks to resilience, oftentimes elevating issues across a range of existing (but frequently siloed) disciplines, such as cybersecurity, IT risks, severe weather events or physical security risks. Already, the second-line plays a material role in many banks. One in two establishes the firm-wide resilience strategy and framework (49%), validates that resilience is in the risk framework and taxonomy (52%), and sets firm-wide resilience metrics (49%). Interestingly, almost half (46%) manage the crisis management plan, rather than the first line[12].

In challenging the first-line's approach to resilience (a role 61% already assume), second-line risk management has to focus on core capabilities to prevent, respond to, recover, and learn from disruptions, the maturity of which vary considerably across the industry. Capabilities linked to disaster recovery and data back-ups are relatively mature, according to banks. Crisis-management and incident-response frameworks have mixed maturity levels. Where banks' capabilities are most in need of enhancing is in the areas of firm-wide governance and strategy, program management and reporting, and articulating the appetite for or tolerance to disruption (the latter is particularly important given the UK regulators' focus on defining and implementing so-called impact tolerances[13]).

> "The integration of end-to-end risk management and core operational processes remains the most significant challenge to maintaining enterprise resilience
>
> – Risk leader

[12]Managing through crises: preparation is key https://www.ey.com/en_gl/financial-services/ten-ways-to-enhance-firmwide-resilience.

[13]UK regulators have proposed that firms develop impact tolerances, which define their upper level of tolerance for disruption to certain business services, under the assumption that disruption will occur. This differs from a risk appetite statement or recovery-time objective, as those incorporate an element of probability. See EY/UK Finance, Perspectives: Operational resilience in financial services, June 2019 (https://www.ey.com/Publication/vwLUAssets/ey-perspectives-operational-resilience-in-financial-services/$FILE/ey-perspectives-operational-resilience-in-financial-services.pdf).

8 Adapting to the effects of fast-shifting geopolitics on banks and their customers

Banks are quick to highlight that they have withstood political pressures and geopolitical risks for years. Many note they have been in operation for decades or hundreds of years. Political issues ebb and flow, and banks generally manage through.

To some degree that is true. Banks have long been subject to direct or indirect political change or pressure over the past decades. More recently, one might argue that the global regulatory agenda of the past decade or the 2009 European sovereign debt crisis illustrated how political and regulatory pressures can become blurred. Yet, most banks coped.

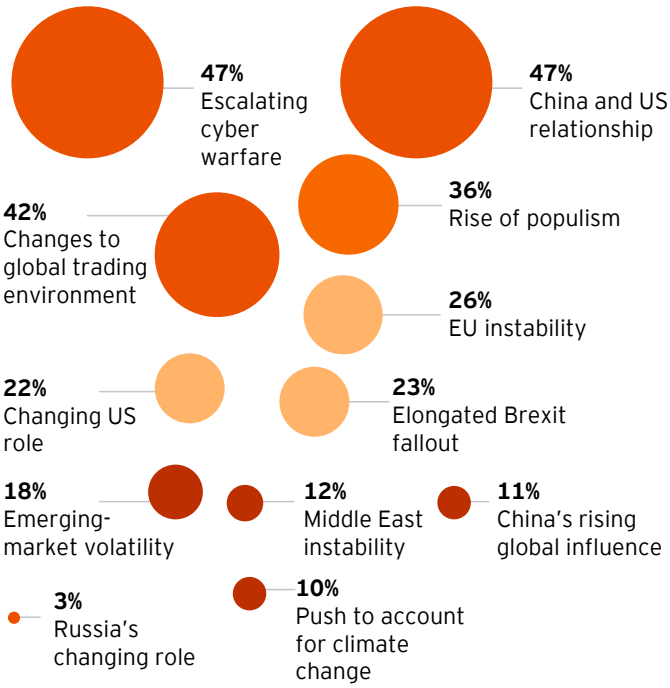
Closer to home

Today, political pressures seem different. The distribution of political power is shifting, especially between East and West. Technology transformations are quickening, making the world more interconnected. Issues of the day, such as immigration and climate change, are cross-jurisdictional global matters. Not surprisingly, three in five banks now view geopolitical – or domestic political – issues as a major emerging risk for the industry over the next five years

Figure 24 highlights the political risks that worry banks the most. The impact of some of these risks is often diffused and therefore hard to discern, such as the changing roles of China, Russia and the US, or the rise of populism across democracies. Others are more palpable, such as being subject to nation-state cyber warfare, or the impact of Brexit on the UK and European Union.[14]

Nevertheless, banks believe political issues will have a more material impact on them and their customers in the coming years. Four in five expect the impact to be somewhat (58%) or much more (22%) significant over the next decade. Banks believe they will likely be affected via the overall impact on global or domestic demand (78%), unexpected market volatility (74%) and the impact on customer demand (41%). More directly, the supply chains of corporate clients (32%) or, to a lesser extent, the operational or financial strength of bank third parties or counterparties (10%), might be adversely affected.

