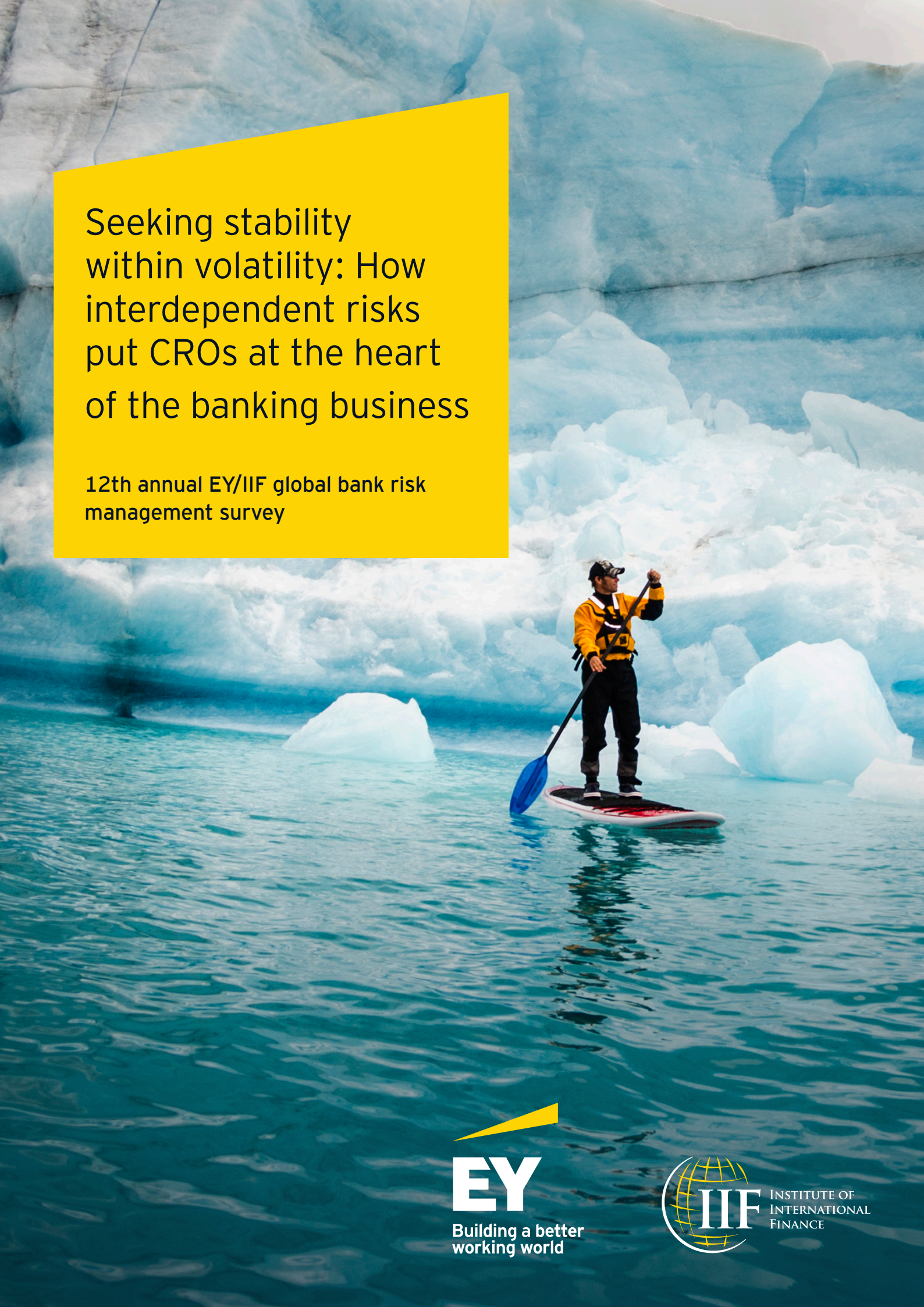
Seeking stability within volatility: How interdependent risks put CROs at the heart of the banking business

12th annual EY/IIF global bank risk management survey



EY
Building a better working world

IIF Institute of International Finance

TABLE OF CONTENTS

Executive summary	04
Chapter 1: External forces and events top the CRO agenda	14
Chapter 2: The digital transformation imperative and other internal pressures present unique and serious challenges	24
Chapter 3: Building a high-performing risk management function	34
Looking ahead: an ever-evolving risk matrix	42
Research methodology and participant demographics	43
Contacts	44

Letter from the authors

This report highlights the findings of our annual global survey of bank chief risk officers (CROs), which EY and the Institute of International Finance (IIF) are pleased to have conducted for the 12th consecutive year. As with past studies, the 2022 results present CROs' views on the most urgent issues facing their organizations, and those that they expect will take on more importance in the next three to five years.

While many familiar risks remain priorities, we detect in this year's results increased complexity caused by overlapping and correlated risks. Consider how the combination of geopolitical and cyber risks threatens operational resilience, while also increasing market risk, particularly for institutions designated as global systemically important banks (G-SIBs). Or how macroeconomic challenges may reveal previously hidden sources of credit risk. The shortage of talent makes it more difficult to manage risks related to data security, consumer privacy, and the use of artificial intelligence (AI) and machine learning. Environmental, social and governance (ESG) strategies, digital transformation and new product development also require multi-dimensional thinking by CROs and fresh approaches to instilling the right controls. And, increased regulatory risk is present in all of these vectors.

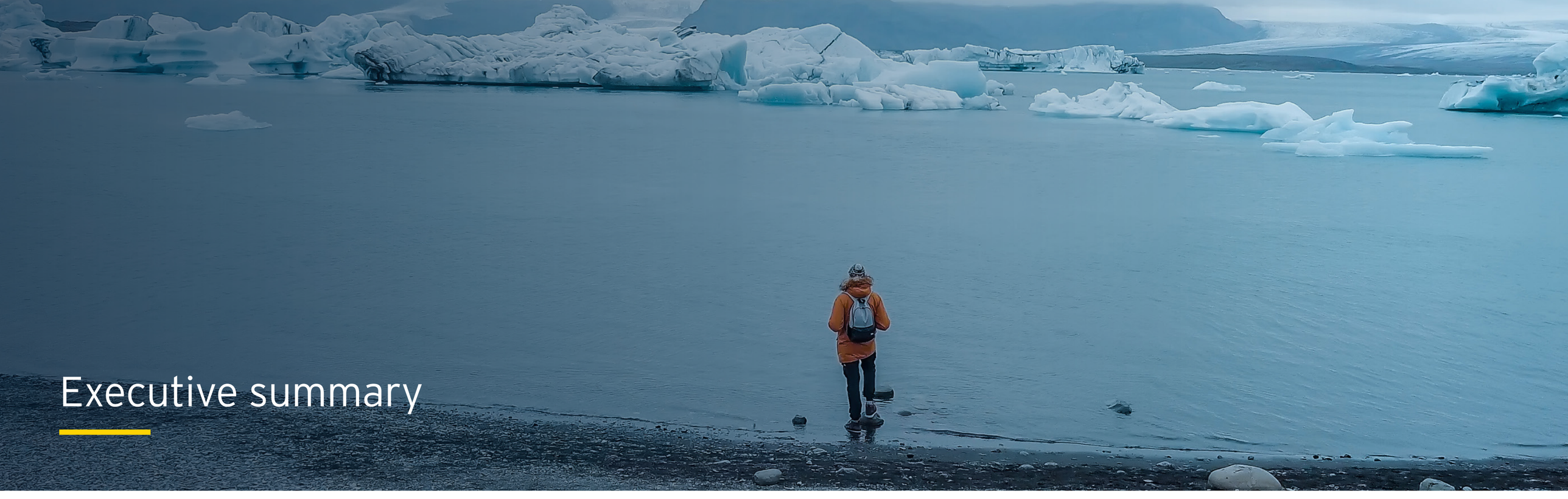
For today's CROs, understanding how intersecting risks can create single or multiple points of failure has become a top priority, even when traditional risk management metrics look stable. Yesterday's compartmentalized taxonomies and more conventional risk modeling processes may not account for the impacts of multiple, simultaneous risk events.

Again, CROs face an extraordinary volume and variety of risks — traditional and emerging, those resulting from external forces and those from internal pressures — nearly all of which seem to be increasing in urgency. That's one reason we believe that in the 20 years since the inception of the CRO role, it has become one of the most difficult jobs in the banking C-suite, a point we've heard directors and senior executives make repeatedly in recent months. New CROs, a significant number of which completed our survey this year, can expect to be challenged constantly.

Yet, to their credit, CROs seem confident that they can build on the momentum of past years to deliver the risk management and resilience that banks need to continue winning over customers, out-performing new and non-traditional competitors, and satisfying the demands and expectations of a variety of stakeholders, including investors and regulators. We hope you find this report to be both insightful and useful. We would be delighted to discuss these results, and their implications for you, in more detail.

Jan Bellens
Global Banking & Capital Markets Sector Leader, EY

Andrés Portilla
Managing Director, Regulatory Affairs, IIF



Executive summary

World events and external forces have complicated traditional risk management categories, expanded responsibilities and rearranged priorities for CROs in the banking industry. The complex interplay between overlapping risks and external and internal forces can result in risk issues moving quickly and in unexpected ways.

Uncertainty and volatility seem to rise in tandem. The sense of "everything happening at once" and the need to look beyond the borders of the bank are driving CROs to find new tools and talent to operate effectively in a highly dynamic risk landscape.

CROs expect to pay the most attention to cyber risk in the next 12 months and during the next three years, particularly as it relates to operational resilience. Also of note, geopolitical risk made the biggest jump up the CRO agenda since last year's survey. Looking ahead, ESG risks, climate risk, and digital transformation risk are also likely to increase the most as priorities during the next 36 months.

The more difficult it is to model a risk and the less clarity there is from regulators, the more challenging it can be to manage. That's especially true when the risks could have serious implications in the immediate term, and when enterprise-level threats transcend traditional risk management disciplines and capabilities. In these situations, banks often decide to hold more capital, which may result in close analysis of return on capital and a careful assessment of business objectives versus risk management goals.

Five key findings from this year's survey

1. Geopolitical risk adds uncertainty to economic turbulence, with varying impacts across regions.

Our results show that CROs continue to pay close attention to the many possible manifestations of geopolitical risk, including economic and market volatility, additional sanctions, increased cyber-attacks from state-sponsored actors and threats to operational resilience. Banks view their geopolitical risk profiles differently, based on their size and operating footprint, with risks materializing from beyond the difficulties arising from the war in Ukraine.

The next year will likely see more formal assessments and extensive risk management activities in the realm of geopolitical risk. CROs are also watching out for more social unrest, in the event that an economic downturn exacerbates rising political tensions in countries around the world.

2. Cyber threats top the agenda, due to their ever-increasing complexity and constant evolution.

Despite billions invested to safeguard core systems and protect vital data assets, CROs consider cyber the top inherent threat and the one most likely to result in a crisis or major operational disruption. Even when they perceive their own internal systems as largely secure, CROs see potential amplifications and concentration of cyber risk lurking everywhere — within geopolitical turbulence, ecosystem strategies and the vast networks of partners, suppliers and vendors on which banks increasingly rely.

The interconnectedness of those networks — and the integrated technology that underpins the entire global financial system — represents a massive attack surface and a huge perimeter to secure. Because bad actors are relentless in seeking vulnerabilities and because successful attacks are so lucrative, it's worth asking if cyber and other threats to resilience will ever recede very far from the top of CRO agendas.

3. Credit risk remains a high priority as banks look out for hidden risks that may materialize in the looming economic downturn.

Given the lessons learned since the global financial crisis and increased capital and liquidity levels, our survey results and discussions indicate that CROs generally are confident in their ability to manage traditional sources of credit risk; after all, credit risk management is a core competency for any bank. However, CROs are notably cautious about the uncertain severity and duration of an economic downturn and "unknown unknowns." Our survey respondents seem to recognize that, when there is broad consensus that core financial risks are under control, the potential for systemic risk may increase.

At the time of the survey, traditional credit risk metrics had yet to show significant deterioration and balance sheets looked strong. But with the macroeconomic developments of subsequent months, including episodic bouts of volatility in financial markets, CROs must continue to challenge their teams to avoid complacency. Certainly regulators are also closely monitoring the effects of an economic downturn on the balance sheets of financial institutions.

Further, CROs must be vigilant in watching for asset class and counterparty vulnerabilities, including from indirect or non-traditional channels (e.g., contagion through connected financial ecosystems, supply chain dependencies, ripple effects from geopolitical events and the build-up of risks in the shadow banking system).

4. From new products and business models to digital assets and ecosystems, customer growth and product innovation strategies demand CRO attention.

Banks are investing in digital transformation to innovate with new products and services, develop new business models and increase operational efficiency. CROs are rightly focused on establishing strong controls for these programs, especially where they involve deep engagement with third parties, such as FinTechs or large-scale ecosystems and platforms with many participants.