Figure 24: Top geopolitical risks that will impact banks over the next decade



It's not simply a matter of guesswork

For many executives, evaluating complex geopolitical trends often seems more of an art than a science. It requires an ability to read between the lines and make bold, but highly speculative, predictions about potential political outcomes, and their broader relevance for their institutions.[14]

Yet, while banks are quick to recognize they will be more subject to political risks in the future, they acknowledge they need to be more aware of those risks, and better adapt to them. Four in five banks say they either need to enhance their understanding of political risks or improve their ability to adapt to those risks as they change.

[14]Why you need a strategic approach to political risk https://www.ey.com/en_gl/geostrategy/why-you-need-a-strategic-approach-to-political-risk.

Geopolitical analysis is not simply for those with arcane policy knowledge. Rather, banks have to establish robust capabilities to evaluate political risk and determine potential actions to address identified risks.[15] As shown in Figure 25, banks highlight that they are very focused on (second order) macroeconomic conditions, as well as on building political considerations into the markets, sectors or clients they are exposed to, or the markets they operate in. Beyond those market-focused decisions, it is important that political issues are built into capital-stress-testing scenarios, annual strategy-planning processes, and business continuity plans.

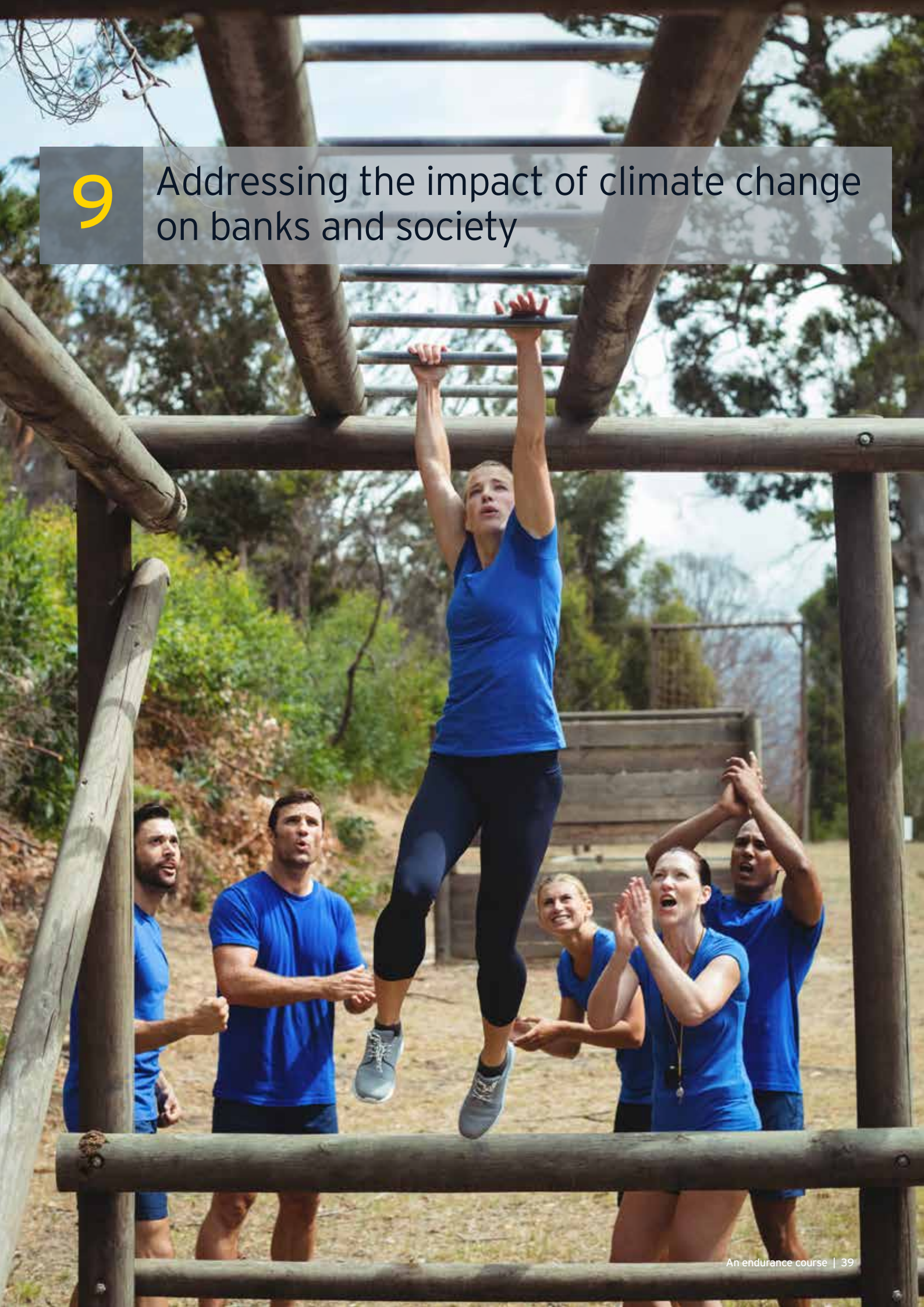
Second-line risk has an essential role translating political intuition and debates into decision-making. As one risk executive put it, "The risk function has a role to help set and define the framework, instill the necessary discipline, and work with and challenge first-line management." A large proportion of banks (75%) have their second line monitor the impact of politics on the bank's risk profile, and challenge how line-of-business plans, or country or sector plans, incorporate political risks (47% and 39%, respectively).