But, they should also proactively engage with business leaders in planning and designing transformation efforts to support more risk-informed decision-making and embed controls directly in digital processes. To do so most effectively, CROs will need to transform their own capabilities and teams to be more agile, especially given the pressure to get new products to market faster. CROs that drive such change can play a more enabling role when working with the business, rather than being forced to act as a "toll gate" later in the transformation process.

5. CROs are looking for more adaptable and agile teams to manage risks across the business and boost performance within their own functions.

Scarce talent, rising employee expectations and the post-pandemic shift to hybrid working all contribute to increased talent risk across the business. Thus, CROs must become more expert in human capital issues and engage with chief human resource officers (CHROs) more strategically and frequently on people and cultural matters. Risk organizations are also impacted by these trends and there is pressure to add new capabilities and to strengthen the culture as risk teams take on more responsibility.

Data science tops the list of in-demand skills, but CROs also value agility and adaptability. Specifically, CROs need people who understand the business and can identify correlated vulnerabilities across risk disciplines. While it's too soon to say whether or to what extent a recessionary environment will ease the labor crunch and wage inflation, the effects are expected to vary across global regions.

> "What's expected of the risk function has grown hugely, even in the last year. We are genuinely having to think globally about politics, regulation and extreme events, and model their impacts both in terms of conduct and prudential. Yet, our function has often valued narrow, specialized and deep technical skills. The kinds of people who can balance broad complexity are few and far between.
>
> – CRO survey respondent

Top CRO risk priorities

In the annual "horse race" for the top risk priority, cyber risk edged back ahead of credit risk. That may be due to having strong controls and capital and liquidity reserves in place or because CROs feel they have done more to address credit risk during the last dozen years. Credit risk may soon become more of a focal point if economic conditions worsen.

The fluctuating positions of digital risk and regulatory risk during the last five years show just how fluid the CRO agenda has been in terms of the most urgent priorities. While these topics are always important, in some years they become slightly less urgent as other issues push them down the agenda. The cluster of issues in the next tier following cyber and credit risk demonstrates the complex matrix of interconnected risks facing CROs today.

Figure 1: Top 10 CRO priorities 2012–22

Rank	2012	2013	2014	2015	2016	2017	2018	2019	2020–21	2022
1	CRE	CRE	CRE	REG	REG	CY	CY	CY	CRE	CY
2	LIQ	RA	RA	RA	CY	REG	CRE	CRE	CY	CRE
3	RA	REG	OR	CRE	CRE	CON	REG	DIG	CLI	ENV
4	MR	OR	REG	OR	RA	CRE	OR	CON	DIG	REG
5	REG	LIQ	RC	CAP	OR	OR	TECH	REG	RES	RES
6	TECH	CAP	CAP	LIQ	TECH	CUL	CON	OR	REG	DIG
7	STR	MR	MR	TECH	STR	TECH	RA	CUL	OR	GEO
8	CAP	STR	LIQ	STR	CON	ERM	BM	PRI	BM	OR
9	RC	TECH	STR	MR	CUL	RA	CUL	RES	ER	RA
10	OR	RC	TECH	CY	ERM	STR	STR	MO	RA	LIQ

Key

Financial risks

- CAP Regulatory capital management
- CRE Credit
- LIQ Liquidity
- MR Market risk
- MO Model
- REG Regulatory implementation
- STR Stress testing

Non-financial risks

- BM Business model
- COM Compliance
- CON Conduct
- CUL Culture
- CY Cybersecurity
- DIG Transition to digital strategies
- ENV Environmental
- ER Employee-related risks
- ERM Enterprise risk management
- GEO Geopolitical risk
- OR Operational
- PRI Data privacy
- RA Risk appetite
- RC Risk controls
- REP Reputation
- RES Operational resilience
- TECH Risk technology architecture

Top 10 CRO risk priorities for the next 12 months

It's notable that 83% of G-SIBs in our survey ranked geopolitical risk as the top threat, followed by environmental and credit risk, both at 58%.

Nearly two-thirds (62%) of CROs for European banks chose geopolitical risk as a top priority, far more than their counterparts in the Asia-Pacific region (28%) and North America (17%). Exactly one-third of our survey respondents from Asia-Pacific chose stress testing and more than a quarter (27%) from Latin America chose model risk, much higher percentages than their peers in other regions.

Evolving board risk priorities

CROs believe they are largely aligned to board-level views of risk priorities. They are more concerned about operational resilience and regulatory implementation and are slightly less worried about geopolitical risk than they perceive board directors to be. While CROs rank liquidity risk as their 10th highest priority, they think boards would put capital risk in that position.

Figure 2: Top 10 Board priorities 2013–22

Rank	2013	2014	2015	2016	2017	2018	2019	2020–21	2022
1	RA	RA	COM	REG	CY	CY	CY	CRE	CY
2	LIQ	COM	RA	CY	REG	REG	CRE	CY	CRE
3	REG	LIQ	CRE	RA	BM	RA	DIG	DIG	ENV
4	CAP	CAP	LIQ	CUL	RA	CRE	CON	CLI	DIG
5	OR	OR	CUL	CRE	CRE	CON	REG	BM	CUL
6	STR	STR	CON	CON	CUL	OR	CUL	RA	GEO
7	ERM	REP	OR	CAP	CON	BM	OR	RES	REG
8	CUL	CON	CAP	STR	REP	REP	BM	REP	RES
9	TECH	CUL	TECH	OR	OR	CUL	RES	REG	OR
10	REP	ERM	STR	TECH	STR	CAP	RA	GEO	CAP

*CROs' views of boards' priorities

Key

Financial risks

- CAP Regulatory capital management
- CRE Credit
- LIQ Liquidity
- MR Market risk
- MO Model
- REG Regulatory implementation
- STR Stress testing

Non-financial risks

- BM Business model
- COM Compliance
- CON Conduct
- CUL Culture
- CY Cybersecurity
- DIG Transition to digital strategies
- ENV Environmental
- ER Employee-related risks
- ERM Enterprise risk management
- GEO Geopolitical risk
- OR Operational
- PRI Data privacy
- RA Risk appetite
- RC Risk controls
- REP Reputation
- RES Operational resilience
- TECH Risk technology architecture

While CROs believe boards have confidence in the controls to protect against credit risk, they may have underestimated directors' rising concern about the impact of a recession. Three out of four CROs at G-SIBs say geopolitical risk is the top issue for boards, followed by environmental risk and cybersecurity, both at 58%. European CROs see their boards as much more focused on credit risk (77%) and geopolitical risk (62%).

Top 10 board risk priorities for the next 12 months (according to CROs)

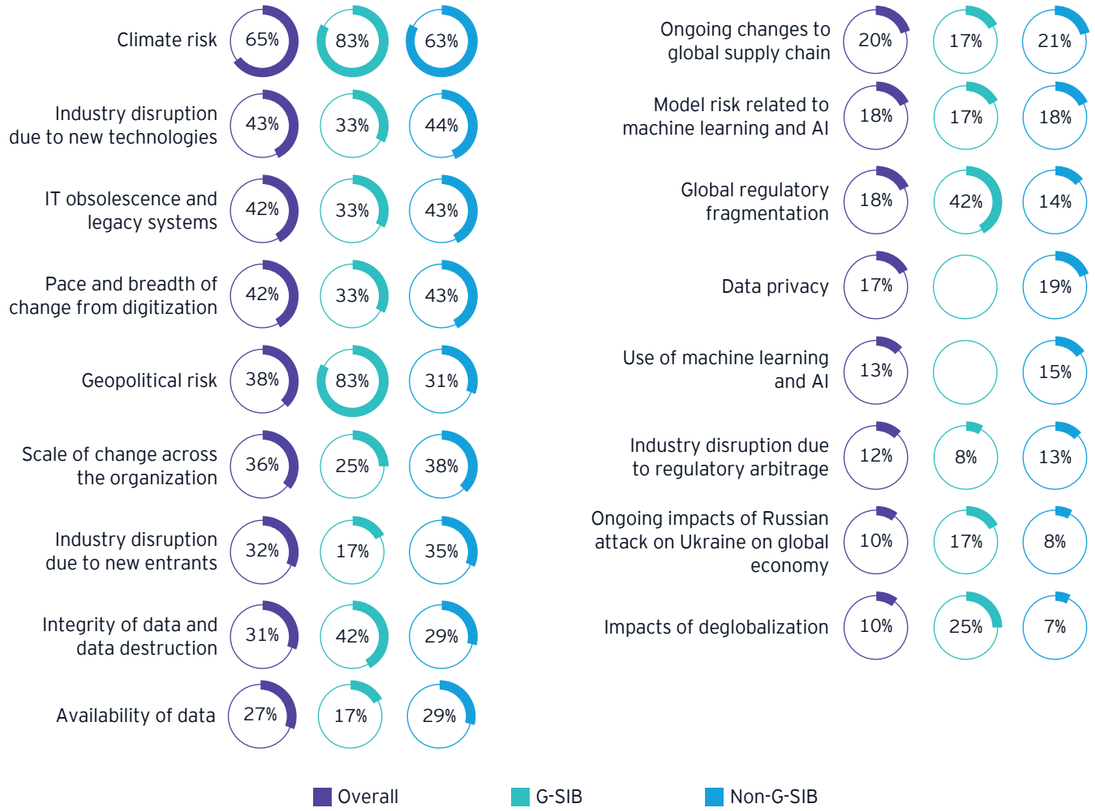
Most important emerging risks over the next five years

Looking ahead, CROs say they will largely focus on the same risks as their regulators, though priorities diverge significantly when it comes to tech-driven disruption, IT obsolescence and data privacy. Here again, CROs at G-SIBs are significantly more focused on geopolitical risk and regulatory fragmentation than their peers at smaller organizations and more so than they perceive regulators to be. CROs say they will prioritize risk from new technologies and digitization to a greater extent than regulators, whom they expect to focus on data privacy and other data issues. Interestingly, no G-SIB CROs selected data privacy as a relatively important emerging risk. *See figure 3.*

Looking at the regional views, concern about climate risk is highest among CROs in Asia-Pacific (89%) and Europe (77%) and lowest in Latin America (40%). North American CROs are most concerned about the scale of organizational change (67%), climate risk (57%) and the pace and breadth of digitization (53%).

Figure 3: Top emerging risks during the next five years

Q What five emerging risks do you believe will be most important for your organization over the next five years?

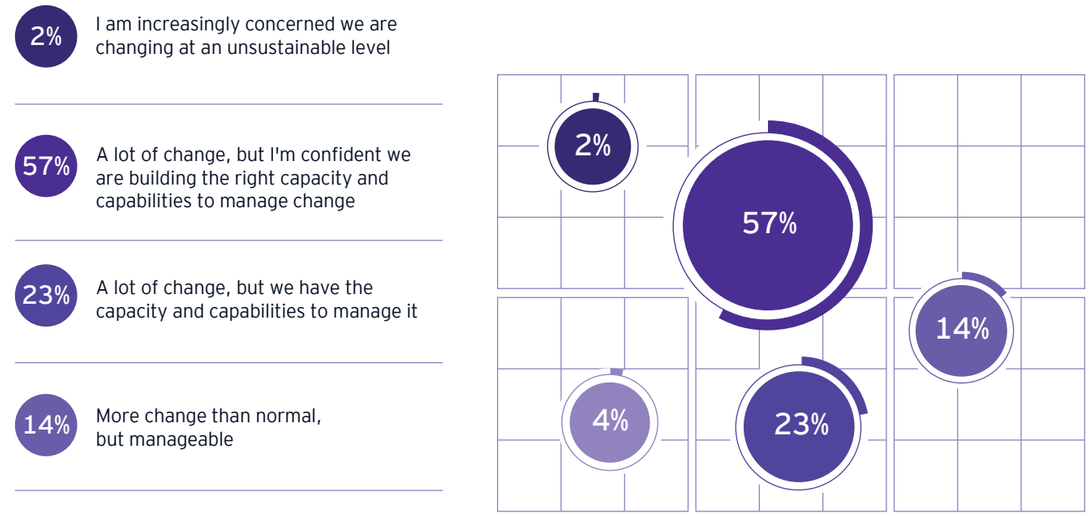


CROs on the level of change in their organizations

CROs seem largely confident in managing the pace of change in their organizations. That is a testament to a decade of progress in establishing robust controls, building new capabilities and engaging more broadly in strategic discussions. The most confident CROs are in Europe (69%) and Asia-Pacific (67%) and the least in North America (53%) and the Middle East/North Africa (44%). *See figure 4.*

Figure 4: Amount of organizational change

Q How would you characterize the level of change occurring in your organization?