Within that context, it is important to translate analysis into action. One CRO highlighted a range of ways his bank incorporates political risks in management decision-making, "We approach it first by looking at country risks, and whether certain countries are becoming riskier, which can impact decisions as to whether we open or keep open certain locations. We also look at where third-party providers are. Finally, we also look at credit risk and direct exposures – we look at our portfolio and the impact on certain sectors – and how best to build it into scenarios that are part of our sector-specific stress-testing exercises." Getting it right will take time. As she noted, as of now, "the majority of what we do are medium-term adjustments."

Figure 25: Ways banks use to analyze impact of geopolitical risks

[15]What we are watching: geostrategic outlook https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/geostrategy/ey-geostrategic-outlook-february-2019.pdf.

9 Addressing the impact of climate change on banks and society



Climate change has risen on public and political agendas. The fact the world has just experienced its hottest summer on record is known by everyone. The realities of fires in Brazil and California, or hurricanes in Asia and Central America, are prime-time television. It could not be more real. Climate change has moved quickly from what seemed like a sometimes esoteric, academic debate (notably about cause and magnitude) to a political and societal issue globally, not least because the biggest impact of climate change will fall on many of the world's poorest countries.

> "Climate change is one of the defining risks of our career to manage
>
> – Bank risk leader

Banks increasingly recognize the importance of this issue. Over half (52%) of banks view environmental and climate change matters as a key emerging risk over the next five years, up from just over a third (37%) a year ago.

Yet, levels of understanding of the potential impact on banks – for example, on credit defaults or corporate loans – varies significantly from bank to bank and continent to continent. Some banks have committed to the recently launched UN Principles for Responsible Banking and are driving climate change commitments deep into their organization, while others are more focused on addressing their environmental footprint and better disclosures. Banks are having to address climate change risk not only in their operations, but also in terms of how it affects them serving their customers and clients and how it affects their balance sheet and capital. The pace of activity will surely quicken in coming years, given the intensifying public demand to act.

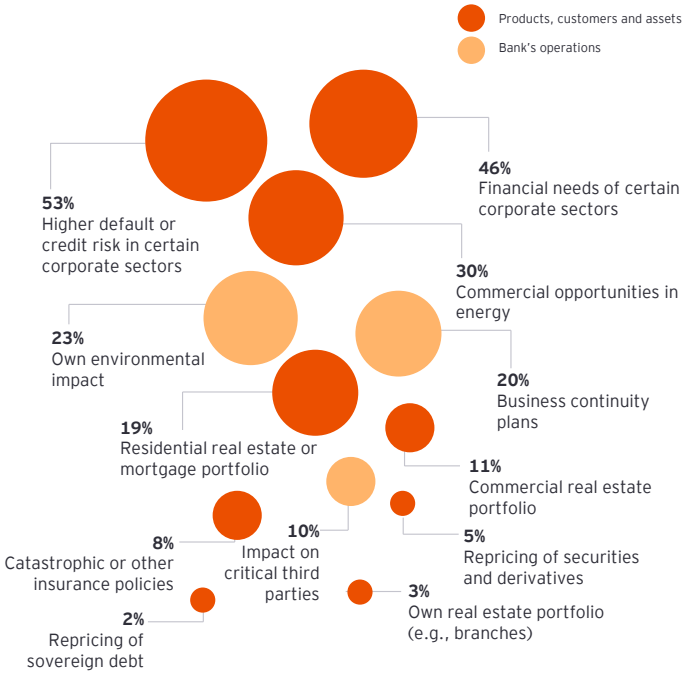
At the center of environmental sustainability

As a result, banks are increasingly under pressure to consider climate change risks, and broader environmental and social risks. Indeed, "rising regulatory impetus and wider societal expectations, alongside our institution's own desire and purpose," have pushed such risks way up the agenda, according to one bank risk officer.

In some ways, banks find themselves in the center of environmental sustainability. Many have significant asset management operations, and in their stewardship role, banks are pushing companies in which they invest to address sustainability, and within that to identify and manage the effects of climate change. In part, this reflects their broader institutional commitments to sustainable business practices and finance, as well as the need to factor in environmental, social and governance (ESG) matters to attract retail and institutional investors who are increasingly attuned to these issues.