Chapter

01

External forces and events top the CRO agenda

When considering their banks' most significant vulnerabilities, CROs are most concerned about large-scale external events and forces occurring outside the boundaries of the bank that are largely beyond their control. Threats to operational resilience, including cyber threats and geopolitical risks, are among the top priorities, as are the credit risks caused by macroeconomic uncertainty. Banks have made extensive preparations for a huge range of possible scenarios, but unknown and highly complex scenarios – those that currently seem unimaginable – may pose the greatest systemic risk.

The ubiquity of cyber threats

CROs see cyber risk everywhere, as our survey results amply demonstrate. It's inherent to every line of business, in day-to-day operations and key strategic change programs, and across extensive networks of partners, suppliers and service providers on which banks increasingly depend. Furthermore, rising regulatory interest and the likelihood of new standards add to the agenda of every CRO.

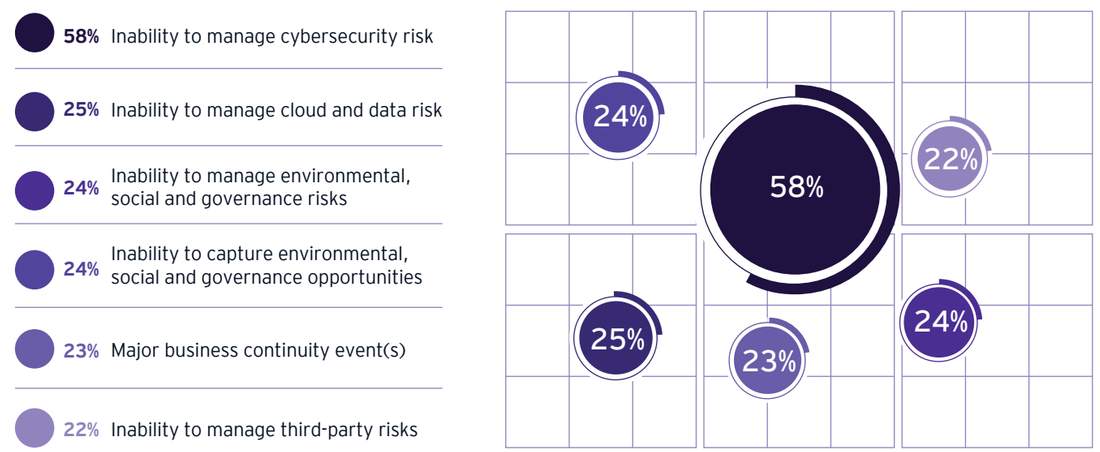
The increasing sophistication of hacking tools and techniques and the ever-expanding attack surface from increasingly digitized operations amplify cyber risks. There is internal complexity to manage when CEOs may not be fully familiar with existing cyber controls and board directors have only limited understanding of the risks; in fact, CROs must often explain and interpret the detailed reports provided by the chief information security officer (CISO).

As with other non-financial risks, cyber risk causes more concern because CROs can't see or manage all the vulnerabilities, particularly those associated with third parties. Then there are the difficulties of ensuring bank employees don't open the door to attack; for all the high-tech tools attackers have, human error is still a prevailing factor in the majority of breaches.

Cyber risk is prominent on both short-term and long-term agendas. That our survey respondents overwhelmingly chose their inability to manage cybersecurity risk as the top strategic risk for the next three years suggests that the presence and urgency of cyber risks won't be falling down the CRO agenda anytime soon, if ever. *See figure 5.*

Figure 5: Top strategic risks over the next three years

Q What are the top strategic risks that concern you over the next three years?



For the largest global banks, with the most robust security models and sophisticated detection and response capabilities, the primary threat is from well-funded, state-sponsored attacks using the most advanced techniques. Regional banks and smaller institutions are less likely to see attacks from state-affiliated groups seeking to disrupt the entire system, but they may be more exposed because attackers rebuffed by effective security at one firm simply move on to the next target.

Cyber has become so pervasive that some CROs are looking to shift away from siloed units of cyber-focused competencies and instead embed cyber expertise in every risk stripe and across all risk management programs. They are also adopting more powerful technology to fight back; 35% of CROs say they are using AI and ML to identify cyber attacks. That's a good thing, because regulators are increasingly turning their attention back to cyber following the pandemic, which placed a premium on operational resilience and business continuity planning.

CROs may feel heartened that the damage from cyber attacks on Ukraine has so far been less devastating than expected. The same is true of attacks on the vital infrastructure — including financial services systems — of countries supporting Ukraine. The country's strong reserve of cyber talent was aided by exchanging information with both the private sector and intelligence agencies, highlighting that cybersecurity requires high levels of cooperation and collaboration.

Credit risk in context

At the time of the survey, most banks felt good about the quality of the loan portfolio and stability of the most traditional measures of credit risk. The strong controls that have been established in the 15 years since the global financial crisis have clearly served banks well and bolstered confidence among boards and senior leaders. But, the declining macroeconomic environment globally will likely have CROs thinking more about credit and other financial risks than they have recently, with an emphasis on addressing hidden sources of risk.

> "I am not currently too fussed about credit risk. Will credit risk deteriorate somewhat? Sure, but it's unlikely to be a catastrophe or a crisis. I think we have learned enough as an industry through the financial crisis. Financial risk is not going to be the next big problem.
>
> "Our credit policy is strong but other areas of the business need to better understand the bank's risk appetite.
>
> — CRO survey respondents

Traditional on-balance sheet credit risk (e.g., probability of default) is generally well known, though risks associated with loss given defaults can be more difficult to evaluate. That's why, as the recessionary environment worsens, prudent CROs will look deeper at "known knowns," evaluate "known unknowns" more extensively, and look into hidden credit risks lurking in the shadow banking system and beyond. These risks may include:

- Leverage in private markets
- Bridge financing
- Markdowns on collateralized loan obligations and similar financial instruments

Beyond the shadow banking system, CROs will also be monitoring asset class and counterparty vulnerabilities, including those that could emerge from indirect channels, including:

- Connected financial ecosystems
- Ripple effects from geopolitical events
- Supply chain dependencies

Complacency risk is also worth mentioning, if only because it's on the mind of some prominent regulators who maintain that systemic risk often increases in tandem with confidence in controls. Ongoing macroeconomic decline and periodic market volatility will inspire CROs to remain vigilant against complacency risk, both within their own teams and across the business.

In gaming out worst-case scenarios, CROs should recognize the loss of organizational knowledge relative to credit risk. Many experienced leaders who were on the front lines of the last financial crisis have retired or moved on. While banks have established strong controls in the last decade and have become much more resilient, for some CROs and risk teams, the next financial crisis may feel like their first.

The difficulty of identifying and managing geopolitical risks

Russia's invasion of Ukraine in February 2022 pushed geopolitical risks to the forefront for global banks. But it is far from the only geopolitical risk. Simmering US-China tensions, regional conflicts and the retreat from globalization — or "slowbalization" — are now part of risk appetite discussions. The largest global banks are reassessing market risk and rethinking where to make new business investments.

These risks are unique as they have tangible impacts (e.g., the effort required to comply with more sanctions) but also present great uncertainty, which forces banks to determine their comfort levels with factors beyond their immediate control.

Geopolitical risks complicate and amplify other risks and CROs are all too aware of their significance:

62%

62% of respondents said geopolitical risks would have a "much more significant" or "somewhat more significant" effect on their organization during the next year; for G-SIBs, that number was 84%.

45%

45% said market volatility from geopolitical risk would have "major" or "moderate-to-high" impact on exposure to market risk.

31%

31% of all respondents, but only 8% of CROs at G-SIBs, said foreign exchange rate volatility would have a "major" or "moderate-to-high" impact on their exposure to market risk.

Social unrest and domestic politics are related concerns. These topics have come up more frequently in our recent engagement with CROs, senior executives and board members. "In the political arena, patience seems to be in short supply as polarization increases," one US-based CRO told us recently. "The low appetite for cooperation across the aisles and the nature of the political environment can be more cause for concern than the business impacts of the political topic of the day." We have heard similar sentiments from European executives.

Geopolitical risk often manifests in the form of increased cyber attacks, which is the biggest worry for CROs; the number of CROs citing such attacks as the top geopolitical risk jumped from 39% in last year's survey to 62% this year. Some banks are assessing where to re-locate security operations centers and whether to move operations out of Eastern Europe and other potentially vulnerable regions.

Here again, G-SIB CROs have different concerns; 58% selected the changing role of China as the top geopolitical risk and only 50% chose escalating cyber attacks. European banks are more focused on the war in Ukraine, understandably so. *See figures 6, 7.*

Other variations in our data highlight the way that geopolitical risk plays out regionally, even locally. For instance, North American CROs are more concerned about cyber warfare between nation states (70%) than their peers in Europe (46%). CROs for banks in the Asia-Pacific region are by far the most focused on changes in the global trade environment (67%) and China's changing global role (78%).

Figure 6: Top geopolitical risks impacting your organization over the next year

Q What are the top geopolitical risks that will most affect your organization over the next year?

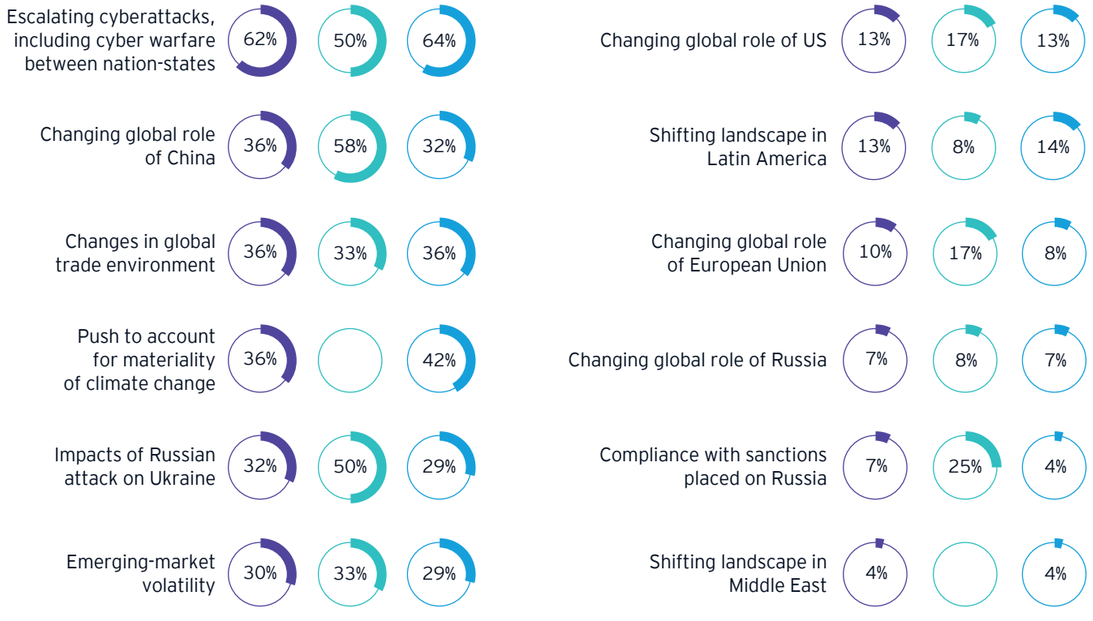
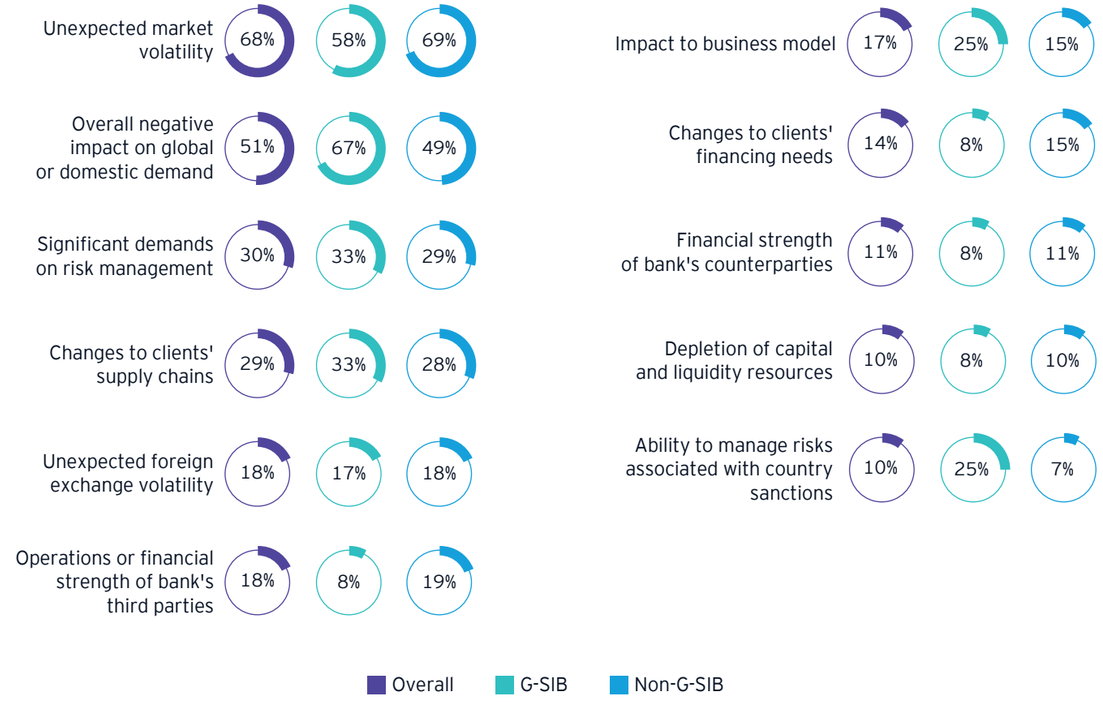


Figure 7: Top impacts of geopolitical risks

Q What are the top ways your organization could be affected by geopolitical risks?



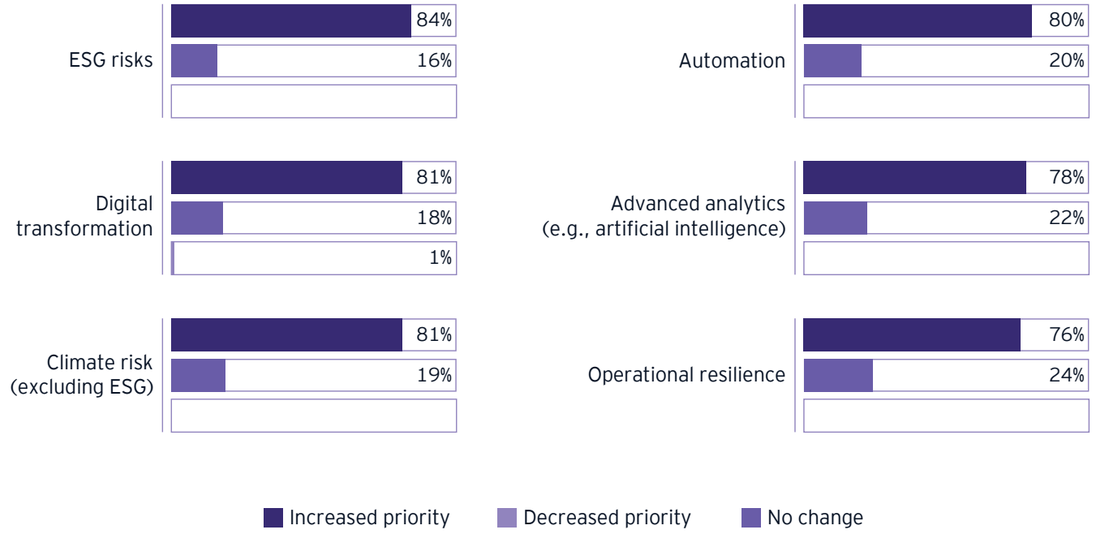
Climate and environmental risk

Though the pandemic and geopolitical concerns have generated more headlines during the last few years, climate risk remains a top-three risk for both boards and CROs over the next 12 months. In this year's survey only 36% of CROs cited environmental risk as a top-five issue that will demand CRO attention during the next 12 months, versus 49% of last year's respondents. This drop is likely a function of the nearer-term urgency around cyber and geopolitical risks. It's also worth noting that 58% of CROs at G-SIBs selected environmental risk as one of their top-five focal points.

However, looking ahead, CROs expect ESG, digital transformation and climate risks to see the greatest increase in priority during the next 36 months. *See figure 8.* Clearly, climate and environmental risk, in its multiple forms, is still on the minds of CROs and the severity and frequency of natural disasters is likely to keep it there. The war in Ukraine also raises environmental questions relative to the European energy mix, and the necessity of expanding fossil fuel usage. For CROs, the focus will continue to be on developing better measures and models of climate risks (including both physical risks and those associated with the transition to a greener economy) for the purposes of more effective credit underwriting.

Figure 8: Risk areas likely to increase most in priority in the next three years

Q For each of the following risk focus areas, indicate whether it will increase in priority, decrease in priority, or there will be no change in the next three years.



Our survey results make clear how much work remains for CROs. A full 84% of survey respondents said their banks had either a "preliminary understanding" (51%) or "somewhat complete understanding" (33%) of climate exposures. *See figure 9.*

Figure 9: Maturity of understanding of climate risk exposure, including both physical and transition risks

Q How would you characterize the maturity of your understanding of your exposure to both climate-change physical risks and transition risks?

Not surprisingly, G-SIBs have more robust capabilities for incorporating climate factors into risk management activities. For instance, 92% cite scenario modeling and stress testing as important activities for incorporating climate risk into their broader risk management approach, compared to 28% of other banks. And half of CROs at G-SIBs say climate change risks are inherent in assessments of material credit exposures, compared to one-third of other banks.

Looking over a five-year horizon, 65% of CROs cited climate risk as the most important concern for their organizations, well ahead of tech-driven disruption (42%), IT obsolescence (42%) and the pace and breadth of change from digitization (42%). The implication is that these latter risks seem more manageable for CROs, compared with environmental risks, which include both physical threats and the disruptions caused by the transition to a greener economy.

Figure 10: Maturity of second-line climate-risk risk management teams

Q How would you characterize the maturity of your second-line climate-risk risk management team?

Further, future activities will certainly include responses to new regulatory requirements, especially in the US; the Office of the Comptroller of the Currency (OCC) is expected to update its draft Principles for Climate-Related Financial Risk Management for Large Banks. Proposals from the Securities and Exchange Commission (SEC) have led finance and risk teams to collaborate on reporting voluntary disclosures. In other words, CROs won't be acting alone in addressing the regulatory dimensions of climate risk.

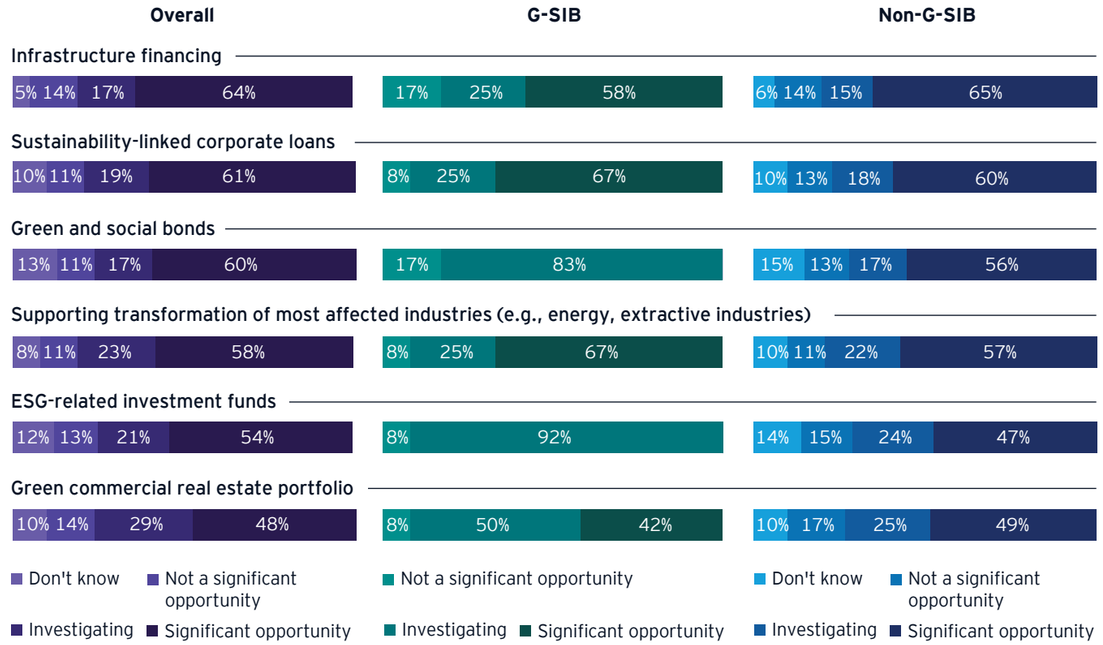
Satisfying regulatory requirements and maturing capabilities: Similarly, 71% expect climate risk to be a concern for regulators during the next five years, well ahead of concerns related to data privacy (40%) and the pace and breadth of digitization (37%).

Given the far-reaching nature of climate risk, it's no surprise that nearly half of CROs expect climate risk to become a bigger priority during the next three years. Banks are taking a range of actions; almost half (48%) of all banks and a full three-quarters of G-SIB CROs say they are building out their climate risk teams. *See figure 10.* We would also expect that most of the 31% still assessing their needs will eventually determine they need more dedicated resources.

The upside of ESG: While climate risk is primarily viewed as an external threat, CROs also view it through the lens of ESG initiatives, which extend from reporting requirements to new product development. CROs see infrastructure financing, sustainability-linked corporate loans and green and social bonds as the products offering the most potential for ESG-related growth. *See figure 11.* G-SIBs see much greater potential with green bonds and ESG investment funds.

Figure 11: Products with the most ESG-related growth opportunities

Q Which products do your firm view as having growth opportunities associated with ESG?

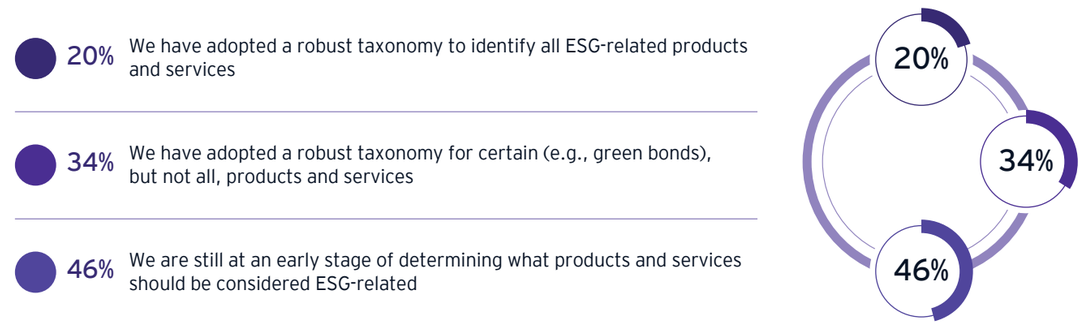


The primacy of infrastructure financing highlights how the transition to a lower-carbon economy is on the minds of CROs and banking leaders in general. Product priorities will evolve based on regulation, as well as perceptions of which green offerings can make a meaningful impact on financial performance. These considerations will vary based on region and organizational size and structure.

Our results indicate that there is work left to do in designing robust taxonomies and monitoring approaches for ESG products. *See figure 12.* These measures will be especially important for banks to navigate rising regulatory interest in ESG products and to avoid charges of greenwashing.

Figure 12: Current approaches to tracking risks related to ESG products and services

Q How confident are you that your bank has a robust approach to tracking which products and services should be considered ESG-related?



Chapter

02

The digital transformation imperative and other internal pressures present unique and serious challenges

Just as different types of external risks are increasingly correlated, internal risks also commonly overlap. And though CROs typically have more urgency in addressing internal risks, they must also consider these complex linkages and intersections.

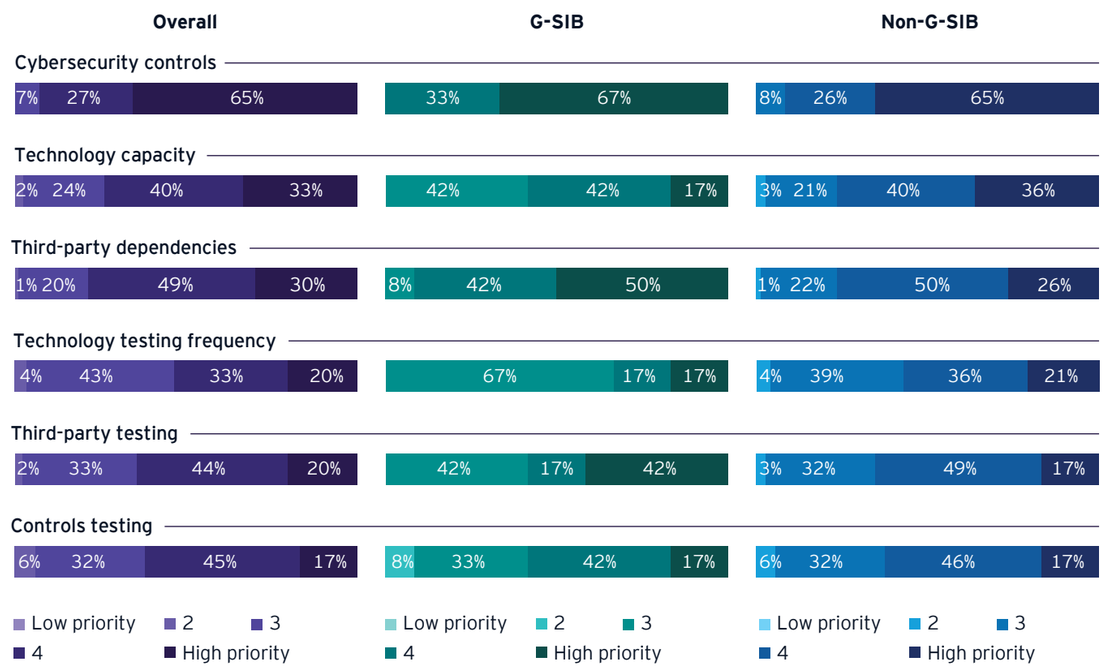
The many forms of operational resilience

It's a good thing banks have worked and invested to boost their operational resilience in recent years, because there are more threats to it than ever. Thus, CROs now take a comprehensive view of operational resilience, from cyber and tech-related concerns to third-party risks.