More broadly, however, banks are concerned about climate change risks for more commercial and practical reasons. As highlighted in Figure 26, banks acknowledge that climate change will impact their customers and clients directly, as well as their own operations. New commercial opportunities will materialize, as highlighted by the direction of regulators in some countries (such as the UK) to understand and report on both risks and opportunities from climate change.

Figure 26: Most significant likely impacts from climate change



Don't guess, analyze

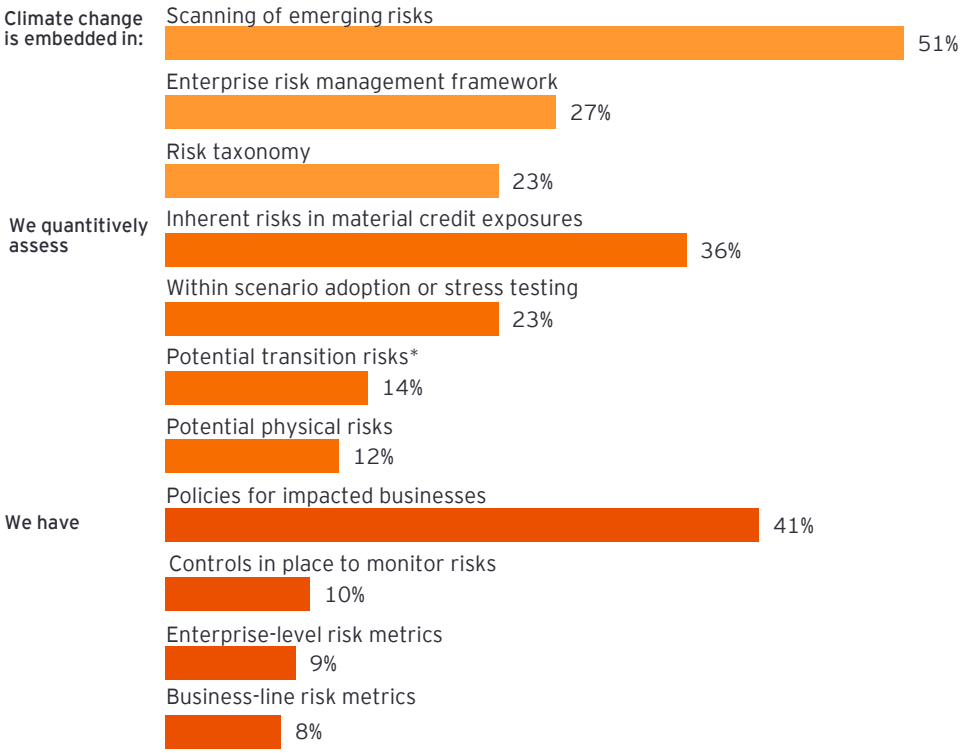
Interestingly, just as insurers are altering their property underwriting policies and pricing in light of climate change, banks are waking up to the fact that they, too, need to consider how climate change affects them. Some banks are investing heavily on their firm-wide climate change strategy.

Banks know deep analysis is required when it comes to such a political and sensitive issue. "It's important to approach this issue in an unemotional way," noted one CRO. Perhaps surprisingly, already, four in five (79%) banks have incorporated climate change into their risk management approach. Half (51%) have built it into their scanning of emerging risks, while two in five (41%) have already adopted policies for impacted businesses.

The most forward-thinking banks have started to build climate change risk into their core risk management capabilities:

- Over a third (36%) have evaluated the inherent risks in material credit exposures and almost a quarter (23%) have built it into their scenario planning for stress-testing purposes.
- Around a quarter have built it into their enterprise risk framework (27%) and risk taxonomy (23%), although only about one in ten have firm-wide (9%) and business-unit (8%) level risk metrics tied to climate change.
- Almost a third (32%) are evaluating the impact on expected credit losses, over a quarter (26%) are determining the impact on capital, and one in five (21%) are focused on the balance-sheet sensitivity changes in external conditions related to climate change.

Figure 27: Ways to incorporate climate change risks into enterprise risk management



*Transition risks of moving to low-carbon economy

The extent to which climate change analysis is embedded in decision-making varies significantly[16]. One executive said, "We address the risk through portfolio analyses and building policies and instructions for the affected areas. Both physical and transition risk are being considered in mitigating climate change risk. In general, climate change risk is being treated as any other risk category, i.e., incorporating it in credit decisions, establishing a scenario modeling, and so on. It is being addressed sector by sector and down to each customer."

The key is getting beyond simple disclosure. Over half of banks (55%) depend on external disclosures to create the necessary governance regimen. But increasingly, banks are enhancing the quality of board and senior-management oversight of climate change, and broader ESG issues. A small minority of banks (8%) even factor climate change into compensation programs.