Cyber controls are the top priority for boosting operational resilience, followed by technology capacity and third-party dependencies. More G-SIB CROs (50%) consider third-party dependencies a higher priority than their counterparts at mid-sized banks (26%). *See figure 13*. That's no surprise in light of larger banks' increased dependence on ecosystems and other partnerships. As mid-sized banks look to expand their use of outsourcing in the future, their concerns about resilience relative to third-parties may rise.

Figure 13: Priorities for operational resilience enhancements over the next three years

Q What level of priority would you assign to each of the following areas of operational resilience for enhancements over the next three years?

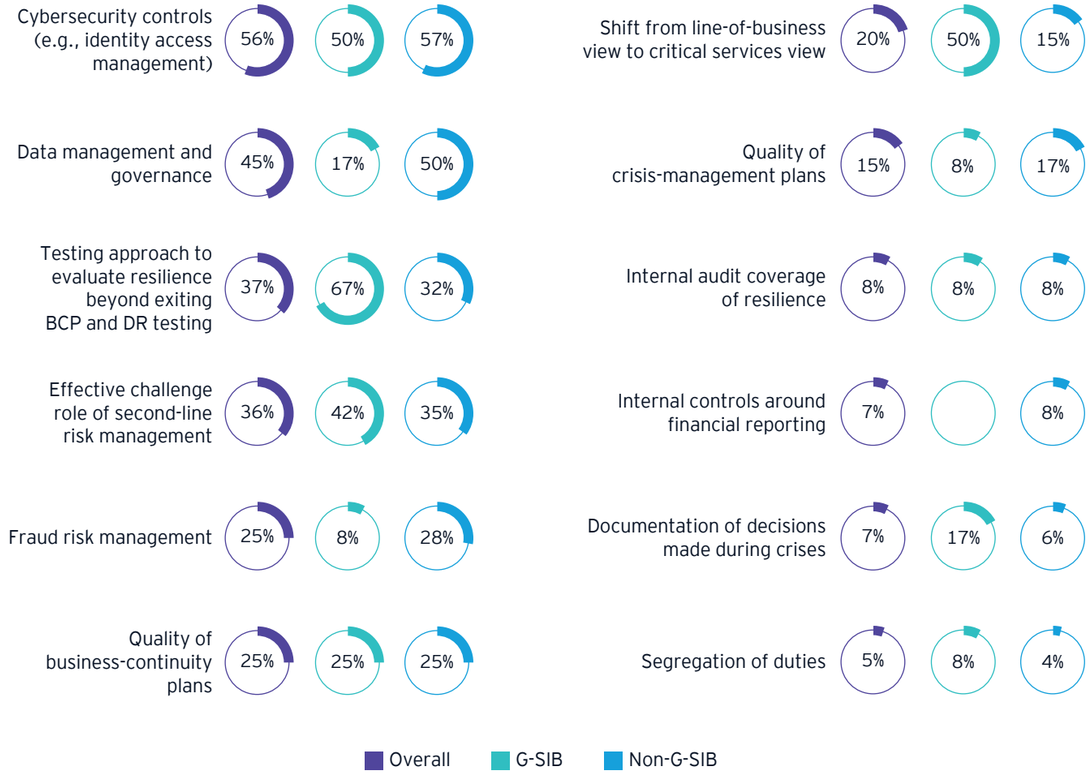


Cybersecurity also tops the list of areas for enhancements to the risk control environment that CROs expect to make. That's true for all types and sizes of banks, though other differences emerge in our research findings. For instance, 50% of mid-sized banks prioritize data management and governance, while only 17% of G-SIBs do. Larger global banks may have already made these vital investments, and their regional peers may be looking to them for lessons learned and leading practices.

Conversely, G-SIBs are much more likely (50%) to prioritize the shift away from line-of-business views than mid-sized banks (15%). The implication is that bigger banks may be following a risk-based approach when it comes to strengthening the control environment. *See figure 14.*

Figure 14: Priorities for control environment enhancements to strengthen operational resilience

Q Which enhancements do you plan on making to your control environment to strengthen operational resilience?



New controls may be required to upgrade protections for tech infrastructure. Many existing policies were designed for physical attacks, having been established after the 9/11 attacks in 2001. With cyber risks now a top priority, business continuity plans need to be updated regularly to ensure back-up and recovery processes can withstand attacks and prevent new vulnerabilities.

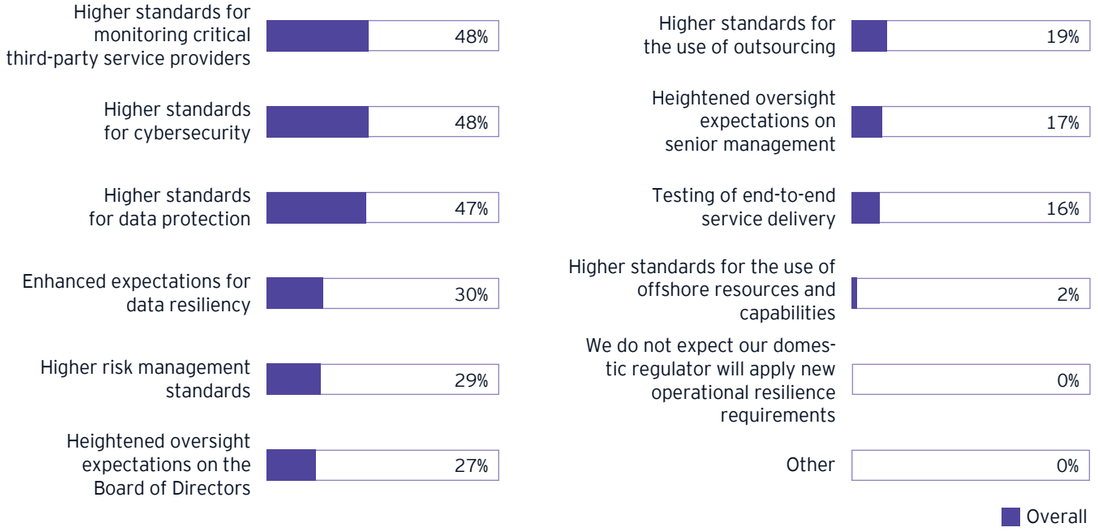
Third-party risk management is something of an evergreen priority, though it's far from a static discipline. High-profile attacks that exploit weak links in supplier networks or the value chain tend to move third-party risk up the agenda. The increased digitization and the interconnectivity of the banking business make third-party risk a major threat to operational resilience for every firm that engages in the broader financial ecosystem.

If they needed any more reason to focus on operational resilience, nearly half (48%) of CROs expect additional requirements for monitoring third-party service provider, alongside regulators raising their standards for cybersecurity in the next two years (48%) and higher standards for data protection (47%). *See figure 15.*

> "Operational resilience is key but most banks still struggle with it because it's complicated and a moving target. Regulators are turning up the heat and expect us to be perfect in the delivery of consumer services.
>
> – CRO survey respondent

Figure 15: Additional operational resilience requirements expected from regulators during the next two years

Q What additional operational resilience requirements do you expect your regulator(s) to impose over the next two years?



The higher cost of controls: Given the expanding need for more robust controls, it's no surprise that 85% of respondents expect the cost of controls to go up in the next three years; nearly a third (32%) expect increases of greater than 15%. Last year only 69% of CROs said they expected higher costs and a significant percentage of respondents expected a decrease, perhaps due to increased automation.

The expected rise in the cost of controls can be partially attributed to risk management's expanding remit and ever-lengthening list of responsibilities. However, the prospect of job cuts and other cost-reduction efforts in the event of a prolonged economic downturn may prevent further investment in controls or indeed the risk management function as a whole.

According to CROs, new regulations and supervisory expectations (56%), accelerated technology transformation (56%) and more extensive cybersecurity (53%) are the main drivers of the cost increases. Notably, last year's top cost driver (the need to automate manual processes) fell to fourth this year, at 40%, down from 76% in 2021's survey. The implication is that automation investments have already been made. But, banks may be coming to realize that lower costs from automation may not compensate for the need to invest in new capabilities, more staff and more robust controls.

The growing risks of necessary transformation programs

Banks are looking to digital channels for both future growth and increased operational efficiency, which explains the vast scope and rapid pace of transformation programs across the business. These programs are also essential to product and service innovation and the development of new business models. As such, digital transformation is an opportunity for CROs to engage with business leaders in a more enabling — rather than restrictive — fashion.

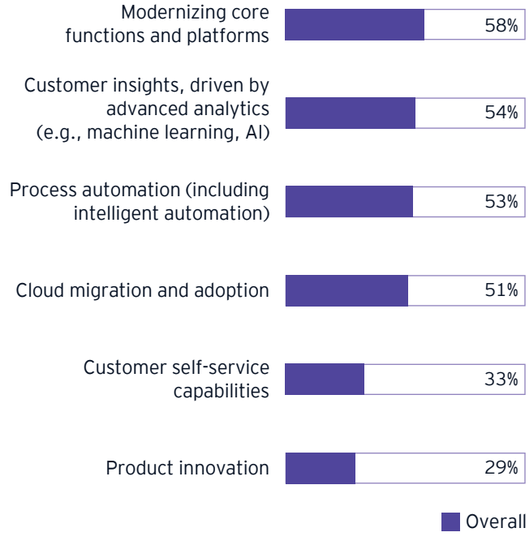
For instance, CROs can seek to embed risk measurement, monitoring and controls directly into processes in ways that don't compromise efficiency or the customer experience. Collaborating with the business to plan transformation programs or design new offerings also presents CROs with an opportunity to demonstrate their knowledge and perspective on upside risk.

To accelerate digital transformation, banks will focus on modernizing core platforms, generating customer insights, automating more processes and moving more operations to the cloud. *See figure 16.*

CROs in Latin America report that their banks are prioritizing customer insights (80%) and cloud migration and adoption (80%) over modernizing core platforms (33%).

Figure 16: Top ways digital transformation will accelerate in the next three years

Q What are the top ways your bank will accelerate digital transformation in the next three years?



As clear and compelling as the business case is, these initiatives also present new risks that should be on CRO radars. Our results show CROs paying a great deal of attention to digital transformation efforts, with an emphasis on establishing the right controls, especially relative to digital asset strategies.

Patience with digital assets: CROs seem to be in "wait-and-see" mode relative to digital asset strategies, a posture that largely mirrors that of management. Nearly half (49%) of banks are still defining their digital asset strategies. Beyond G-SIBs, relatively few organizations have begun executing their plans.

	All respondents	G-SIBs
Enabling digital asset purchases	19%	33%
Processing digital asset payments and settlements	15%	42%
Facilitating digital asset investments	14%	33%
Supporting industry efforts to improve acceptance of digital assets	13%	42%

The implosion of large crypto exchanges in the Fall of 2022 served as a reminder of the need for robust risk management practices at digital-native firms, FinTechs and all non-traditional financial services firms. The regulatory uncertainty will remain a formidable barrier to more activity and solution development, even if CROs recognize that the business will be attracted to the transformative potential of distributed ledger technology to streamline key back-office processes.

Still CROs understand that they'll need to take action on several fronts — including policy, technology, training and talent — when digital assets eventually become a more common feature in banking portfolios. Nearly all CROs at G-SIBs expect such changes. *See figures 17, 18.*

> "We could play in the [digital asset] space but the regulators are unfamiliar. We will stay out of it until we have a good understanding of what we can do with it as a bank and what is an appropriate service or solution to offer our customers and that our regulators will be comfortable with.
>
> — CRO survey respondent

Figure 17: Top changes you will need to make to your enterprise risk management approach to address risks associated with your bank's digital asset strategy

Q Which are the top changes you will need to make to your enterprise risk management approach to address risks associated with your bank's digital asset strategy?

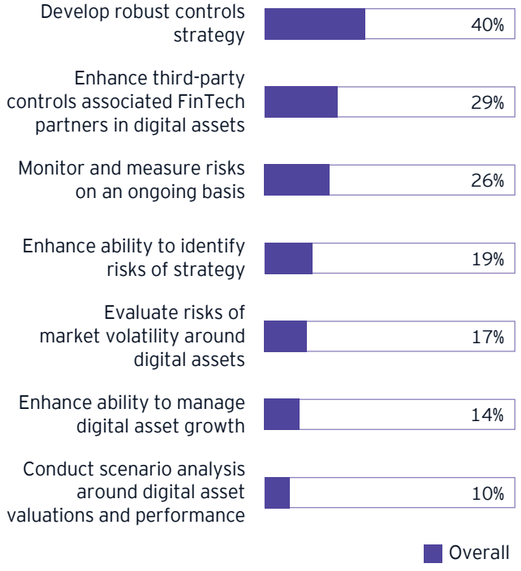
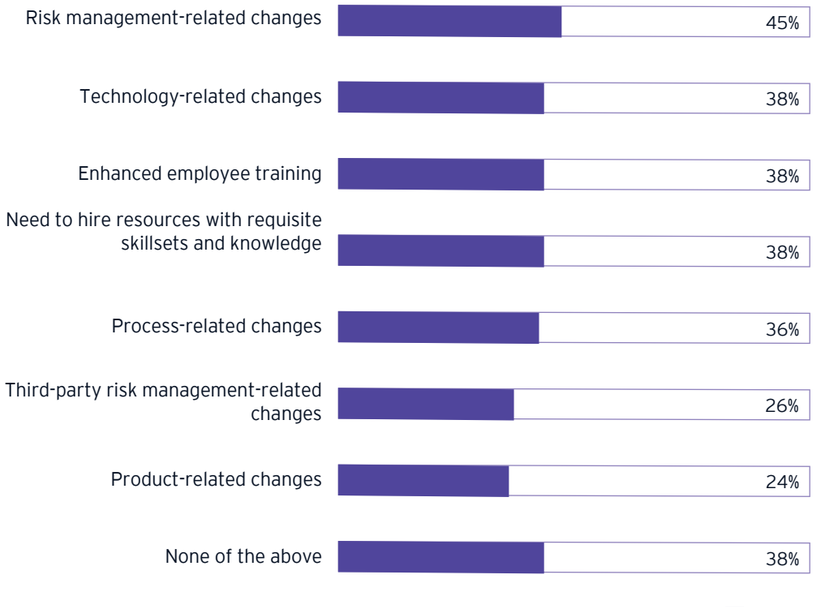


Figure 18: Necessary changes to manage risks associated with digital asset strategies

Q What changes will your bank need to make to manage risks associated with your digital asset strategy?



The imperative to grow through business model innovation inevitably points to more digital operations. Yet the more digital a bank, the more vulnerable it is. That tension justifies CROs' close involvement in — even leadership of — key strategic discussions with business leaders.

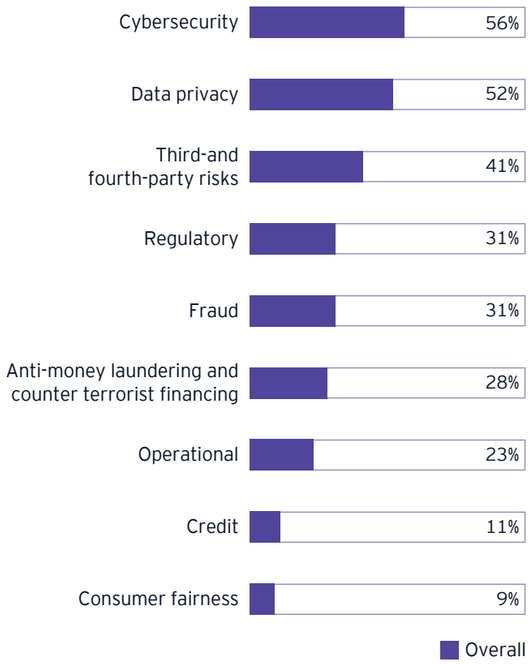
The risk profile of alliances and ecosystems

Digital transformation provides a foundation for banks to grow through ecosystems and alliance strategies. In fact, nearly two-thirds of banks (65%) are executing or developing revised strategies for ecosystems. Nearly as many (63%) focus on customer acquisition in their ecosystem and alliance strategies. Nearly nine in 10 CROs (86%) in Asia-Pacific say customer acquisition is the top priority for alliances and ecosystems. For North American banks, increased efficiency and lower costs are the top objective for ecosystems and alliances, according to 70% of CROs.

All of the potential benefits of ecosystems and alliances are accompanied by increased risk. Cybersecurity and data privacy are the top priorities relative to ecosystems and alliances, though there are other potential issues to track, especially third- and fourth-party risk. *See figure 19*. Just as the success of ecosystems largely depends on the strength of the participants, banks' vulnerabilities depend on the security and data privacy practices of their partners. These risks can vary considerably based on different strategies — full ecosystem development and orchestration, direct investments in joint ventures, looser alliances — banks may adopt. They also vary by region: only 40% of CROs at banks in Europe cite cybersecurity as a top ecosystem risk, versus 77% of their peers in the Middle East and North Africa.

Figure 19: Top risks that will require the most attention from CROs in the next three years with regard to ecosystem and alliance strategies

Q Which are the top risks that will require the most attention from the CRO with regard to your ecosystem and alliance strategy in the next three years?



Half of CROs expect new regulatory requirements on FinTech alliances to have a moderate or major impact on these strategies; the same number expects minimal or no impact. Larger global banks are more prepared to deal with new requirements and are more focused on third- and fourth-party risks, presumably because they'll be involved in larger ecosystems. What's much clearer is that ecosystems and alliances are here to stay and CROs will be more focused on them in coming years.

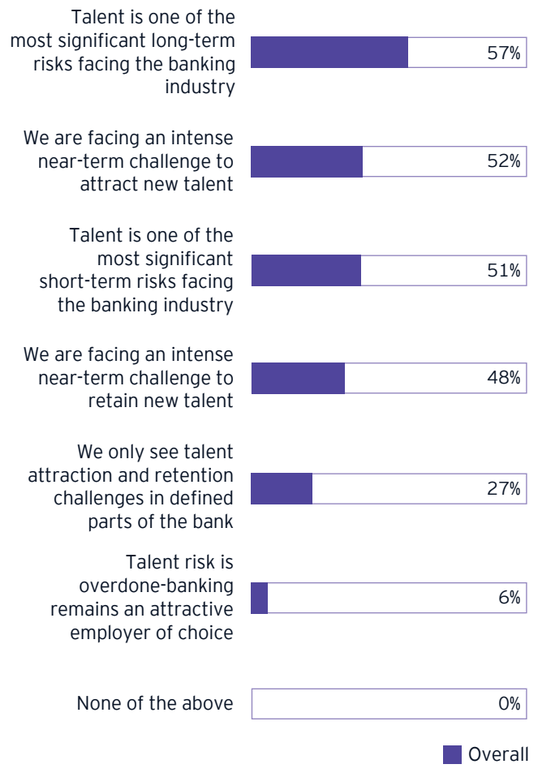
Persistent talent risk across the business

As much as the banking business is being digitized and automated, the vast majority of CROs, along with their C-suite peers, view talent as critical to future success. First and foremost, banks are still struggling to attract the talent they need, both in the risk management function (see chapter 3) and across the business. It's not clear how much, if at all, a recession might soften the labor market. But the fact that business units and functions (not to mention CROs) are all seeking data scientists, data analysts and other tech-oriented skills is an argument for upskilling.

CROs view talent and culture risks to the business from both the short- and long-term perspectives, and from multiple angles. *See figure 20.* Remote and hybrid working, mental wellness, more pervasive use of third-party relationships and alliances — all of these are related to the ongoing shortage of talent that banks are experiencing across the business.

Figure 20: The significance of talent risk to banks

Q How significant is talent risk to your bank and the banking industry?



> "I'm concerned with having the right skills and attracting talent, but also about human capital as a resiliency risk.
>
> — CROs

That more CROs now consider talent a matter of operational resilience illustrates just how urgent talent risk has become. Even strategic changes are now viewed in terms of competing for talent; indeed, 49% of all respondents cited increased ability to attract and retain talent as a top-three reason for enhancing the business model in the next three years, behind only the implementation of major technologies (65%) and improved cost efficiencies (61%).

That number reflects the reality that strategic workforce planning is now a matter for the C-suite and boards, in addition to human resources.

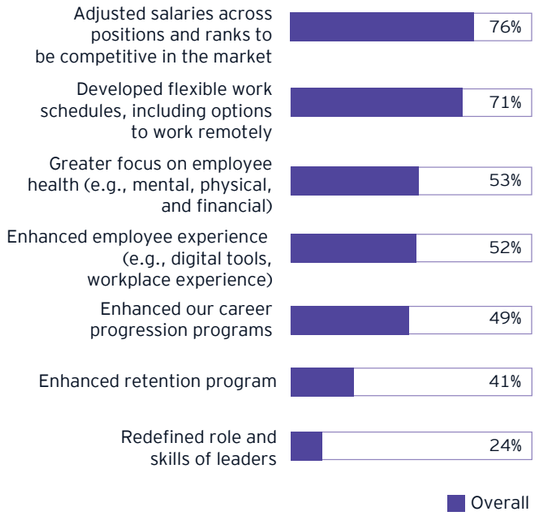
When CROs were asked how they assess their organization's ability to manage change, two of the top three choices were employee-related, with notably higher percentages at G-SIBs. Again, it's clear just how hard it is for banking business leaders to find the people they need to keep pace in a rapidly changing environment.

	All respondents	G-SIBs
Employee turnover	52%	75%
Number of regulatory actions	50%	67%
Employee engagement	45%	67%

Banks have adopted a range of strategies and tactics to address their talent gaps, and despite the industry outlook for the latest bonus season, have started with higher compensation. *See figure 21.* These "all-of-the-above" approaches look likely to become standard operating procedure as banks and firms in other sectors continue to fight for the same scarce skillsets.

Figure 21: Ways in which banks are seeking to attract and retain talent

Q In which of the following ways is your bank addressing the war for talent?



CROs and other senior banking executives, particularly those based in the US, are interested in how the highly liquid talent market will be affected by a recession. They are wondering if labor demand will finally soften and, if so, what the impact on wage inflation will be. CROs may also consider the cultural impacts if workforce reductions become necessary or if popular employee programs (e.g., mental wellness) launched during the pandemic are cut due to cost considerations. If the employee experience deteriorates alongside the economy, banks will find it ever harder to find and retain the right people.

Today, CROs collaborate with chief human resource officers (CHROs) mainly to respond to regulatory inquiries (e.g., skills assessments for internal auditors). Looking ahead, more sophisticated workforce risk competencies with dedicated specialists able to model and mitigate different forms of talent risk will be a hallmark of high-performing risk management functions.

Chapter

03

Building a high-performing risk management function

Like their counterparts in the business, CROs are looking for better technology and new skillsets to drive transformation in pursuit of better outcomes and more efficiency. Those shared needs create empathy and the basis for more strategic and productive collaborations with senior leaders across the enterprise. Part of the pressure that CROs face in determining how many people they need and where to deploy them is that they are often forced to juggle multiple disruptions – internal transformation programs and new regulatory requirements, for instance – in addition to the constants of cyber, credit and operational risks.

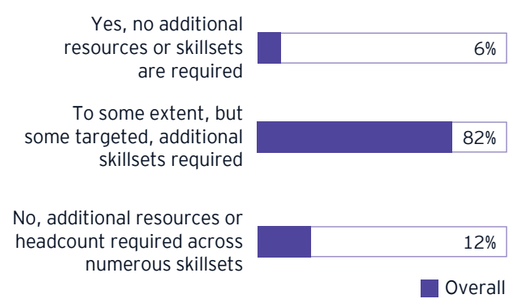
> “I continue to see it’s the people that make the difference. If you’ve got the right talent, you will figure out the tools you need.
>
> – CRO survey respondent

Staffing and talent needs

Highly effective risk management starts with high-performing people, according to CROs. A vast majority (94%) say they need some or many new skills and resources to meet the changing needs of the risk management function. Only a fraction think they have the talent they need. *See figure 22*.

Figure 22: Presence of skills required to address changing risk management needs

Q Is your talent pool equipped to meet the changing needs of the risk management function over the next three years?



The top six most important skills for risk management functions are the same as last year’s survey, with data science and cyber topping the list. *See figure 23*. That everyone is looking for the same skills is a pattern that increases talent risk, as well as labor costs, a dynamic that applies within risk management and other bank functions.

The most in-demand skills reflect the increasingly data-driven nature of risk management. CROs, like their peers in the business, need analytically minded and tech-savvy professionals that can review large amounts of data and find meaningful trends and patterns, especially those that cut across risk management disciplines. But talent needs will morph over time, both as risk profiles change and regulatory requirements evolve. Consider how risk management professionals with design thinking skills can help ensure processes are set up to conform with complex requirements, such as the UK’s Consumer Duty regulation.