Getting good data to drive decision-making will prove essential. Official-sector initiatives, such as the Financial Stability Board's Task Force on Climate-related Financial Disclosures and the activities of central banks in the Network for Greening the Financial System, will spur better, more consistent public disclosures. A plethora of private-sector firms are also developing climate change risk or ESG ratings. However, today, the quality of climate change or ESG data is still fairly nascent. As one executive noted, "It is critically important now that we get the right data to enable banks to model and manage the risk, but data sources are not there yet." Another executive agreed, saying, "It is challenging to collect the right data. A lot of ESG-driven measures are still quite fuzzy about data quality."

[16]How can you prepare for tomorrow's climate, today? https://www.ey.com/en_gl/banking-capital-markets/how-can-you-prepare-for-tomorrows-climate-today.

First climate change, then what?

Some banks recognize that climate change is simply the tip of the iceberg. Banks will increasingly be drawn into broader environmental or societal issues.

Climate change is not the only environmental issue that requires attention. Take water shortages. One risk executive, who is worried about operational resilience and the dependence on shared services in certain locations, linked resilience to the broader environmental concerns, "There's a growing water shortage. We may be able to get our staff to work, but what if they don't have immediate access to water? Won't that threaten the practicality of our business continuity plan?"

Beyond environmental matters, there are controversial social issues. CROs highlight that, while climate change may be the most prominent ESG risk at the moment, social risks create, arguably, more challenging issues for banks. A North American CRO pointed to gun control – banks may be able to identify, isolate and potentially cease financing gun manufacturers, but how will they do the same for stores that sell guns? Similarly, given the focus on immigration and more broadly on detention matters, are banks to stop financing commercial prisons?

10 Meeting emerging customer demands for customized, aggregated lifetime offerings

Consumer preferences and buying behaviors for financial products and services are changing. EY NextWave financial services research shows that the average consumer is shifting away from owning and buying, to renting and using. The impact on banks will likely be a shift from delivering and pricing specific products and services, to delivering and pricing a comprehensive bundle of products, services and value-added capabilities.

The pricing model may become subscription-based (i.e., in which financial products are bundled, often with nonfinancial products, and purchased on a per-period subscription basis) versus a flat-fee basis (i.e., in which financial products are purchased on a per transaction or activity basis). These bundled products, services and capabilities will increasingly center on key life events[17] (e.g., getting married, becoming parents), when a complex set of financial needs should be addressed holistically.

This shift to a new model for meeting consumer needs will affect how banks operate and call for new approaches to managing inherent risks.

> "We are trying to change the way we do business in a way that meets customer needs and expectations in the future
>
> – CRO

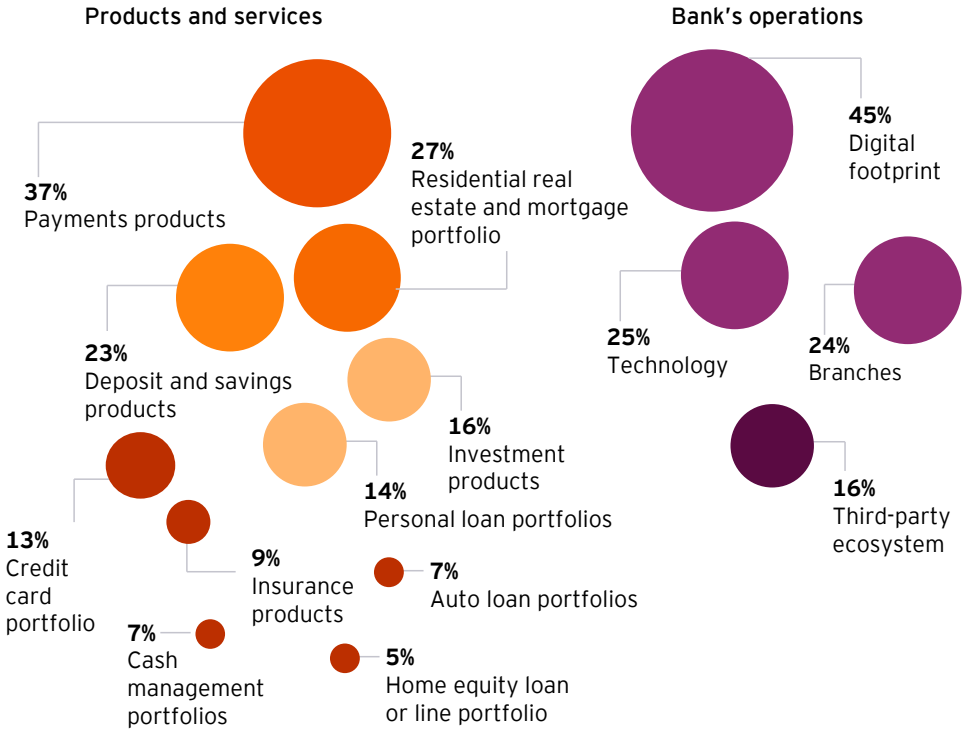
Significant impact on products and operations

Even though the industry is in the early stages of moving toward radically different business and service models based on subscriptions, risk professionals are intuitively aware of the impact of such change.

Figure 28 highlights the most likely affected aspects of a bank. As one might expect, products and services linked to payments and residential real estate will likely be most immediately affected – after all, they have been most swayed by the rise of non-bank or FinTech competitors. Deposit, savings and investment products will also be affected, though less so in the minds of CROs.

Bank operations will also be affected, notably the bank's digital or online operations, as well its technology strategy and branch footprint.

Figure 28: Areas most affected by meeting new consumer needs



[17]NextWave Consumer Financial Services: financial subscriptions are coming https://cdn.foleon.com/upload/3941/nextwave_cfs_research_report_final_april_2019.67be3d331ef6.pdf.

Meeting the challenges head on

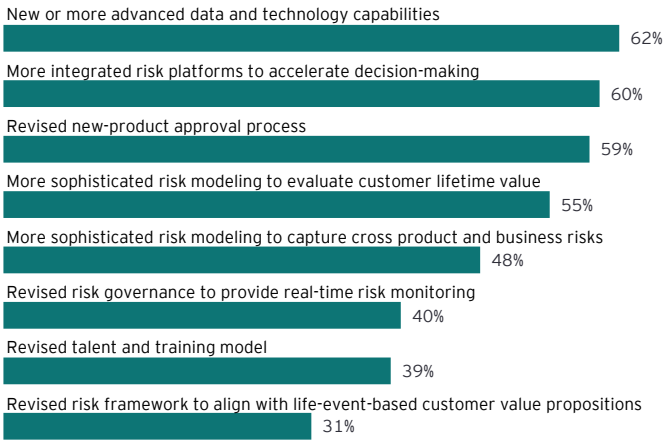
In some ways, the analytical impact on banks is hard to predict. The move to subscription-based models – or anything akin to it – requires bank risk leaders to recommend novel new risks, based on untried business models. Indeed, one executive asserted, "The whole concept of personalization may open a Pandora's box for risk. Are offerings discriminatory if not done the 'right' way?"

Yet, over two-fifths (44%) of risk professionals realize the most pressing challenge will be pricing the service properly, and a third understand that it will be even more challenging to do so over the lifetime of the bundled offering. Some see some embedded risks, such as those associated with compliance (25%) and product-related risks (23%). As a result, some banks highlight challenges related to being transparent to the customer on pricing investments (26%) and to risk to the customer (24%). As one CRO said, "Risks are rising because the tolerance of clients is decreasing. What was acceptable two years ago, no longer is."

New or enhanced risk capabilities will be required

Meeting customer needs in materially different ways will require enhanced or new risk capabilities, as highlighted in Figure 29. First and foremost, it will necessitate data analytics and ways to model customer value over the lifetime of the product or service, and to capture risks across products or associated businesses. Such analysis will need to be incorporated into revised new-product approval processes. Risk monitoring will have to expand, in part to spur faster, more informed decision-making. Training around the risks will need to adapt, as will talent needs.

Figure 29: Potential required changes to risk capabilities



As one CRO put it, the risk dimension of delivering new value to customers in new ways highlights many issues: "How do you make sure the customer is buying the products in the right way? How do you know you are selling it the right way? How do you make sure they are generally reading and understanding the terms and conditions?"

Headlines a decade from now will tell the story

Looking back over the past 10 years, it is comforting to sit back and provide a compelling narrative that bank risk management is vastly better than it was pre-crisis. It doesn't matter whether changes were made to comply with legislation or regulatory and supervisory rules or were voluntary; change was good overall.

Everyone remembers the headlines of a decade or so ago. The media wrote constantly about the industry in unflattering ways. Every week a new blockbuster hit bookstands telling a tale of the run up to the crisis and how it was mismanaged in the early weeks and months as it unfolded.

No one was free from criticism. Politicians, among others, supported growth-oriented fiscal and other policies, and pressed for ever-increasing homeownership, especially in the US. Regulators promoted light-touch regulation. Bank boards of directors inadequately governed management. Senior management was self-interested and compensated simply for growth. Credit rating agencies were complicit in issuing top ratings to complex, esoteric structured finance products. The accounting profession was quizzed on its role.

We have come a long way since then.

As one looks forward, what will headlines involving banking look like over the next 10 years?

Will they be positive? "Bankers help arrest climate change?" "Banks support small businesses, despite months of economic turmoil globally."

Or negative? "Banks have given way to techno-financiers." "AI failed us – banks admit misconduct ran deep in their code." "Yesterday, cyber attackers brought the global financial system to a standstill."

Only time will tell. But, without hyperbole, risk management will play an influential role in determining which set of outcomes is more likely.