Interestingly, CROs at G-SIBs see a greater need for more talent in governance, risk and controls (58%), climate change (50%) and operational resilience (50%) than their peers. Agility and adaptability are highly sought-after attributes for risk management pros, especially at large organizations that are trying to break down organizational silos in their risk management functions. *See figure 24*. There is every reason to believe these transferable skills will continue to grow in importance.

> “We need specialized skills to challenge what’s going on in technology.
>
> – CRO survey respondent

Figure 23: Top skills required in the risk management function over the next three years

Q What are the most important skillsets required in the risk management function over the next three years?

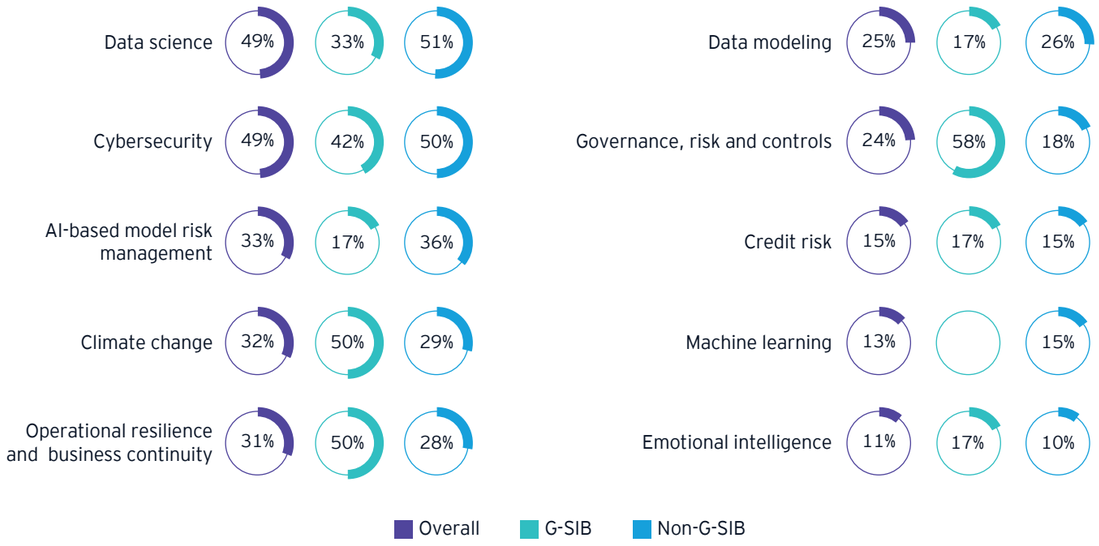
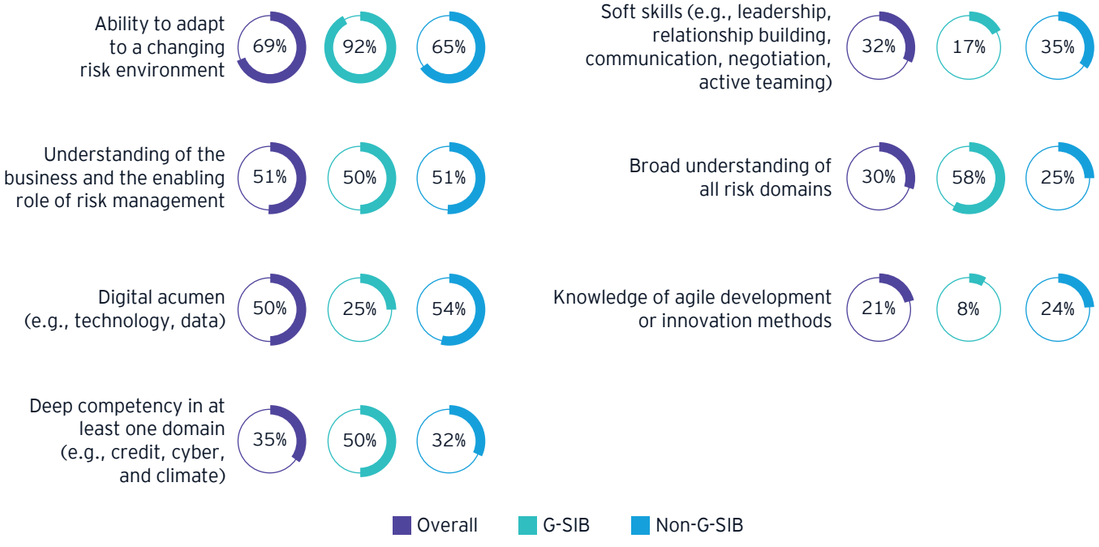


Figure 24: Top-priority skills for risk management teams to better manage risk

Q In the coming years, what are the top skillsets your risk management resources should prioritize to better manage risk?



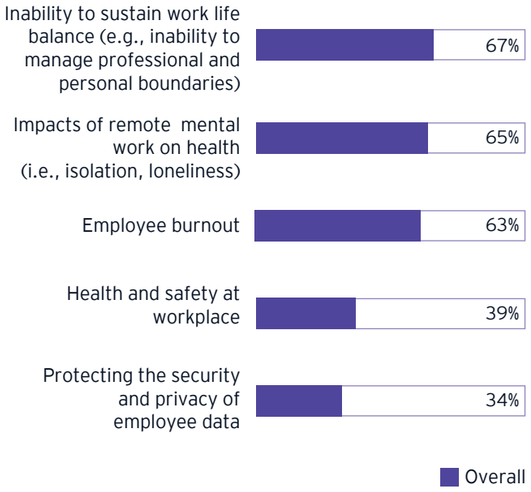
In many cases, CROs are looking to retrain existing risk staff in particular areas of expertise, including emerging competencies, such as climate. Some banks are engaging third-party providers for these critical services. Though 77% of CROs expect to increase their headcount, a recession may force them to operate with fewer – but more skilled – people. Their counterparts on the business side will likely face the same challenge. More business acumen is necessary to pre-empt risk, rather than simply respond to incoming threats.

Supporting current teams and talent: CROs are focused on the mental health of their employees and concerned about the cultural impact of remote and hybrid working, which are also enterprise-wide concerns. *See Figure 25.* As underscored during the pandemic, mental health concerns highlight the link between operational resilience and workforce resilience.

> "I am a big believer of having employees starting in the business, earning the experience and then moving into a risk role with the perspective from those other positions.
>
> – CRO survey respondent

Figure 25: Top concerns associated with protecting employee wellbeing, health and safety on an ongoing basis

Q As you consider your approach to a post COVID-19 new normal, what are your top concerns associated with protecting employee wellbeing, health and safety on an ongoing basis?



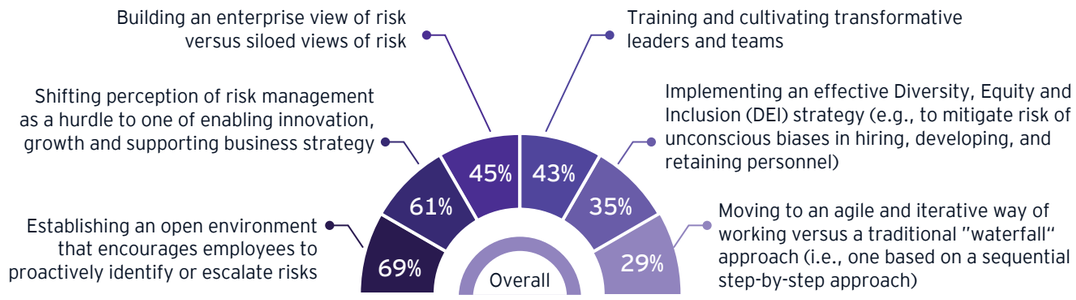
The challenges regarding isolation and work-life balance may be substantial at some organizations. However, some CROs tell us that they are accustomed to hybrid working because they have long maintained operations in different markets and regions. Other CROs may look to source talent from more locations if their banks support "work from anywhere" models in the future.

Sustaining strong cultures with risk management

CROs aspire to build cultures that encourage the proactive identification of risks and that are capable of enabling the business and motivated to do so. *See figure 26*. That means more than just sharing risk knowledge and leading practices with the business. Rather, the goal for risk leaders should be to fully engage in the formation of new business models and in the execution of growth and innovation strategies. Because hybrid working has created new challenges for managing people, it's likely that more banks will emphasize training for transformative leadership in the future. Discipline in managing risk must be a tenet of transformative leadership in the banking sector, particularly given the degree of disruption posed by hybrid and remote working models.

Figure 26: Top steps to building positive cultures, behaviors and ways of working in your risk organization

Q What are the top steps to building a positive culture, behaviors and ways of working in your risk organization?



Two-thirds of survey respondents cited culture as the top concern related to remote and hybrid working models, a notable jump from 55% last year. *See figure 27*. Notably information, data security and cyber risk are now less urgent concerns (cited by only 33% of CROs in this year's survey) as many banks hardened the endpoints of systems and platforms that support remote working. CROs see remote and hybrid working as a challenge to sustaining strong cultures and in developing people and teams. *See figure 28*.

> "The wellbeing of talent continues to be a risk. We are mitigating turnover by addressing single person dependencies.
>
> – CRO survey respondent

Figure 27: Biggest concerns about remote and hybrid working models

Q Many organizations have concluded increased levels of remote and virtual working will be part of their future hybrid operating model. What are your biggest concerns about this working model?

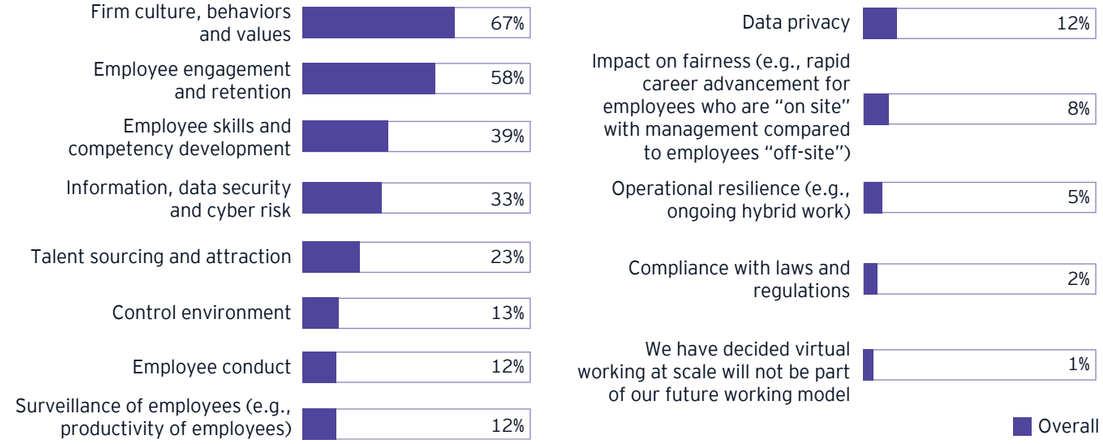
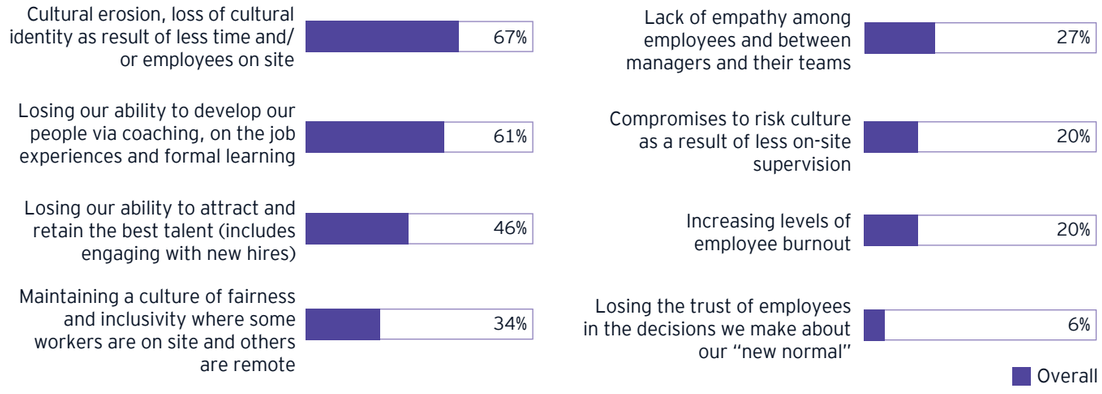


Figure 28: Top challenges to maintaining a common culture

Q Looking forward, what are the top challenges to maintaining a common culture?



Reflecting the importance of sustaining cultures, CROs plan to more actively monitor employee wellbeing and engagement through a range of tools and metrics, including:

- More routine employee surveys: **59%**
- Cultural dashboards: **48%**
- Turnover, number of open and filled positions and other human capital measures: **42%**
- More routine use of focus groups and interviews: **36%**
- Monitoring control and risk metrics: **34%**

These can be effective tools, though in the future we expect to see adoption of even more sophisticated techniques for analyzing employee sentiment through continuous employee listening (e.g., always-on feedback channels, "pulse" and topical surveys, and monitoring engagement in the metaverse).

Advancing risk management technology

As with their peers in the business, CROs see technology as a means to optimize their own operations and equip their teams to perform their jobs more efficiently and effectively. Currently, AI and machine learning are mainly being used within risk management to automate manual tasks, support better credit decision-making, identify cyber attacks and monitor for potential financial crimes. *See figure 29.* CROs expect those applications to be the priorities during the next few years as well. At G-SIBs, there is much greater focus on automation and financial crime monitoring. *See figure 30.*

Figure 29: Activities with the most significant use of AI and machine learning

Q What are the most significant ways your organization is using machine learning and/or AI?

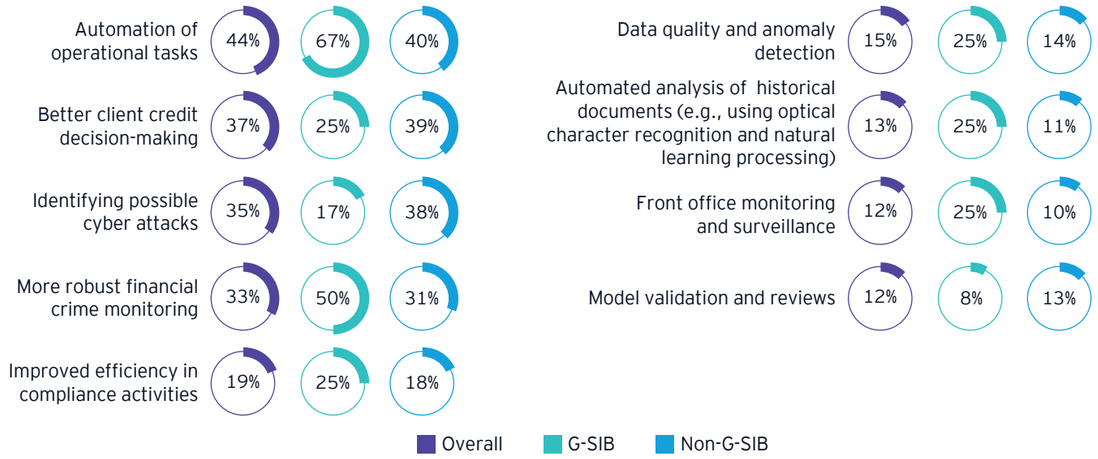
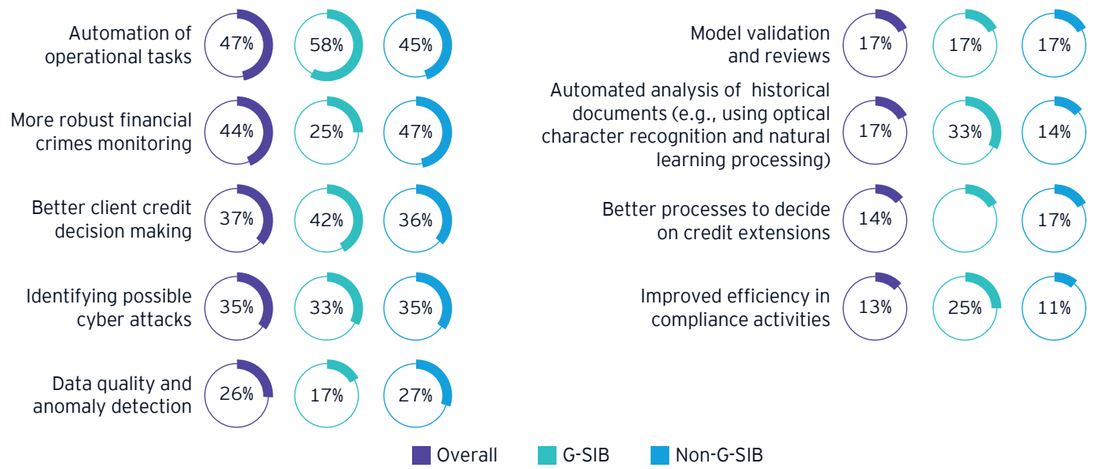


Figure 30: Activities where machine learning and AI will materially increase in the next three years

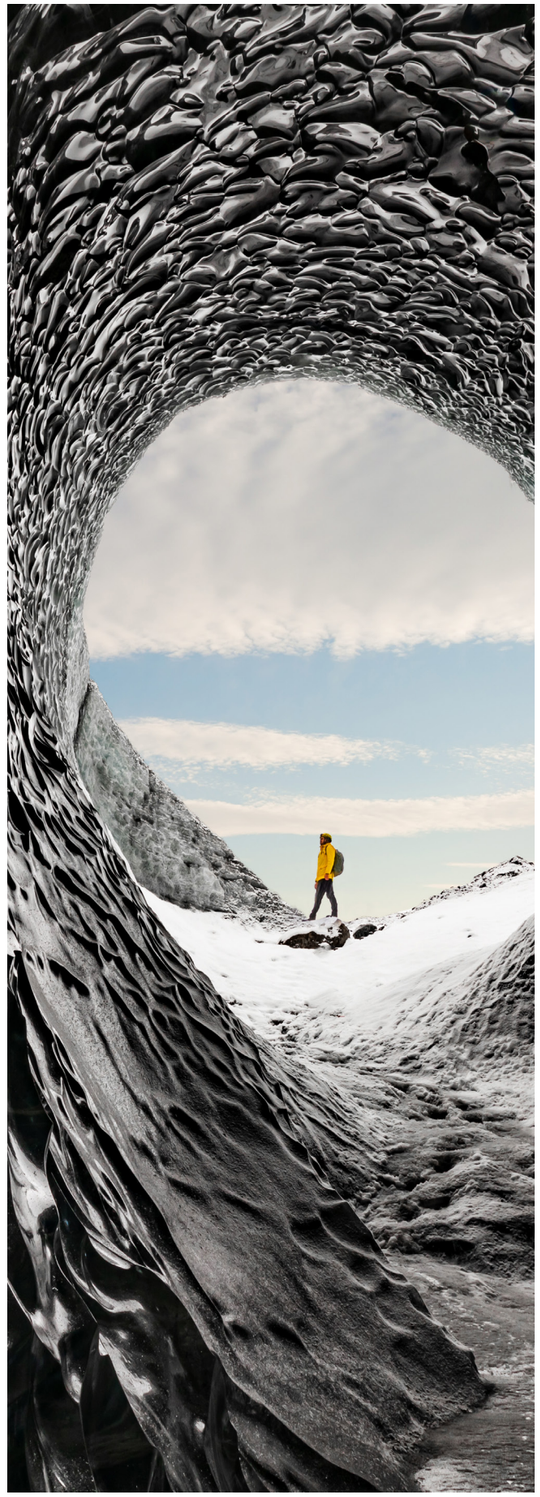
Q For which of the following activities is your organization using machine learning and/or AI that will materially increase in the next three years?



CROs are also leading digital transformation initiatives within risk operations, with many of the same priorities, plus more extensive use of analytics and automation. *See figure 31.*

Figure 31: Digital transformation priorities for risk management and the second line of defense

Q In what areas do you think you will accelerate your digital transformation of second line of defense and risk management (top six choices)?



Looking ahead: an ever-evolving risk matrix

The results of the latest EY-IIF survey of banking CROs indicate that risk management remains at the heart of banking. The findings also make clear that CROs' jobs won't be getting any easier in the near future. Immediate-term priorities are frequently disrupted by world events and other external forces. Consider how steadily worsening economic conditions in the months since we conducted our survey have likely increased CRO focus on credit risk.

While this year's survey saw cyber jump ahead of credit as the top CRO risk priority for the next 12 months, the respective positions could very well flip next year, if the deteriorating economic environment results in more credit losses than banks have seen in years. Large-scale cyber attacks and ongoing geopolitical volatility could put further pressure on banks' financial situations. Indeed, the intricate connections among these different types of risks require CROs to conceive of threats outside of traditional categories, as well as to design new types of controls and, in some cases, refine how they structure their teams.

Emerging risks that become suddenly urgent today don't alleviate the need for CROs to think deeply about what's coming tomorrow — or next quarter, or next year, or in 36 months. The job description requires CROs to both see around corners and to make sure all the doors and windows are safely locked — all day, every day — and how to respond if and when there is a breach. The bottom line is that the most effective banking CROs must excel in both the strategic and tactical realms, while also helping the business succeed in delivering innovative, differentiating and fully secure services that satisfy ever-rising customer expectations.

There is no denying that banks have made substantial progress since the global financial crisis in enhancing risk management practices and establishing robust controls across the business. Effectively managing risks during the next decade necessitates building on that impressive track record, with creative thinking and bold action, more advanced technology and new talent.

Research methodology and participant demographics

The global EY organization, 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 2022 through October 2022. Participating banks' CROs or other senior risk executives were interviewed, completed a survey, or both. In total, 88 financial institutions across 30 countries participated.

Participating banks were fairly diverse in terms of asset size, geographic reach and type of bank. Regionally, those banks were headquartered in Asia-Pacific (11%), Europe (16%), Latin America (18%), Middle East and Africa (19%) and North America (36%). Of those, 14% are G-SIBs.

EY contacts

Global

Jan Bellens
US
jan.bellens1@ey.com
+1 212 360 9098

Federico Guerreri
Italy
federico.guerreri@it.ey.com
+39 027 221 22326

Sonya Koerner
UK
skoerner@uk.ey.com
+44 207 951 6495

Christopher Woolard
UK
christopher.wooldard@uk.ey.com
+44 207 760 8166

Americas

Tom Campanile
US
thomas.campanile@ey.com
+1 212 773 6461

Peter Davis
US
peter.davis@ey.com
+1 212 773 7042

Marlene Devotto
Chile
marlene.devotto@cl.ey.com
+56 229 162 752

Adam Girling
US
adam.giring@ey.com
+1 212 774 9514

Bill Hobbs
US
bill.hobbs@ey.com
+1 704 338 0608

Debra Greenberg
US
debra.greenberg@ey.com
+1 212 773 6592

Mario Schlener
Canada
marrio.schlener@ca.ey.com
+1 416 932 5959

Marc Saidenberg
US
marc.saidenberg@ey.com
+1 212 773 9361

Asia-Pacific

Eugène Goyne
Hong Kong
eugène.goyne@hkey.com
+852 2849 9470

Doug Nixon
Australia
douglas.nixon@au.ey.com
+61 29 276 484

Kentaro Ogata
Japan
Kentaro.ogata@jp.ey.com
+81 335 031 110

David Scott
Hong Kong
david.scott@hk.ey.com
+852 2670 3070

Radish Singh
Singapore
radish.singh@sg.ey.com
+65 6540 7338

EMEIA

Kristin Bekkeseth
Norway
Kristin.bekkeseth@no.ey.com
+47 942 47 130

Richard Brown
UK
rbrown@uk.ey.com
+44 20 7951 4090

Bernhard Hein
Germany
bernhard.hein@de.ey.com
+49 711 9881 14338

Ivica Stankovic
Kuwait
Ivica.s@kw.ey.com
+965 229 550 56

Stuart Thomson
UK
sthomson@uk.ey.com
+44 131 777 2446

Matthew Walker
South Africa
matthew.h.walker@za.ey.com
+27 11 772 4436

Max Weber
Germany
Max.weber@de.ey.com
+49 711 9881 15484

IIF contacts

Andrés Portilla
Managing Director and Head, Regulatory Affairs
US
aportilla@iif.com
+1 202 857 3645

Martin Boer
Senior Director, Regulatory Affairs
US
mboer@iif.com
+1 202 857 3636

Hillary Veals
Program Associate, Regulatory Affairs
US
hveals@iif.com
+1 202 857 3601

Thank you ...

A special thank you to the EY core survey team members for their work on the survey, including **Mohammed Bishawi, Victoria Bolton, J.P. Burns, Skylar Liang, A.J. Stanley, Tyler Teague and Griffin Wilson.**

About the Institute of International Finance

The Institute of International Finance (IIF) is the global association of the financial industry, with about 400 members from more than 60 countries. The IIF provides its members with innovative research, unparalleled global advocacy, and access to leading industry events that leverage its influential network. 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, professional services firms, exchanges, 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

EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

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 are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

What makes EY distinctive in financial services

Over 84,000 EY professionals are dedicated to financial services, serving the banking and capital markets, insurance, and wealth and asset management sectors. We share a single focus — to build a better financial services industry, one that is stronger, fairer and more sustainable.

© 2022 EYGM Limited.
All Rights Reserved.

EYG no. 011242-22Gbl
2209-4090634 BDFSO
ED None

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

ey.com