Research methodology and participant demographics

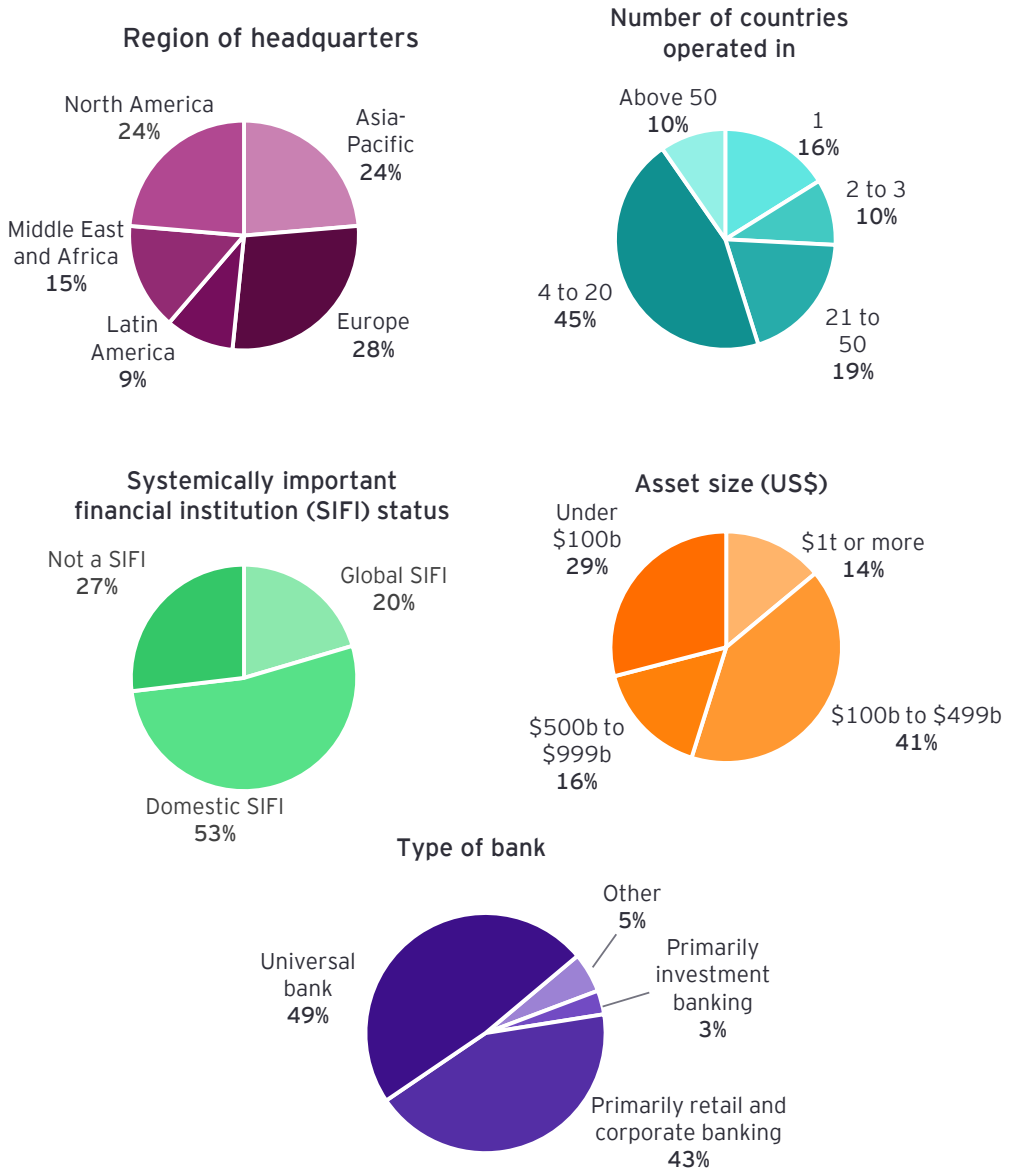
Research methodology and participant demographics

EY, in conjunction with the IIF, surveyed IIF member firms and other banks in each region globally (including a small number of material subsidiaries that are top-five banks in their home countries) from June 2019 through September 2019. Participating banks' CROs or other senior risk executives were interviewed, completed a survey, or both.

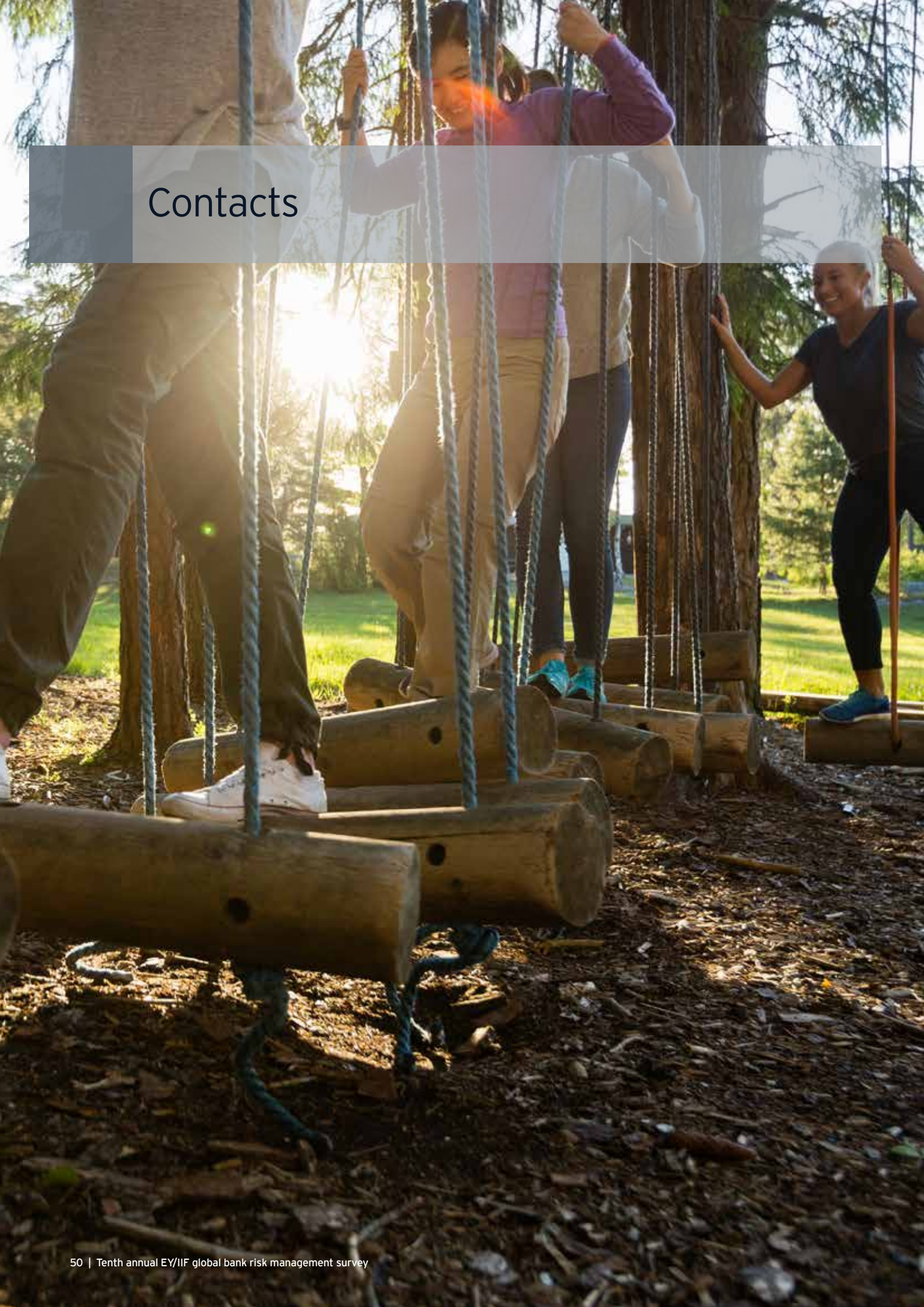
In total, 94 firms across 43 countries participated (up from 74 banks in 2018). Regionally, those banks were headquartered in Asia-Pacific (21), Europe (26), Middle East and Africa (14), Latin America (10) and North America (23). Of those, 19 are globally systemically important banks and 49 have been designated as systemically important domestically. Data in this report relates to the 92 banks that completed the quantitative survey, and the narrative includes insights gleaned from qualitative interviews with some of those and other banks. As shown in Figure 30, participating banks were fairly diverse in terms of asset size, geographic reach and type of bank.

It is worth noting that 21 other financial institutions participated informally by responding to the survey. Their data is not included in this survey report, but directionally it did inform this report's narrative.

Figure 30: Participant demographics



Contacts



EY and IIF contacts

EY

Global

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

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

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

Americas

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

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

Diego Pleszowski
Latam Financial Services Leader
Santiago
diego.pleszowski@cl.ey.com
+569 9321 3284

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

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

Asia-Pacific

Eugène Goyne
Associate Partner, Financial Services
Hong Kong
eugene.goyne@hk.ey.com
+852 2849 9470

Maggi Hughes
Partner, Financial Services
Singapore
maggi.hughes@sg.ey.com
+65 6309 8268

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

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

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

EMEIA
(Europe, Middle East, India, Africa)

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

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

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

Vibhuti Lalloo
Partner, Financial Services Africa
Sandton
vibhuti.lalloo@za.ey.com
+27 76 440 0585

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

IIF

Andres Portilla
Managing Director, Regulatory Affairs
Washington, D.C.
aportilla@iif.com
+1 202 857 3645

Martin Boer
Director, Regulatory Affairs
Washington, D.C.
mboer@iif.com
+1 202 857 3636

Stefan Gringel
Policy Advisor, Regulatory Affairs
Washington, D.C.
sgringel@iif.com
+1 202 682 7456

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. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation is available via ey.com/privacy. 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. 004903-19Gbl
1909-3267866 (BD FSO)
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